Bundesamt
für Sicherheit in der
Informationstechnik

Ausgewählte Informationen für IT-Betreiber

Cyber-Sicherheit bei Wahlen

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: 0800 274 1000 (kostenfreie Service-Hotline des BSI)
E-Mail: oeffentlichkeitsarbeit@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

Einleitung

Die Digitalisierung des beruflichen und privaten Alltags bringt viele Vorteile mit sich. Routineaufgaben lassen sich automatisieren, Abläufe werden effizienter und bisher voneinander unabhängige Prozesse können miteinander verknüpft werden, sodass neue Möglichkeiten entstehen. Als Bindeglied fungiert das Internet, indem es zentrale Dienste und mobile Systeme weltweit miteinander vernetzt. Das Smartphone ist dabei nur ein Zwischenschritt bei der zunehmenden Durchdringung des Alltags mit "smarten" Gegenständen.

Andererseits wird unsere Gesellschaft durch die Digitalisierung aber auch verwundbarer gegenüber Fehlfunktionen und Angriffen auf die Informationstechnik. Der jährliche Lagebericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zeigt, dass inzwischen alle gesellschaftlichen Bereiche von Cyber-Angriffen betroffen sind. Oft geht es den Tätern dabei ums Geld, etwa bei der Erpressung mittels Schadprogrammen, die unerlaubt Dateien verschlüsseln ("Ransomware"), oder mittels Überlastungsangriffen auf Webseiten ("Denial of Service"). Es gibt jedoch auch Cyber-Angriffe, bei denen Angreifer gezielt vertrauliche Informationen stehlen oder Schäden bei der betroffenen Institution anrichten wollen.

Insbesondere vor dem Hintergrund der Diskussion in den USA über mögliche Einflussnahmen auf die dortige Präsidentschaftswahl besteht auch in Deutschland die Sorge, dass hierzulande Wahlen durch Cyber-Angriffe beeinträchtigt oder manipuliert werden könnten. Zwar erfolgt die Stimmabgabe bei der Bundestagswahl auf Papier, dennoch spielt die Informationstechnik sowohl im Wahlkampf als auch bei der Organisation der Wahlen sowie bei der Aufbereitung und Präsentation der Wahlergebnisse eine große Rolle. Auch die Medienarbeit und Kommunikation ist in hohem Maße von funktionierender Informationstechnik abhängig. Täter könnten beispielsweise versuchen, Benutzerkonten von Kandidaten in Sozialen Medien zu kapern und über diese Konten falsche Informationen zu verbreiten. Oder sie könnten versuchen, vertrauliche Informationen von einer Partei zu stehlen und zu veröffentlichen, um dieser Partei zu schaden.

Im Folgenden hat das BSI deshalb für Betreiber von Informationstechnik einige ausgewählte BSI-Publikationen mit Hinweisen und Empfehlungen zusammengestellt, die aus Sicht des BSI für die Cyber-Sicherheit im Kontext von Wahlen besonders relevant sind. Diese Empfehlungen ersetzen nicht die systematische Herangehensweise, wie sie beispielsweise im IT-Grundschutz des BSI beschrieben ist, sondern sollen ein Schlaglicht auf die Aspekte werfen, die im Hinblick auf die oben dargestellten Gefahren im besonderen Maße berücksichtigt werden sollten. Darüber hinaus empfiehlt das BSI, die Informations- und Dienstleistungsangebote der Allianz für Cyber-Sicherheit (https://www.allianz-fuer-cybersicherheit.de) zu nutzen und für den Schutz der eigenen Institution anzuwenden.

Bundesamt
für Sicherheit in der
Informationstechnik

SENSIBILISIERUNG

Cyber-Bedrohungen – ein Einstieg

Häufig gestellte Fragen und Antworten

Cyber-Angriffe und Cyber-Sicherheit werden derzeit intensiv in der Öffentlichkeit diskutiert. Für Hersteller, Dienstleister und Anwender von Informationstechnik stellen sich in diesem Zusammenhang viele Fragen, insbesondere hinsichtlich der Betroffenheit des eigenen Verantwortungsbereichs. Das vorliegende Dokument greift die wichtigsten und häufigsten Fragen zur Cyber-Sicherheit auf und vermittelt anhand der Antworten einen schnellen Einstieg in das Thema.

Was sind Cyber-Angriffe?

Informationstechnische Systeme (IT-Systeme) werden heute kaum noch isoliert eingesetzt, sondern sind in der Regel global vernetzt. Die Kommunikation zwischen den IT-Systemen erfolgt meist über lokale und globale Netze, beispielsweise über das Internet oder über Mobilfunknetze. Auch werden fast alle Computer, die nicht ständig an ein Datennetz angeschlossen sind, ab und zu mit neuen Informationen versorgt, zum Beispiel wenn neue Datenbestände oder neue Programmversionen mit Hilfe von Datenträgern eingespielt werden.

Die Gesamtheit dieser global miteinander kommunizierenden IT-Systeme wird *Cyber-Raum* (cyber space) genannt. Ein wichtiger Teil des Cyber-Raums ist das Internet, in das immer mehr IT-Kommunikationsbeziehungen verlagert werden. Weltweit werden jedoch auch viele andere Vernetzungsstrukturen genutzt.

Die Möglichkeiten der globalen Vernetzung werden allerdings auch von Tätern für schädliche Aktivitäten missbraucht. Von einem *Cyber-Angriff* (cyber attack) spricht man, wenn der Cyber-Raum als primärer Angriffsweg benutzt wird oder selbst das Ziel eines Angriffs ist. Trotz der großen Anzahl unterschiedlicher Angriffsziele und möglicher Angriffsmethoden kann die Motivation hinter einem Cyber-Angriff häufig auf Geld, Informationsbeschaffung, Sabotage, Einflussnahme oder Durchsetzung politischer Interessen zurückgeführt werden.

Wer sind die Cyber-Angreifer?

Die vorsätzlich handelnden Angreifer im Cyber-Raum lassen sich in folgende Gruppen differenzieren:

- Cyber-Aktivisten: Angreifer, die durch einen Cyber-Angriff auf einen politischen, gesellschaftlichen, sozialen, wirtschaftlichen oder technischen Missstand aufmerksam machen oder eine diesbezügliche Forderung durchsetzen wollen („Hacktivismus“). Die Motivation hinter dem Angriff ist Einflussnahme. Der durch einen Cyber-Angriff entstandene Schaden wird in Kauf genommen bzw. forciert, um eine höhere Aufmerksamkeit zu erlangen. Sogenannte *ethische Hacker* fokussieren sich auf gesellschaftliche oder soziale Themen.
- Cyber-Kriminelle: Die Motivation von Cyber-Kriminellen ist es, mithilfe der Informationstechnik auf illegalen Wegen Geld zu verdienen. Die Bandbreite reicht von organisierter Cyber-Kriminalität bis hin zu einfacher Kriminalität mit geringen Schäden.

- Wirtschaftsspione im Cyber-Raum: Durch die Vorteile des Internets ergeben sich für Spione neue Möglichkeiten. Wirtschaftsspionage und Konkurrenzausspähung dienen finanziellen Interessen. Interne Informationen über Mitbewerber und deren Produkte bieten geldwerte Vorteile im globalen Wettbewerb.
- Staatliche Nachrichtendienste im Cyber-Raum: Cyber-Angriffe durch staatliche Nachrichtendienste dienen – im Gegensatz zur Wirtschaftsspionage – nicht primär finanziellen Interessen, sondern der Informationsbeschaffung und der Einflussnahme.
- Staatliche Akteure im Cyber-War: Im militärischen Sektor wird der Cyber-Raum inzwischen vielfach als weitere wichtige Domäne neben den klassischen militärischen Domänen Land, See, Luft und Weltraum angesehen.
- Cyber-Terroristen: Terroristen können Cyber-Angriffe wie staatliche Akteure und Kriminelle nutzen, um unterschiedliche Ziele anzugreifen und somit ihre Ideologie zu verbreiten und ihren Einfluss auszuweiten.
- Skript-Kiddies: Die Gruppe der Skript-Kiddies führt Cyber-Angriffe durch, um Fähigkeiten und Wissen in der Praxis auszutesten. Es werden keine finanziellen Interessen verfolgt. Die Auswahl der Angriffsziele ist unspezifisch und vielfach allein vom Grad der Absicherung abhängig.

Diese Tätergruppen unterscheiden sich vor allem hinsichtlich ihrer Motivation, Zielsetzungen und Ressourcen. Auf technischer Ebene lässt sich hingegen nicht immer unmittelbar feststellen, welche Tätergruppe hinter einem konkreten Cyber-Angriff steckt.

Warum ist der Cyber-Raum so attraktiv für Täter?

In der Informationsgesellschaft hängt vieles von der schnellen und kostengünstigen Kommunikation über den Cyber-Raum ab, denn immer mehr geschäftliche und gesellschaftliche Prozesse werden dort hin verlagert. Durch diese Entwicklung ist der Cyber-Raum auch für Angreifer immer attraktiver geworden.

Der Cyber-Raum hat eine Reihe von Eigenschaften, die für einen potenziellen Angreifer günstig sind: Räumliche Entfernungen spielen kaum eine Rolle. Der Angreifer kann aus der Ferne agieren, ohne sich vor Ort einem unmittelbaren Risiko auszusetzen. Gerade im Internet bestehen außerdem vielfältige Tarnungsmöglichkeiten für den Täter, da viele Dienste im Internet bewusst offen gestaltet sind.

Besonders Cyber-Kriminelle profitieren davon, dass es im Cyber-Raum mithilfe spezieller Angriffstechniken möglich ist, eine Vielzahl unterschiedlicher Ziele parallel anzugreifen. Selbst wenn ein solcher Angriff nur bei einem geringen Prozentsatz an Zielen tatsächlich erfolgreich ist, entsteht oftmals insgesamt ein erheblicher Schaden. Hierzu trägt auch die starke Verbreitung von Bezahlverfahren und Finanztransaktionen über das Internet bei.

Welche Arten von Cyber-Angriffen gibt es?

Cyber-Angriffe werden häufig anhand des Angriffszwecks kategorisiert, also entsprechend der Wirkung, welche die Angreifer auf den Angriffszielen herbeiführen wollen:

- Angriffe auf die Vertraulichkeit: Die Täter können versuchen, vertrauliche Informationen auszuspionieren, indem sie zum Beispiel ein Funknetz abhören oder gelöschte Informationen wiederherstellen.
- Angriffe auf die Integrität: Manipulationen, zum Beispiel an Informationen, Software oder Schnittstellen, spielen bei vielen Cyber-Angriffen eine wichtige Rolle.
- Angriffe auf die Verfügbarkeit: Die Täter können versuchen, Informationen oder IT-Dienste zu sabotieren, beispielsweise durch verteilte Denial-of-Service-Angriffe (DDoS-Angriffe).

Hierbei ist zu beachten, dass Cyber-Angriffe häufig mehrere Angriffsschritte umfassen, wobei die einzelnen Schritte unterschiedliche Zwecke haben können. Ein Cyber-Angriff mittels eines Spionage-Schadprogramms umfasst beispielsweise zumindest die Installation des Schadprogramms (Angriff auf die Integrität) und den eigentlichen Abfluss von Informationen (Angriff auf die Vertraulichkeit).

Neben dem Angriffszweck können Cyber-Angriffe auch dahingehend unterschieden werden, ob es sich um gezielte Angriffe (ein Ziel oder wenige ausgesuchte Ziele) oder um großflächige Angriffe (möglichst viele beliebige Ziele gleichzeitig) handelt. Diese beiden Angriffsarten sind mit bestimmten Vor- und Nachteilen für den Täter verbunden: Ein breit gestreuter Angriff verspricht z. B. eine höhere Wahrscheinlichkeit, dass

der Angriff zum Erfolg führt. Allerdings fallen derart großflächige Angriffe meist eher auf und provozieren so zeitnahe Gegenmaßnahmen.

Eine umfassende Übersicht der gegenwärtig bekannten Cyber-Angriffsmethoden hat das BSI in der Cyber-Sicherheits-Analyse *Register aktueller Cyber-Gefährdungen und -Angriffsformen*[1] zusammengestellt.

Welchen Schaden können Cyber-Angriffe anrichten?

Typische Angriffsziele im Cyber-Raum sind Informationen, IT-Dienste und IT-Systeme. Der mögliche Schaden, der durch Cyber-Angriffe entstehen kann, richtet sich somit nach dem Wert dieser Ziele für Bürger, Institutionen und die Gesellschaft.

Für den einzelnen Bürger besteht insbesondere die Gefahr, dass er erhebliche finanzielle Verluste durch Cyber-Angriffe erleidet. Manipulationen bei Internet-Bezahlvorgängen oder beim Internet-Banking können dazu führen, dass Geld auf den Konten der Täter landet oder dass das Konto des Opfers leergeräumt wird.

Wirtschaftsspionage und Konkurrenzausspähung sind ein besonderes Risiko für innovative Unternehmen. Durch den Diebstahl von vertraulichen Informationen, etwa aus den Bereichen Produktstrategie oder Forschung und Entwicklung, kann sich ein Konkurrent unter Umständen entscheidende Vorteile verschaffen. Angebotskalkulationen in einem Bieterverfahren oder Vertriebsinformationen sind für Wettbewerber ebenfalls von Interesse. Cyber-Angriffe können auch eine Rolle bei der Erpressung von Unternehmen spielen. Die Täter können zum Beispiel damit drohen, vertrauliche Informationen zu veröffentlichen oder wichtige IT-Dienste, die das Unternehmen für Kunden oder Partner anbietet, für einen längeren Zeitraum zu stören.

Ein besonders hohes Schadenspotenzial besteht bei Angriffen auf die Verfügbarkeit Kritischer Infrastrukturen. Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

Bei der Bewertung des möglichen Schadens ist zu beachten, dass sich Cyber-Angriffe zwar häufig gegen konventionelle Informationstechnik – also beispielsweise Webserver oder Datenbanken – richten, allerdings können auch Systeme zur industriellen Prozesssteuerung / -automatisierung / -leittechnik sowie digitale Mess- / Steuerungs- / Regelsysteme von Cyber-Angriffen betroffen sein. Solche Angriffe können direkte Auswirkungen auf die Sicherheit einer industriellen Anlage haben. Der auch in der Öffentlichkeit intensiv diskutierte Vorfall „Stuxnet“ hat gezeigt, dass dies nicht nur ein theoretisches Szenario ist.

Warum sind Cyber-Angriffe möglich?

Um erfolgreiche Cyber-Angriffe durchzuführen, machen sich Täter vor allem die folgenden Arten von Schwächen zunutze: Software-Schwachstellen, Design-Schwachstellen, Konfigurationsschwachstellen und menschliche Fehlhandlungen. Alle diese Arten von Schwächen lassen sich bei der heutigen Komplexität der Informationsverarbeitung prinzipiell nicht vollständig vermeiden.

- Software-Schwachstellen (Implementierungs-Schwachstellen): Oft können Schwachstellen auf Programmierfehler zurückgeführt werden. Da der Quellcode größerer Software-Produkte mehrere Millionen Programmierzeilen lang sein kann, sind solche Software-Schwachstellen nicht selten.
- Design-Schwachstellen: Anders als Software-Schwachstellen sind Design-Schwachstellen nicht in der konkreten Programmierung einer Software begründet, sondern in der Spezifikation von Funktionsweisen, Schnittstellen, Datenformaten, Übertragungsprotokollen o. ä.

1 https://www.bsi.bund.de/ContentBSI/Themen/Cyber-Sicherheit/Analysen/Grundlagen/BSIa001.html

- Konfigurationsschwachstellen: Software-Produkte lassen sich in der Regel mittels Konfigurationseinstellungen an die jeweilige konkrete Einsatzumgebung anpassen. Solche Einstellungen haben häufig auch Einfluss auf die Sicherheit, sodass durch ungeeignete Konfiguration von Software ebenfalls Schwachstellen entstehen können – zum Beispiel, wenn Sicherheitsfunktionen deaktiviert oder Zugriffsrechte nicht restriktiv genug konfiguriert werden.
- Menschliche Fehlhandlungen: Täter verwenden vielfältige Tricks, um Mitarbeiter zur Mithilfe bei Cyber-Angriffen zu bewegen („Social Engineering"). Zum Beispiel werden verlockende Inhalte in Aussicht gestellt, um die Benutzer dazu zu bringen, auf eine bestimmte Schaltfläche zu klicken oder es werden Sicherheitsprobleme vorgegaukelt, um den Benutzern ihre Passwörter zu entlocken. Oft ist den Mitarbeitern gar nicht bewusst, dass sie zu einem Sicherheitsvorfall beigetragen haben.

Hersteller veröffentlichen oft Aktualisierungen (Patches oder Updates) für ihre Produkte, wenn technische Schwachstellen darin bekannt werden. Dies ist bei Design-Schwachstellen in der Regel schwieriger als bei Software-Schwachstellen. Meist ist es Aufgabe der Benutzer, die Aktualisierungen auf ihren Systemen einzuspielen, um die jeweiligen Schwachstellen zu beseitigen. Verfahren, bei denen Software-Produkte selbsttätig im Internet nach Aktualisierungen suchen und diese gegebenenfalls einspielen, gewinnen zunehmend an Bedeutung.

Um den Zeitraum bis zur Veröffentlichung eines Patches zu überbrücken, werden häufig auch sogenannte Workarounds veröffentlicht. Hierbei handelt es sich um Hinweise, wie durch Änderungen der Konfiguration, der Anwendungsumgebung, der Nutzungsart o. ä. vermieden werden kann, dass die Schwachstelle ausgenutzt wird. Workarounds können auch darin bestehen, bestimmte Funktionen der Software nicht zu nutzen, bis ein entsprechender Patch zur Verfügung steht.

Insgesamt wird der Erfolg von Cyber-Angriffen vor allem durch folgende Faktoren begünstigt:

- In vielen Fällen nutzen Täter technische Schwachstellen aus, bevor sie öffentlich bekannt werden („Zero Day"). Programme, die solche neuen Schwachstellen ausnutzen („Exploits"), werden auf Untergrundmarktplätzen gehandelt.
- In dem Zeitraum zwischen dem Bekanntwerden einer Schwachstelle und dem Erscheinen eines entsprechenden Patches sind viele betroffene Systeme ungeschützt. Workarounds sind oft unbequem oder können aus organisatorischen Gründen nur schwer umgesetzt werden.
- Neu veröffentlichte Updates und Patches werden bei vielen Institutionen erst nach Tagen, Wochen oder überhaupt nicht eingespielt. Dies kann zum Beispiel an mangelnden Ressourcen, organisatorischen Problemen oder an Inkompatibilitäten zwischen verschiedenen Komponenten liegen.
- Informationstechnik und die damit verbundenen Sicherheitsaspekte sind heute so komplex, dass viele Benutzer trotz Sensibilisierung und Schulung mit der Einhaltung der Sicherheitsrichtlinien überfordert sind.

Welche aktuellen Bedrohungen der Cyber-Sicherheit gibt es?

Über Cyber-Angriffe wird zunehmend auch außerhalb der Fachkreise in den Medien berichtet. Große Aufmerksamkeit hat beispielsweise eine Serie von Cyber-Angriffen auf IT-Dienste des Konzerns SONY im Jahr 2011 ausgelöst. Die Täter hatten sich dabei Zugriff auf IT-Systeme verschafft, auf denen große Mengen an Kundendaten gespeichert waren. Im Verlauf der Bewältigung hat SONY umfangreiche Maßnahmen ergriffen, zeitweise wurden auch bestimmte IT-Dienste abgeschaltet.

Erhebliche Folgen hatte auch der Cyber-Angriff auf das niederländische Unternehmen DigiNotar, das als Zertifizierungsstelle sogenannte *TLS/SSL-Zertifikate* herausgegeben hat. Mithilfe solcher TLS/SSL-Zertifikate können IT-Systeme die Identität anderer IT-Systeme, mit denen sie über das Internet kommunizieren, überprüfen. 2011 gelang es dem Täter, sich Zugriff auf Systeme von DigiNotar zu verschaffen und gefälschte Zertifikate zu erstellen. Dies ist ein schwerwiegender Sicherheitsvorfall, da solche gefälschten Zertifikate unter Umständen für vielfältige Folgeangriffe benutzt werden können. Durch Änderungen an zentralen Sperrlisten bzw. durch Software-Updates mussten die Hersteller von Internet-Browsern die gefälschten Zertifikate für ungültig erklären. Nur wenige Wochen nach dem Vorfall war das Unternehmen DigiNotar insolvent.

Dass sich Cyber-Angriffe auch über einen sehr langen Zeitraum erstrecken können, zeigen Berichte über Cyber-Angriffe auf das kanadische Technologieunternehmen Nortel. 2012 wurde bekannt, dass Täter ab dem Jahr 2000 mehrere Jahre lang Cyber-Spionage bei Nortel betrieben haben.

Das Lagezentrum des BSI beobachtet und bewertet die Bedrohungslage im Cyber-Raum kontinuierlich. Auch Analysen der abgewehrten Angriffe auf die Regierungsnetze des Bundes fließen dabei ein. Die folgenden statistischen Informationen zeigen, dass Cyber-Angriffe bei Weitem keine Ausnahmeerscheinung sind:

- Etwa alle zwei Sekunden erscheint ein neues Schadprogramm oder eine neue Variante.
- Pro Minute werden etwa zwei digitale Identitäten in Deutschland gestohlen.
- Pro Tag werden etwa vier bis fünf gezielte Trojaner-E-Mails im Regierungsnetz detektiert.
- Pro Monat werden etwa 40.000 Zugriffsversuche aus dem Regierungsnetz auf schädliche Webseiten blockiert.

Die Analysen des BSI zeigen, dass Cyber-Angriffe in vielen Fällen von hochprofessionellen Tätern mit ausreichenden Ressourcen durchgeführt werden. Die Angreifer verwenden dabei vielfältige, teilweise sehr ausgefeilte Methoden und attackieren unterschiedlichste Ziele.

Studien zeigen, dass durch Cyber-Angriffe enorme Schäden entstehen. Im *Norton Cybercrime Report 2011* kommt die Firma Symantec beispielsweise zu dem Ergebnis, dass in einem Jahr in Deutschland ein direkter finanzieller Schaden von über 16 Milliarden Euro durch Internet-Kriminalität entstanden ist. Die Studie *The Cost of Cyber Crime* von Detica für das Cabinet Office aus dem Jahr 2011 nennt für das Vereinigte Königreich (UK) einen Betrag von 27 Milliarden Pfund.

Was kann man tun, um sich vor Cyber-Angriffen zu schützen?

Zwar gibt es keinen absoluten Schutz, jedoch können Cyber-Angriffe durch geeignete Maßnahmen deutlich erschwert und in ihren Auswirkungen abgeschwächt werden. Neben den präventiven Maßnahmen kommt es dabei auch auf das möglichst frühe Erkennen und auf das professionelle Reagieren im Falle eines Cyber-Angriffs an.

Das BSI hat auf seinen Webseiten eine Vielzahl an Hinweisen und Empfehlungen veröffentlicht. Diese Publikationen werden regelmäßig ergänzt und aktualisiert:

- BSI-Analysen und BSI-Empfehlungen zur Cyber-Sicherheit (https://www.bsi.bund.de/cyber-sicherheit): Auf diesen Themenseiten bietet das BSI Informationen, Hilfestellungen und Aktivitäten zur Cyber-Sicherheit für professionelle Anwender an und informiert über Aktionen und Kooperationen in diesem Bereich.
- IT-Grundschutz (https://www.bsi.bund.de/grundschutz): IT-Grundschutz bietet eine einfache Methode, dem Stand der Technik entsprechende Sicherheitsmaßnahmen zu identifizieren und umzusetzen.

Das BSI empfiehlt allen Unternehmen, Behörden und anderen Institutionen, die Informationsangebote zum Thema *Cyber-Sicherheit* zu nutzen und die notwendigen Maßnahmen für einen angemessenen Schutz vor Cyber-Angriffen zu realisieren.

Wie kann ich mit dem BSI in Kontakt treten?

Bei Fragen zu Kooperationen, Themen und Inhalten rund um die Cyber-Sicherheit wenden Sie sich bitte an:

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
E-Mail: cs-info@bsi.bund.de

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **cs-info@bsi.bund.de** gesendet werden.

Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IM UNTERNEHMEN

Basismaßnahmen der Cyber-Sicherheit

Die Absicherung von Netzen und IT-Systemen in Unternehmen, Behörden und anderen Organisationen stellt angesichts der hochdynamischen Entwicklung der Bedrohungslage im Cyber-Raum eine komplexe und immer wieder neu herausfordernde Aufgabe dar.

Um den zahlreichen aus Perspektive der Cyber-Sicherheit entstehenden Anforderungen gerecht zu werden, bieten nationale und internationale Standards, Leitfäden und Handlungsempfehlungen den Verantwortlichen für IT-Planung und -Betrieb mögliche Vorgehensweisen an. Autoren und Herausgeber sind dabei sowohl staatliche Stellen, Hersteller und Sicherheitsdienstleister als auch die akademische Forschung.

Eine Herausforderung besteht jedoch darin, aus der Vielzahl verfügbarer Quellen die entscheidenden Antworten auf Schlüsselfragen der Cyber-Sicherheit zu identifizieren und daraus abgeleitete Maßnahmen wirksam umzusetzen.

Ziel

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) richtet sich mit einer großen Bandbreite von Veröffentlichungen an IT-Verantwortliche in öffentlicher Verwaltung und Wirtschaft, um sie bei der wirksamen Absicherung ihrer Netze und IT-Systeme zu unterstützen. Mit den hier vorliegenden konkreten und pragmatischen Basismaßnahmen sollen besonders wichtige Einzelthemen in einer übersichtlichen Darstellung zusammengefasst werden, mit denen die kritischsten Handlungsfelder der Cyber-Sicherheit in großen Behörden, Unternehmen und anderen Organisationen charakterisiert werden können. Voraussetzung für die Identifikation dieser Handlungsfelder ist eine möglichst präzise Kenntnis der eigenen Betroffenheit. Hier bietet die separat erhältliche BSI-Empfehlung zur Feststellung der Cyber-Sicherheits-Exposition ein einfach umsetzbares Vorgehen an.

Mit Hilfe der *Cyber-Sicherheits-Exposition* soll das Management unterstützt werden, die reale Betroffenheit herauszuarbeiten, den Schutzbedarf festzustellen und darauf aufbauend das anzustrebende Cyber-Sicherheitsniveau zu definieren. Dabei unterscheidet die *Cyber-Sicherheits-Exposition* zwischen Bedrohungen der Vertraulichkeit, Verfügbarkeit und Integrität und bildet damit die klassischen Schutzziele der Informationssicherheit differenziert ab.

Anhand der Management-Entscheidung ist es dann Aufgabe der Verantwortlichen für IT und IT-Sicherheit (CIO und CISO), Art und Umfang sinnvoller und angemessener Maßnahmen abzuleiten und umzusetzen. Dazu liefern die *Basismaßnahmen der Cyber-Sicherheit* pragmatische Handlungsempfehlungen, deren Beachtung die Grundlagen für robuste Netze und resistente IT-Systeme legt. So werden die Voraussetzungen für eine wirksame Abwehr von Angriffen über das Internet geschaffen.

Mit diesem Vorgehen soll sichergestellt werden, dass angesichts der vielen notwendigen Detailmaßnahmen die wesentlichen Basismaßnahmen der Cyber-Sicherheit stets im Blick behalten werden.

Basismaßnahmen zur Cyber-Sicherheit

Die Bestimmung der *Cyber-Sicherheits-Exposition* der zu schützenden Infrastruktur bildet die Voraussetzung für die Planung und Umsetzung angemessener Maßnahmen und ihre anschließende Bewertung auf Notwendigkeit, Angemessenheit und Wirtschaftlichkeit. Mithilfe der im Folgenden dargestellten Basismaßnahmen der Cyber-Sicherheit sollen die Verantwortlichen für IT-Planung und -Betrieb in die Lage versetzt werden, orientiert an der zuvor bestimmten *Cyber-Sicherheits-Exposition* ein angemessenes Cyber-Sicherheits-Niveau zu realisieren.

Absicherung von Netzübergängen

Die Absicherung von Netzübergängen ist einer der entscheidenden Faktoren für eine wirksame Abwehr von Angriffen aus dem Internet. Auf Grundlage der Netzstrukturaufnahme müssen Abwehrmaßnahmen für alle Netzübergänge sowie die entsprechenden Prozesse (wie z. B. ein Change Management) geplant und umgesetzt werden.

Identifikation aller Netzübergänge

Abwehrmaßnahmen in den Netzen bilden bereits ab einer **normalen** *Cyber-Sicherheits-Exposition* einen entscheidenden Faktor zum Schutz vor Angriffen. Wichtig ist dabei die Aufteilung des Netzes in verschiedene Segmente, die sowohl gegeneinander als auch bei der Anbindung an das Internet abgesichert werden müssen.

Dazu sind alle Netzübergänge des Unternehmens oder der Behörde im Rahmen einer *Netzstrukturaufnahme* sowohl im Hinblick auf ihre Anzahl als auch auf die spezifische Art des Übergangs zu identifizieren und zu dokumentieren. Kritisch sind hierbei insbesondere Lösungen, die Schutzmaßnahmen der allgemeinen Netzinfrastruktur umgehen können, etwa:

- individuelle DSL-Zugänge
- UMTS-Datenverbindungen mobiler Geräte
- verschlüsselte Kommunikationswege wie z. B. von IT-Nutzern selbst eingerichtete und genutzte VPN-Verbindungen

Von besonders kritischer Bedeutung sind Zugänge zu Netzen und IT-Systemen für Administratoren, vor allem solche Zugänge, die auch eine Fernwartung/Fernadministration erlauben.

Darüber hinaus sind auch Netzübergänge zwischen verschiedenen Liegenschaften und Anbindungen von Produktivsystemen zu erfassen.

Segmentierung des Netzes und Minimierung der Übergänge

Voraussetzung für eine in der Praxis umsetzbare und im Betrieb beherrschbare Lösung ist eine am Schutzbedarf unterschiedlicher Bereiche orientierte Netzsegmentierung (z. B. mittels physikalischer Trennung oder VLAN) sowie eine weitgehende Minimierung der externen Netzübergänge. Praxisbeispiele zeigen, dass große Unternehmensnetze mit nur zwei redundanten externen Netzübergängen betrieben werden können.

Eine Umgehung dieser minimierten Zahl an Netzübergängen, z. B. durch parallel betriebene DSL- oder UMTS-Zugänge, muss technisch und organisatorisch unterbunden werden.

Sicherheitsgateways

Die minimierte Zahl an Netzübergängen muss mit einem geeigneten Sicherheitsgateway abgesichert werden, das mindestens über folgende Eigenschaften verfügt:

- Application Level Gateway bzw. Proxy Firewall
- Intrusion Detection (ab einer **hohen** *Cyber-Sicherheits-Exposition* in Bezug auf *Vertraulichkeit* oder *Integrität*)
- Intrusion Prevention (ab einer **sehr hohen** *Cyber-Sicherheits-Exposition* in Bezug auf *Vertraulichkeit* oder *Integrität*)
- Überprüfung von Datenströmen wie E-Mail, HTTP und FTP auf Schadprogramme
- Möglichkeit für Blacklist- und Whitelist-Lösungen, insbesondere beim Zugriff auf Webseiten

Schnittstellenkontrolle

Eine Umgehung des Sicherheitsgateways ist durch eine technische Schnittstellenkontrolle auf Client-Systemen, Servern oder weiteren IT-Systemen auszuschließen, um beispielsweise Angriffe über externe Speichermedien (z. B. USB-Speichermedien, Digitalkameras oder MP3-Player) abwehren zu können.

Absicherung mobiler Zugänge

Mobile IT-Systeme – wie Smartphones oder Laptops – unterliegen einem sehr hohen Verlust- und Diebstahlrisiko. Oftmals kann nicht ausgeschlossen werden, dass mobile IT-Systeme im authentisierten Zustand (d. h. mit angemeldetem Nutzer) abhandenkommen und für Angriffszwecke missbraucht werden.

Daher sind die Berechtigungen, mit denen sich Nutzer über ein mobiles IT-System im Netz bewegen können, auf das unbedingt erforderliche Mindestmaß zu beschränken. Berechtigungen auf Dateiservern und Datenbanken sollten immer nur für die tatsächlich benötigte Zeitspanne und eingeschränkt auf den von außerhalb des Unternehmens oder der Behörde benötigten Bereich gewährt werden.

Verlustfälle mobiler IT-Systeme müssen im Vorfeld eingeplant werden. Reaktive Maßnahmen müssen geübt und im Ernstfall schnell umgesetzt werden, auch außerhalb üblicher Arbeitszeiten. Dazu gehören insbesondere die Löschung des mobilen IT-Systems aus der Ferne, die Sperrung des Zugangs zu den eigenen Netzen für das mobile System und die Einleitung von Lokalisierungsmaßnahmen, um Informationen zum möglichen Verbleib des Geräts erlangen zu können.

Abwehr von Schadprogrammen

Die gestaffelte Verteidigung von Angriffen unter dem Einsatz von Schadprogrammen (Viren, Würmer und Trojanische Pferde) muss über eine große Zahl von Systemen verteilt werden. Der eigentliche Client als Arbeitsplatzsystem ist dabei die letzte Verteidigungslinie.

Insbesondere sind Schutzprogramme gegen Schadsoftware auf folgenden Systemen durchgängig einzusetzen:

- Sicherheitsgateway
- E-Mail-Server
- Dateiserver
- mobile und stationäre Arbeitsplatzsysteme

Bei der Auswahl von Schutzprogrammen sollte ab einer **hohen** *Cyber-Sicherheits-Exposition* in Bezug auf *Vertraulichkeit* oder *Integrität* darauf geachtet werden, dass mehrere Lösungen unterschiedlicher Anbieter eingesetzt werden. Verteilt über die verschiedenen Systeme sollten mindestens drei unterschiedliche Lösungen eingesetzt werden. Entscheidend für die Erreichung einer ausreichenden Schutzwirkung ist dabei, dass diese unterschiedlichen Lösungen in der Praxis auf verschiedene Virensignatur-Datenbanken zurückgreifen. Nutzen mehrere Lösungen die gleiche Virensignaturdatenbank, wird keine erhöhte Schutzwirkung durch den Einsatz verschiedener Produkte entfaltet.

Auf dem Sicherheitsgateway sollten ab einer **hohen** *Cyber-Sicherheits-Exposition* in Bezug auf *Vertraulichkeit* oder *Integrität* verschiedene Lösungen parallel betrieben werden.

Darüber hinaus hat es sich als wertvoll erwiesen, die Installation und ggf. Ausführung von nichtautorisierter Software mit technischen Mitteln zu unterbinden.

Es sollte dauerhaft überprüft werden, ob die eigenen Systeme (z. B. unter Angabe der autonomen Systeme, deren Bestandteil die eigenen IP-Netze sind) in externen Datenbanken (z. B. google.com/webmasters) als gefährlich gekennzeichnet werden. Die Prüfung nach außen angebotener Dienste (insbesondere von Webservern) auf Verteilung von Schadsoftware kann zusätzlich mithilfe eines regelmäßigen Abrufs durch einen automatisierten Crawler und eine anschließende Analyse der heruntergeladenen Inhalte erfolgen.

Inventarisierung der IT-Systeme

Zur Planung und anschließenden Umsetzung von Abwehrmaßnahmen auf den eingesetzten IT-Systemen ist zunächst eine vollständige Inventarisierung der eingesetzten IT-Systeme notwendig. Mithilfe dieses Inventarverzeichnisses ist insbesondere zu klären, welche verschiedenen Systemtypen in der Organisation im Einsatz sind.

Leitfragen für die Inventarisierung sind:

- Welche Betriebssysteme und Anwendungen werden auf Servern eingesetzt?
- Welche Betriebssysteme und Anwendungen werden auf stationären und mobilen Clients eingesetzt?
- In welchen Versionen werden die eingesetzten Betriebssysteme und Anwendungen betrieben?
- Welche Patchstände haben die eingesetzten Betriebssysteme und Anwendungen?
- Welche Server werden mit welchem Funktionsumfang, d. h. in welchen Rollen betrieben (Mail-Server, File-Server, Druck-Server, ...)?
- Welche Systeme sind von außerhalb der Organisation über welche Wege erreichbar?

Anhand der Inventarisierung sollte auch die Frage geklärt werden, ob die erhobene Vielfalt an Systemen sicherheitstechnisch und administrativ beherrschbar ist.

Vermeidung von offenen Sicherheitslücken

Patchmanagement

Der überwiegende Teil von Angriffen gegen IT-Systeme erfolgt über Schwachstellen in eingesetzten Softwareprodukten, die in aktuelleren Versionen bereits durch die Hersteller geschlossen wurden. Mit vergleichsweise geringem Aufwand kann daher eine besonders große Schutzwirkung durch ein effizientes Patchmanagement erzielt werden. Aktualisierungen der eingesetzten Software müssen stets kurzfristig installiert werden.

Stärkere Abwehrmechanismen in aktuellerer Software

Darüber hinaus entwickeln die Hersteller Schutzmaßnahmen in ihren Produkten stetig weiter. Um von erweiterten Schutzmaßnahmen neuerer Produkte zu profitieren, sollte sich die IT-Planung an die (oftmals kurzen) Veröffentlichungszyklen neuer Produktversionen anpassen.

Beispiele für diese notwendige Anpassung sind:

- Microsoft versorgt Windows XP derzeit noch mit Sicherheitsaktualisierungen, gleichwohl sind die grundsätzlichen Schutzmechanismen von Windows 7 erheblich stärker. Die IT-Planung sollte daher z. B. bei Windows-Betriebssystemen den Veröffentlichungszyklus von Microsoft berücksichtigen und auf die Migration neuer Betriebssystemversionen vorbereitet sein. Gleiches gilt für den Adobe Reader, der in der Version 9 noch vom Hersteller gepflegt wird, allerdings nicht über die robusten Abwehrmechanismen der aktuellen Version 10 (Adobe Reader X) verfügt. Auch hier sollte immer die neueste Version des Produkts eingesetzt werden, auch dann, wenn Adobe noch ältere Versionen mit Sicherheitsaktualisierungen versorgt.

- Hochkritische Komponenten wie Internet-Browser müssen praktisch permanent auf den neuesten Stand gebracht werden, sodass hier der Ansatz einer „Migrationsplanung“ bereits zu kurz greift. Die eigenen Geschäftsabläufe müssen vielmehr stets mit der neuesten Version des eingesetzten Browsers funktionieren, ein Browser sollte dabei mindestens alle sechs Wochen aktualisiert werden. Statt einer Migration auf neue Versionen zu wenigen definierten Zeitpunkten muss in diesem Fall eine laufende Aktualisierung erfolgen.

Workarounds und Sicherheitsaktualisierungen

Workarounds müssen bei vorhandenen Sicherheitslücken bis zur Verfügbarkeit einer Aktualisierung für ein betroffenes Produkt auf ihre Wirksamkeit in der eigenen Infrastruktur getestet und umgesetzt werden. Bereitgestellte Sicherheitsaktualisierungen müssen anschließend kurzfristig installiert werden. Ab einer **hohen** *Cyber-Sicherheits-Exposition* in Bezug auf *Vertraulichkeit, Verfügbarkeit* oder *Integrität* ist eine Reaktion auf die Veröffentlichung von Workarounds oder Sicherheitsempfehlungen innerhalb von 72 Stunden unbedingt erforderlich.

Sichere Interaktion mit dem Internet

Alle Vorgänge, bei denen Daten und Dienste aus dem Internet abgefragt und verarbeitet werden, sind mit geeigneten Maßnahmen abzusichern. Die jeweilige Stärke der eingesetzten Schutzmechanismen muss dem Schutzbedarf der auf dem jeweiligen IT-System verarbeiteten Daten sowie den einem Angreifer zur Verfügung stehenden möglichen Weiterleitungsmechanismen gerecht werden. Dabei ist insbesondere in Betracht zu ziehen, dass ein zu schützendes System dem Angreifer ggf. nur als Zwischenstation für einen darüber hinaus gehenden Angriff gegen vollkommen andere Ziele im selben Netzsegment dient.

Sichere Browser

Eine der aus Sicherheitssicht kritischsten Komponenten auf einem IT-System bildet der Internet-Browser. Daher sollte ein besonderes Augenmerk auf dessen Absicherung gelegt werden. Bei Bedarf empfiehlt sich der Einsatz von umgebenden Schutzmechanismen.

In jedem Fall sollte der Browser bereits im Hinblick auf den Speicherschutz seiner eigenen und der von ihm geladenen Komponenten sowie auf die Abschottung besonders gefährdeter Codestellen durch eine Sandbox über starke Sicherheitseigenschaften verfügen.

Ab einer **hohen** *Cyber-Sicherheits-Exposition* in Bezug auf *Vertraulichkeit* oder *Integrität* sollte der Browser zusätzlich durch eine schützende Umgebung gegen Angriffe aus dem Internet abgeschirmt werden, z. B. durch die Minimierung von Ausführungsrechten oder mithilfe des Einsatzes von Virtualisierungssoftware. Eine Anwendungsvirtualisierung kann nahezu nahtlos in die Betriebssystemumgebung integriert werden.

Für den VS-Bereich zugelassene Lösungen wie die SINA Virtual Workstation bieten sehr starke Absicherungsmechanismen, wenn für die Interaktion mit dem Internet der Browser in eine von den kritischen Daten abgeschottete Sitzung ausgelagert wird. Derartige Lösungen sind ab einer **sehr hohen** *Cyber-Sicherheits-Exposition* in Bezug auf *Vertraulichkeit* angeraten.

Sichere E-Mail-Anwendungen

Im Vergleich zu Browsern können E-Mail-Anwendungen oftmals nicht ähnlich streng von kritischen Daten getrennt werden, da über sie u. a. kritische Daten ausgetauscht werden müssen. Zur Realisierung dieses Austauschs müssen die kritischen Daten aus einer sicheren Dateiablage in die E-Mail-Anwendung überführt werden, damit sie von dort weiter versandt werden können. Daher muss die E-Mail-Anwendung über einen Zugriff auf solche kritischen Daten verfügen und kann nicht vollständig abgeschottet werden.

Die Abwehr von Angriffen über E-Mails und insbesondere E-Mail-Anhänge erfordert eine zentrale Untersuchung des eingehenden E-Mail-Verkehrs auf Schadprogramme. Hier kann auch auf externe Dienstleister zurückgegriffen werden. Im Falle von Bundesbehörden in den Regierungsnetzen übernimmt das BSI dies

als gesetzliche Aufgabe und zentrale Dienstleistung. Bei einer **hohen** oder **sehr hohen** *Cyber-Sicherheits-Exposition* in Bezug auf *Verfügbarkeit* von E-Mail ist eine zentrale Filterung von Spam-Nachrichten einzurichten, die sich dynamisch an neue Spam-Wellen anpasst.

Ab einer **hohen** *Cyber-Sicherheits-Exposition* in Bezug auf *Vertraulichkeit* oder *Integrität* kann neben der Ende-zu-Ende-Verschlüsselung ebenfalls auf externe Dienstleistungen zurückgegriffen werden, die – wie z. B. DE-Mail – Vertraulichkeit und Verbindlichkeit gewährleisten können. Innerhalb eines Unternehmens oder einer Behörde können zentrale Lösungen wie die virtuelle Poststelle eingesetzt werden.

Schließlich kann zur Reduzierung der Angriffsfläche ggf. auch auf eine dedizierte clientseitige E-Mail-Software verzichtet werden und vielmehr eine Webmail-Umgebung im Browser genutzt werden. In solchen Fällen greifen auch für die Darstellung und das Bearbeiten von E-Mails die Schutzmechanismen des Browsers.

Sichere Darstellung von Dokumenten

So gut wie alle Arbeitsabläufe in Unternehmen und Behörden erfordern eine Darstellung und Bearbeitung von Dokumenten. Für die Darstellung von Dokumenten aus externen Quellen, insbesondere von solchen, die per E-Mail von Personen außerhalb der eigenen Organisation oder als Download aus dem Internet auf dem lokalen System gespeichert worden sind, sollte eine sichere Darstellungsoption verwendet werden. Beispiele sind die „Geschützte Ansicht“ in Microsoft Office 2010 oder der „Geschützte Modus“ im Adobe Reader X. Darüber hinaus können die Darstellungskomponenten durch Applikationsvirtualisierung noch stärker abgesichert werden.

Logdatenerfassung und -auswertung

Oftmals bleiben Sicherheitsvorfälle unerkannt, weil kurzfristig kein sichtbarer oder offensichtlicher Schaden eintritt. Mithilfe eines gut getarnten und hinreichend vorsichtigen Vorgehens ist es Angreifern aber u.U. möglich, über längere Zeiträume die Kontrolle über Zielsysteme zu übernehmen, ohne dass diese Angriffe unmittelbar aufgrund singulärer Ereignisse detektiert werden. Daher ist es notwendig, ebenfalls Verfahren zur Aufdeckung von nicht offensichtlichen Sicherheitsvorfällen und langfristig angelegten Angriffen zu entwickeln.

Eine zentrale Rolle spielt hierbei die regelmäßige Auswertung von Logdaten. Dazu ist bei der IT-Planung ein Konzept zu entwickeln, welche Logdaten auf welchen Systemen erfasst werden müssen, um Angriffe erkennen zu können. Wichtige Quellen für Logdaten sind in jedem Fall das Sicherheitsgateway und die eingesetzten Betriebssysteme.

Insbesondere die auf Intrusion Detection Systemen (IDS) anfallenden Daten sind ab einer **hohen** *Cyber-Sicherheits-Exposition* in Bezug auf *Vertraulichkeit* oder *Integrität* bei der regelmäßigen Auswertung mit einzubeziehen. Der Einsatz von Lösungen zum Security Information and Event Management (SIEM) ist vorzusehen.

Weitere wichtige Hinweise auf Angriffsversuche liefern Informationen zu anormalen Verhaltensmustern von IT-Systemen, vor allem Daten in Zusammenhang mit Systemabstürzen. Entwickler von Schadsoftware sind in der Regel nicht in der Lage, diese vollkommen zuverlässig auf allen Zielsystemen zur Ausführung zu bringen. Immer wieder kommt es daher in der Praxis zu Systemabstürzen, deren Logdaten ab einer **hohen** *Cyber-Sicherheits-Exposition* in Bezug auf *Vertraulichkeit* oder *Integrität* zentral erfasst und auf Hinweise zu Angriffsmustern und Anomalien ausgewertet werden sollten.

Sicherstellung eines aktuellen Informationsstands

Die Fähigkeit zur Planung wirksamer Cyber-Sicherheits-Maßnahmen wird im Wesentlichen durch die Qualität und den Umfang des eigenen Informationsstands bestimmt. Daher muss die Versorgung mit aktuellen und fachlich verlässlichen Informationen zur Cyber-Sicherheit sichergestellt werden.

Grundlegend wichtige Informationsquellen sind:

- Warn- und Informationsmeldungen eines etablierten CERT
- Warn- und Informationsmeldungen zu industriellen Steuerungsanlagen (Industrial Control Systems CERT, ICS-CERT)
- Lagebilder von staatlichen Stellen, Herstellern und Sicherheitsdienstleistern
- Warnungen und Sicherheitsempfehlungen von zuständigen Sicherheitsgruppen der jeweiligen Hersteller innerhalb des Unternehmens oder der Behörde eingesetzter Informationstechnik, z. B. des Microsoft Security Response Centers oder des Adobe Product Security and Incident Response Teams

Diese Quellen müssen täglich ausgewertet werden. Kritische Informationen müssen unmittelbar zu Reaktionen führen.

Bewältigung von Sicherheitsvorfällen

Vorbereitung auf Sicherheitsvorfälle

Die Bewältigung von Sicherheitsvorfällen sollte geübt werden, um die Geschäftsabläufe auch unter den erschwerten Bedingungen eines Sicherheitsvorfalls aufrecht erhalten oder zumindest schnell wiederherstellen zu können. Maßnahmen zur Eingrenzung des Schadens müssen bei der IT-Planung konzipiert werden, im Ernstfall schnell umsetzbar sein und eben daher immer wieder geübt werden.

Eine der wichtigsten Maßnahmen dabei ist eine regelmäßige Erstellung von Backups, die im Ernstfall auch tatsächlich wieder zurückgespielt werden können.

Meldung von Sicherheitsvorfällen

Neben der Bewältigung des eigenen Schadens besteht bei vorsätzlichen Handlungen die Möglichkeit, Strafanzeige zu erstatten, um weitere Vorfälle in anderen Organisationen zu vermeiden und den Polizeibehörden weitergehende Ermittlungen zu ermöglichen.

Darüber hinaus kann sowohl bei vorsätzlichen Handlungen als auch bei gravierenden technischen Problemen (zumindest anonym) eine Meldung an das BSI erfolgen, damit die Informationen zu dem gemeldeten Vorfall in das allgemeine Lagebild einfließen und übergreifende Zusammenhänge erkannt werden können. Nur so kann großflächigen IT-Schadensereignissen koordiniert begegnet werden.

Sichere Authentisierung

Zweifaktor-Authentisierung

Im Rahmen der Authentisierung, für die eine Nutzung eines sicheren Verzeichnisdienstes vorausgesetzt wird, sollte ab einer **hohen** *Cyber-Sicherheits-Exposition* in Bezug auf *Vertraulichkeit* oder *Integrität* ein Zweifaktor-Mechanismus verwendet werden. Eine Authentisierung allein mit Nutzername und Passwort ist nicht ausreichend. Schadprogramme wie Trojanische Pferde oder Keylogger greifen unmittelbar die Passwörter ab, sodass auch komplexe Passwörter oder ein häufiger Passwortwechsel keinen hinreichenden Schutz bieten. Wirksam abgewehrt werden solche Angriffe erst mittels eines zweiten, außerhalb des Systems liegenden Faktors wie z. B. eines Hardware-Tokens.

Trennung von Authentisierungsdaten für verschiedene Aufgaben

Weiterhin sind Bereiche unterschiedlichen Schutzbedarfs zu identifizieren, die in der Folge unterschiedliche Authentisierungen erfordern. Dabei ist besonders auf eine Trennung der Konten von Administratoren und anderen Nutzern zu achten. Unterschiedliche Rollen erfordern verschiedene Authentisierungsdaten. Ergänzend zu der unter *Durchführung nutzerorientierter Maßnahmen* beschriebenen Rollentrennung auch dann, wenn die Rollen von ein und derselben Person wahrgenommen werden. Darüber hinaus dürfen keine gemeinsam genutzten Funktionskonten zur Authentisierung verwendet werden. Die Autorisierung für ein Funktionskonto erfolgt durch die Authentisierung mit einem personenbezogenen Konto.

Die Trennung unterschiedlicher Authentisierungsbereiche ist besonders kritisch in Bezug auf Produktivdatenbanken. Die Authentisierung gegenüber einer Datenbank muss mit der übrigen Authentisierungsstruktur abgestimmt sein. Weder dürfen allgemeine Authentisierungskonzepte durch einen direkten Zugriff auf eine Datenbank umgangen werden können, noch darf die Datenbank selbst ungeschützt bleiben. Native Authentisierungsmechanismen von Datenbanken müssen genutzt werden. Ihre Absicherung darf nicht allein durch die Umgebung erfolgen.

Gewährleistung der Verfügbarkeit notwendiger Ressourcen

Bereitstellung ausreichender eigener Ressourcen

Die wirksame Abwehr von Bedrohungen der Cyber-Sicherheit erfordert die Bereitstellung ausreichender Ressourcen. Diese Aufwände müssen von Unternehmen und Behörden in jeder Phase der IT-Planung und dem anschließenden IT-Betrieb hinreichend berücksichtigt und entsprechende finanzielle und personelle Mittel bereitgestellt werden.

Einbindung externer Dienstleister

Ein umfassender Schutz ist in der Regel nur durch Einbindung verschiedener externer Dienstleister umsetzbar. Wesentliche Bereiche, in denen auf externen Sachverstand zurückgegriffen werden sollte, sind:

- Durchführung einer herstellerneutralen Cyber-Sicherheitsberatung
- Penetrationstests gegen die eigene IT
- regelmäßige Cyber-Audits
  - Cyber-Quickcheck
  - automatisierte Schwachstellen-Überprüfungen
  - Grundschutz-Audit
- Informationssicherheits-Revisionen
- Analyse und Bewältigung von Sicherheitsvorfällen durch ein externes Computer Emergency Response Team (CERT), sowohl in simulierten Übungsszenarien als auch im Ernstfall
- Durchführung forensischer Maßnahmen

Die Gewichtung und Priorisierung dieser Bereiche sollte auf Grundlage der zuvor bestimmten *Cyber-Sicherheits-Exposition* erfolgen.

Gerade Ressourcen, die erst bei unvorhergesehenen Sicherheitsvorfällen benötigt werden, sollten rechtzeitig eingeplant werden. Bereits lange vor dem tatsächlichen Vorfall muss feststehen, auf welchen externen Dienstleister im Ernstfall verlässlich und kurzfristig zurückgegriffen werden kann.

Durchführung nutzerorientierter Maßnahmen

Sensibilisierung und Schulung

Auch das eigene Personal muss in den Mittelpunkt einer Cyber-Sicherheitsstrategie gerückt werden. Sämtliche technischen Vorkehrungen können durch menschliche Fehler oder bewusste Fehlhandlungen unwirksam werden.

Daher ist das Personal - vom Nutzer der Informationstechnik bis hin zum Administrator, von der Arbeitsebene bis hin zur Leitungsebene, umfassend zu sensibilisieren. Dies gilt auch für die Mitarbeiter von externen Dienstleistern, die in der Organisation eingesetzt werden. Die Sensibilisierung muss sowohl gezielte Schulungen als auch regelmäßige Kurzinformationen zu aktuellen Themen und zur Auffrischungen des notwendigen Wissens während des normalen Arbeitsalltags umfassen. Ein besonderes Augenmerk ist dabei auf Erhalt und Ausbau der Kompetenz von Administratoren zu legen.

Rollentrennung

Die Personalplanung muss zudem in Bezug auf die eingesetzte IT folgende Aspekte umfassen:

- Definition der technischen und organisatorischen Rollen
- Klärung von Verantwortlichkeiten eines jeden Einzelnen
- Festlegung von Zuständigkeiten (auch unter Einbeziehung externer Dienstleister)

Diese Planung soll eine klare Trennung von Rollen vorsehen. Eine Konzentration vieler oder aller Zuständigkeiten in einer Rolle sollte immer vermieden werden.

Sichere Nutzung Sozialer Netze

Neben den IT-Systemen, die unter der direkten Kontrolle des Unternehmens bzw. der Behörde stehen, gewinnen externe Dienste wie Soziale Netze eine zunehmende Bedeutung für bestimmte Geschäftsabläufe, insbesondere im Bereich des Marketings oder der Öffentlichkeitsarbeit.

Der sichere und damit auch seriöse Auftritt einer Organisation sowie die (beruflichen) Profile der Beschäftigten in Sozialen Netzen wie Facebook, Google+ und Xing ist daher in die IT-Planung einzubeziehen. Die Sensibilisierung von Mitarbeitern muss insbesondere das Verhalten in Sozialen Netzen in Form verbindlicher Vorgaben (Social Media Guidelines) und durch Aufklärungsmaßnahmen umfassen.

Sicherheitsmaßnahmen, die von den Betreibern der Sozialen Netze angeboten werden, müssen bekannt sein und so wirksam wie möglich genutzt werden. Dabei müssen gerade auch die Grenzen der IT-Sicherheit, die in Sozialen Netzen umsetzbar ist, stets allen Nutzern innerhalb der Organisation verdeutlicht werden. Existieren direkte Schnittstellen zwischen Sozialen Netzen und der organisationseigenen Infrastruktur, so sind diese Übergänge besonders abzusichern. Falls dies nicht möglich ist, sind diese Übergänge im Zweifel zu trennen.

Zusatzmaßnahmen bei höherer Cyber-Sicherheits-Exposition

Die Verfügbarkeit, Vertraulichkeit und Integrität von Informationstechnik bilden die klassischen Grundwerte für einen sicheren Betrieb. In Abhängigkeit des individuellen Schutzbedarfs eines Systems, Netzsegments oder der gesamten Organisation sind zur Gewährleistung dieser Grundwerte zusätzliche Maßnahmen erforderlich. Die Notwendigkeit folgt insbesondere aus der oben beschriebenen Feststellung der *Cyber-Sicherheits-Exposition*, sobald **hohe** oder **sehr hohe** Werte in Bezug auf *Vertraulichkeit, Verfügbarkeit* oder *Integrität* festgestellt werden.

Verfügbarkeit

Falls für die *Cyber-Sicherheits-Exposition* (*Verfügbarkeit)* ein Wert von **hoch** oder **sehr hoch** bestimmt wurde, muss die notwendige Verfügbarkeit von Informationstechnik primär durch Schaffung von Redundanzen erzielt werden. Dazu sind auf allen Ebenen Komponenten zu identifizieren, die für eine Aufrechterhaltung des Geschäftsbetriebs erforderlich sind. Diese Komponenten müssen orientiert an den jeweiligen Verfügbarkeitsanforderungen individuell hinreichend redundant ausgelegt werden. Konkret sind z. B. geschäftskritische Systeme mehrfach vorzuhalten, die Netzanbindung an das Internet muss über voneinander unabhängige Übergangsstellen erfolgen, zwischen denen nahtlos gewechselt werden kann. Ebenso muss es möglich sein, bei Ausfall des Providers den Internetzugang kurzfristig über einen alternativen Provider zu realisieren. Entsprechende Dienstleistungen müssen präventiv gebucht und deren Verfügbarkeit regelmäßig getestet werden.

Diese Redundanzanforderungen beinhalten auch die ständige Verfügbarkeit eines zweiten Internet Browsers, falls der üblicherweise genutzte Browser aufgrund von kritischen Sicherheitslücken zeitweise nicht genutzt werden kann. In solchen Fällen muss schnell auf ein alternatives Produkt gewechselt werden können, da die Nutzung eines Browsers, der über bekannte Sicherheitslücken über das Internet erfolgreich angegriffen werden kann, ausschließbar sein muss.

Zur Gewährleistung der Verfügbarkeit von nach außen angebotenen Diensten, insbesondere der Verfügbarkeit von Internetangeboten und E-Mail, sind Maßnahmen gegen Distributed-Denial-of-Service-Angriffe (DDoS) zu implementieren. Zur Abwehr solcher Angriffe kann auch auf externe Dienstleister zurückgegriffen werden. Im Rahmen der Prävention sind diese externen Dienstleistungen vorab einzukaufen. Sowohl interne als auch externe Maßnahmen sind regelmäßig zu üben.

Vertraulichkeit

Einer *Cyber-Sicherheits-Exposition (Vertraulichkeit)* mit einem Wert von **hoch** oder **sehr hoch** wird vor allem durch Einsatz kryptographischer Verfahren begegnet. Dies gilt sowohl für die Verschlüsslung von E-Mails und Dokumenten als auch für die Absicherung von Festplatten – vor allem in mobilen IT-Systemen. Hierfür sind Festplatten vollständig mit wirksamen kryptographischen Mitteln zu verschlüsseln.

Integrität

Neben den Primärzielen des Angreifers, die vor allem die Verfügbarkeit und Vertraulichkeit gefährden, kann es bei mehrstufigen und langfristig durchgeführten Angriffen auch um die Manipulation von Datenbeständen gehen, sodass die *Cyber-Sicherheits-Exposition* in Bezug auf die *Integrität* mit **hoch** oder **sehr hoch** zu bewerten ist. Dieser Bedrohung der Integrität ist frühzeitig durch integritätssichernde Maßnahmen, wie der kryptographischen Signatur zu begegnen.

Neben der Kommunikation ist jedoch auch die Integrität der IT-Systeme selbst eines der wichtigen Schutzziele. Dazu müssen sowohl während der Beschaffung als auch im Betrieb verschiedene technische und organisatorische Maßnahmen umgesetzt werden, z. B.

- der Einsatz von Trusted Boot oder Secure Boot
- IT-Revisionen
- bereits im Vorfeld des Betriebs ein auf Sicherheit ausgerichtetes Supply-Chain-Management

Durchführung von Penetrationstests

Ab der *Cyber-Sicherheits-Exposition* **hoch** ist die Durchführung regelmäßiger Penetrationstests angebracht. Diese sollten von Experten, die nicht an der Planung der IT beteiligt waren, durchgeführt werden. Aufwand und Intensität des Penetrationstests sind der Exposition anzupassen.

Unterstützende Maßnahmen zur Abwehr gezielter Angriffe

Die *Cyber-Sicherheits-Exposition* eines Unternehmens oder einer Behörde bildet ein gutes Maß für die Wahrscheinlichkeit, in das Zielspektrum von Angeifern zu geraten. Dabei sind solche Täterkreise von besonderer Relevanz, denen es nicht um ungerichtete Breitenangriffe gegen mehr oder minder wahllose Ziele geht, sondern die es vielmehr gezielt auf eine bewusst ausgewählte Organisation abgesehen haben. Die Abwehr solcher gezielter Angriffe gegen die Vertraulichkeit oder die Verfügbarkeit, deren Techniken von Angreifern auf die spezielle Situation der angegriffenen Organisation angepasst werden können, stellt eine der größten Herausforderungen der Cyber-Sicherheit dar.

Eine gestaffelte Verteidigung im koordinierten Zusammenspiel der hier aufgezeigten Maßnahmen ist in der Lage, auch gezielte Angriffe massiv zu erschweren.

Bei höherem Schutzbedarf, d. h. einer *Cyber-Sicherheits-Exposition (Vertraulichkeit* und/oder *Verfügbarkeit)* mit Werten von **hoch** oder **sehr hoch**, sollte darüber hinaus auch der Einsatz speziell gehärteter (auch alternativer) Betriebssysteme und Anwendungen in Betracht gezogen werden. Die Verwendung von Standardkonfigurationen im Bereich der Betriebssysteme und Anwendungen erleichtern gezielte Angriffe deutlich. Ziel muss es daher sein, die Vorhersagbarkeit von Plattformeigenschaften weitestgehend auszuschließen.

Wenn in der Risikoabschätzung deutlich wird, dass Schutzmechanismen an Netzübergängen nicht in der Lage sind, erwartete gezielte Angriffe abzuwehren, sind zudem Netze, in denen die zu schützenden Daten verarbeitet werden, vollständig von der Umgebung zu trennen.

Checkliste zu den Basismaßnahmen der Cyber-Sicherheit

Folgende Checkliste fasst die Umsetzung der Basismaßnahmen der Cyber-Sicherheit zusammen:

- ☐ Der Bedrohungsgrad der eigenen Infrastruktur sowie die Transparenz der Institution gegenüber Angreifern wurde bestimmt. Daraus wurde die *Cyber-Sicherheits-Exposition* abgeleitet.
- ☐ Sämtliche Netzübergänge sind identifiziert und hinreichend abgesichert.
- ☐ Die Infektion mit Schadprogrammen wird mit wirksamen Maßnahmen unterbunden.
- ☐ Die IT-Systeme wurden inventarisiert und auf ihre sicherheitstechnische Beherrschbarkeit hin geprüft.
- ☐ Offene Sicherheitslücken auf IT-Systeme werden vermieden.
- ☐ Eine Interaktion mit dem Internet findet nur über abgesicherte Komponenten statt.
- ☐ Logdaten werden zentral erfasst und ausgewertet.
- ☐ Die eigene Organisation wird mit allen notwendigen Informationen versorgt.
- ☐ Die Organisation ist auf die Bewältigung von Sicherheitsvorfällen vorbereitet.
- ☐ Die eingesetzten Mechanismen zur Authentisierung verhindern eine missbräuchliche Nutzung durch Dritte.
- ☐ Es stehen ausreichende interne Ressourcen zur Verfügung, externe Dienstleister werden eingebunden.
- ☐ Das eigene Personal wird in Fragen der Cyber-Sicherheit qualifiziert und sensibilisiert.
- ☐ Es werden nutzerorientierte Maßnahmen zur Rollentrennung durchgesetzt.
- ☐ Die Organisation und ihre Mitglieder bewegen sich sicher in Sozialen Netzen.
- ☐ Bei höherem Schutzbedarf werden Vertraulichkeit, Verfügbarkeit und Integrität durch wirksame Maßnahmen gewährleistet und Penetrationstests durchgeführt.
- ☐ Zur Abwehr gezielter Angriffe werden unterstützende Schutzmaßnahmen ergriffen.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an cs-info@bsi.bund.de gesendet werden.

Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IM UNTERNEHMEN

Sichere Nutzung von PCs unter Microsoft Windows 7

Empfehlungen für kleine Unternehmen und Selbstständige

1 Ausgangslage

Viele nützliche und wichtige Dienstleistungen wie Online-Banking, E-Commerce oder E-Government, werden heute über das Internet angeboten und genutzt. Auch in Zukunft wird sich die Anzahl der Online-Services noch weiter erhöhen. Hinzu kommt der verstärkte Einsatz mobiler Endgeräte, wie Smartphones und Tablets, mit denen diese Dienste auch unterwegs genutzt werden können. Im Geschäftsleben setzen viele Unternehmer und Selbständige dennoch weiterhin auf Personal Computer (PCs), die mit verschiedenen Betriebssystemen wie Microsoft Windows, Apple Mac OS X oder einer Linux-Variante ausgestattet sind.

2 Ziel

Die vorliegende BSI-Veröffentlichung zur Cyber-Sicherheit bietet Hilfestellungen für die weitestgehend sichere Konfiguration eines Windows-PCs zum Einsatz in kleinen Unternehmen. Diese Empfehlung behandelt das verbreitete Microsoft Windows 7.

Sinnvoll ist dabei zunächst die Betrachtung des Lebenszyklus eines Rechners:

- Entscheidungen vor der Installation
- Installation und erste Inbetriebnahme
- Regelmäßiger Betrieb
- Entsorgung des Systems

Mit wenigen Maßnahmen können PCs unter einem aktuellen Microsoft Windows 7 so abgesichert werden, dass eine weitgehend sichere Nutzung von Dienstleistungen über das Internet möglich ist.

3 Entscheidungen vor der Installation

Bereits bei der Anschaffung des Systems gibt es wichtige Aspekte, die Sie für einen späteren sicheren Betrieb eines PCs beachten sollten.

3.1 Hardware und Betriebssystem

Achten Sie auf die Verwendung möglichst aktueller Hardware. Um die von Windows bereitgestellten Sicherheitsmechanismen vollständig nutzen zu können, sollte der PC über eine 64-Bit-CPU (Prozessorarchitektur) verfügen und eine 64-Bit-Version des Betriebssystems eingesetzt werden.

3.2 Virenschutzprogramm

Für einen hinreichenden Schutz des Systems gegen Computer-Viren und andere Schadprogramme kommen verschiedene Varianten von Virenschutz-Software infrage. Diese unterscheiden sich in der Erkennungsleistung, Bedienungskomfort und Funktionsumfang, wie beispielsweise:

- zentralisiertes Management
- DNS-Schutzfilter
- Überwachung Ihrer Browser- und E-Mail-Aktivitäten auf Schadprogramme sowie
- erweiterte, verhaltensbasierte Erkennung von Schadsoftware

Sofern erforderlich, können Sie einige dieser zusätzlichen Funktionen auch mithilfe von kostenlosen Lösungen abdecken, z. B.:

- Browserfilter mit Phishing- und Malwareschutz in Google Chrome oder Mozilla Firefox bzw. mit dem SmartScreen-Filter des Microsoft Internet Explorer
- DNS-Schutzfilter mit OpenDNS Premium DNS (http://opendns.com/business-solutions/premium-dns/benefits, engl.).

Entscheiden Sie sich für ein Virenschutz-Programm, das in seinem Funktionsumfang Ihren Anforderungen entspricht und, basierend auf Ergebnissen unabhängiger Testinstitute, eine möglichst gute Erkennungsleistung aufweist. Betreiben Sie Ihr System nicht ohne aktuelles Virenschutzprogramm und beachten Sie unbedingt die regelmäßig notwendige Verlängerung der Lizenz (in der Regel nach 12 Monaten).

Der gleichzeitige Betrieb mehrerer Virenschutzlösungen auf einem System kann zu unvorhersehbaren Wechselwirkungen führen. Daher gilt: Haben Sie zu jedem Zeitpunkt immer nur ein Virenschutzprogramm installiert bzw. aktiviert!

Sofern das Virenschutzprogramm eine integrierte Firewall anbietet, sollte diese nicht aktiviert werden. Nach Einschätzung des BSI reicht die Windows-eigene Lösung im Normalfall aus (siehe Abschnitt Personal Firewall).

3.3 Backups

Um Sicherungskopien sowohl des Systems als auch Ihrer Daten zu erstellen, können Sie die in Windows 7 eingebaute Funktionalität verwenden (http://windows.microsoft.com/de-DE/windows7/products/features/backup-and-restore). Der Kauf einer gesonderten Backup-Software ist für Windows 7 im Allgemeinen nicht erforderlich. Im geschäftlichen Einsatz von Windows 7 ist gegebenenfalls zu prüfen, ob ein professionelles Sicherungssystem eingesetzt werden sollte, welches spezifische Anforderungen – beispielsweise an Revisionssicherheit, Reporting oder Disaster Recovery – gewährleisten kann.

3.4 Anwendungen

Prüfen Sie im Einzelfall, ob Sie wirklich jede installierte Anwendung zur Darstellung ihrer Dateien benötigen. Je weniger zusätzliche Anwendungen Sie nutzen, desto kleiner ist die Angriffsfläche des Systems.

Zur Darstellung von PDF-Dateien sollten Sie die jeweils aktuelle Version des kostenlosen Adobe Acrobat Readers (http://adobe.com/reader) nutzen, da diese über zusätzliche Sicherheitsmaßnahmen, wie eine „Sandbox“ (engl. übersetzt: „Sandkasten“, d. h. diese Software ist vom Rest des Systems abgeschirmt), verfügt.

Bei allen zusätzlichen Anwendungsprogrammen, die Sie etwa zur Bearbeitung von Fotos oder zum Komponieren und Abspielen von Musik nutzen, sollten Sie darauf achten, dass die Produkte mit einer Funktion zur automatischen Aktualisierung ausgestattet sind. In der Regel lässt sich dies unter dem Menüpunkt *Einstellungen* in der jeweiligen Software überprüfen und konfigurieren. Updates sollten idealerweise ohne Ihr Zutun automatisch im Hintergrund installiert werden. Verbreiteter sind Aktualisierungsfunktionen, die Sie bei verfügbaren Updates benachrichtigen. Die Installation sollten Sie stets zeitnah durchführen. Für die im Folgenden beispielhaft genannten Produkte aus dem Bereich Bürosoftware gibt es solche Aktualisierungsmechanismen, die standardmäßig nach der Installation bereits aktiviert sind:

- kostenlos: LibreOffice (http://www.libreoffice.org), OpenOffice (http://openoffice.org)
- kostenpflichtig: Microsoft Office (http://office.com)

4 Installation und erste Inbetriebnahme

Einen wichtigen Grundstein für die Systemsicherheit Ihres PCs können Sie bereits bei der Installation und ersten Inbetriebnahme des Rechners legen.

4.1 Installation aller vorhandenen Sicherheitsaktualisierungen

Üblicherweise ist Microsoft Windows 7 im Auslieferungszustand eines neu erworbenen PCs bereits vorinstalliert. Ist dies – etwa bei einem Gebrauchtgerät – nicht der Fall, so führen Sie zunächst eine vollständige Neuinstallation von Windows 7 durch.

Neben dem vorinstallierten Windows-Betriebssystem sind meist weitere Software-Produkte vorinstalliert. Diese sollten auf ihre Lizenzdauer, die unter Umständen zeitlich beschränkt ist, geprüft werden. Nicht benötigte Software-Produkte sollten deinstalliert werden.

Bei der ersten Inbetriebnahme eines Windows 7 Betriebssystems sollten Sie Ihren PC mit dem Internet verbinden und die von Microsoft angebotenen Software-Aktualisierungen herunterladen und installieren. Bei den Aktualisierungen von Microsoft über Windows-Update ist es dabei ausreichend die „wichtigen Updates“ zu installieren, um das Betriebssystem in einem geschützten Zustand zu halten. Das Häkchen bei „Empfohlene Updates auf die gleiche Weise wie wichtige Updates bereitstellen“ benötigen Sie hierfür nicht. Bitte achten Sie darauf, bei vorinstallierten PCs nicht nur Updates für Windows, sondern auch für andere möglicherweise installierte Microsoft-Produkte (z. B. Microsoft Office) herunterzuladen. Aktivieren Sie in diesem Zuge die Auto-Update-Funktion, sodass in Zukunft weitere Aktualisierungen automatisch heruntergeladen und installiert werden.

4.2 Benutzerkonten

Das bei der Installation von Windows 7 angelegte Benutzerkonto ist ein Administrator-Konto mit umfassenden Berechtigungen zur Systemkonfiguration. Achten Sie darauf, dass nur diejenigen Anwender Admin-Rechte erhalten, die diese Funktionalität auch benötigen und beherrschen. Legen Sie für die tägliche Verwendung des Windows-PCs auf jeden Fall zusätzlich ein Standard-Benutzerkonto an. Sollte der Windows-PC von mehreren Anwendern genutzt werden, sollten Sie für jeden Anwender ein eigenes Benutzerkonto anlegen.

Verwenden Sie neben dem Standard-Benutzerkonto, welches Sie für die tägliche Arbeit ver-

wenden, ein zusätzliches Benutzerkonto, um transaktionsbezogene Aktivitäten wie Online-Banking durchzuführen oder um kritische Daten online zu versenden.

4.3 Verschlüsselung der Festplatte

Falls Sie ein Notebook besitzen, das Sie auch unterwegs nutzen, sollten Sie unbedingt die Festplatte verschlüsseln, um Daten bei Verlust oder Diebstahl des Geräts zu schützen. Wenn Sie einen Desktop-PC besitzen, ist abzuwägen, ob ein möglicher Leistungsverlust Ihres Systems aufgrund der Verschlüsselung in einem angemessenen Verhältnis zum Schutz Ihrer Daten vor dem Zugriff unbefugter Dritter steht.

Das Betriebssystem Windows 7 verfügt in den Editionen *Ultimate* und *Enterprise* über die eingebaute Festplattenverschlüsselung *BitLocker Drive Encryption*, die eine Schlüsselverwaltung mithilfe eines TPM (Trusted Platform Module) durchführen kann. In diesem Fall wird der Kauf eines PCs mit TPM Version 1.2 empfohlen. Erstellen Sie nach der Festplattenverschlüsselung einen Wiederherstellungsschlüssel.

Wählen Sie hierfür ein sicheres Passwort, welches Sie sich gut einprägen können. Schreiben Sie sich dieses Passwort zusätzlich auf und bewahren Sie den Zettel räumlich getrennt von Ihrem PC an einem sicheren Ort auf. Hinweise zur Erstellung eines sicheren Passworts finden Sie bei auf der BSI-Webseite „BSI für Bürger[1]“.

Einen vergleichbaren Schutz können Sie durch die Verwendung der kostenfrei verfügbaren Lösung *VeraCrypt* (https://veracrypt.codeplex.com) erreichen. Erstellen Sie während des Verschlüsselungsvorgangs unbedingt eine „VeraCrypt Rescue Disk“. Diese hilft, wenn Probleme beim Entschlüsseln der Festplatte auftreten sollten.

4.4 Personal Firewall

Windows 7 besitzt eine integrierte Personal Firewall, die im Auslieferungszustand oder nach einer Neuinstallation bereits aktiviert ist. Achten Sie darauf, dass Sie diese Firewall in den Systemeinstellungen nicht versehentlich deaktivieren. Die Installation einer zusätzlichen Firewall ist nicht mehr erforderlich, da das System durch die von Windows 7 bereitgestellte Firewall hinreichend gegen Angriffe aus dem Netz geschützt wird.

4.5 Überprüfung auf Sicherheitsaktualisierungen

Um das Sicherheitsniveau des PCs konstant hoch zu halten, ist es erforderlich, alle Sicherheitsaktualisierungen nach deren Erscheinen zu installieren. Am einfachsten geschieht dies durch die Nutzung der sowohl im Betriebssystem (Microsoft-Update) als auch in den meisten gängigen Anwendungsprogrammen vorhandenen Auto-Update-Funktion.

4.6 Internet-Browser

Während der Installation bzw. der ersten Inbetriebnahme von Windows 7 werden Sie zur Auswahl eines Internet-Browsers aufgefordert.

Ihr Internet-Browser ist die zentrale Komponente für die Nutzung von Online-Angeboten im Internet und stellt somit eins der beliebtesten Ziele für Cyber-Angriffe dar. Verwenden Sie daher möglichst einen Browser mit Sandbox-Technologie. Konsequent umgesetzt wird dieser Schutz gegenwärtig z. B. von Google Chrome (https://www.google.com/chrome). Vergleichbare Mechanismen sind in anderen Browsern derzeit entweder schwächer implementiert oder noch nicht vorhanden.

1 https://www.bsi-fuer-buerger.de/Passwoerter

Vorteilhaft sind bei Google Chrome die kurzen Update-Intervalle sowie die Funktion zur automatischen Aktualisierung, die auch den integrierten Adobe Flash Player umfasst. Dadurch wird auch der Adobe Flash Player stets auf dem neuesten Stand gehalten. Wenn Sie ausschließlich Google Chrome verwenden, sollten Sie einen eventuell zusätzlich installierten Adobe Flash Player von Ihrem PC entfernen.

Eine weitverbreitete Angriffsform bildet der Versuch, Sie unter Vortäuschung falscher Tatsachen zum Download schädlicher Programme zu bewegen und diese in der Folge auf Ihrem PC auszuführen – diese Angriffstechnik wird auch als eine Form des „Social Engineering“ bezeichnet. Solche Angriffe, bei denen Sie bewusst einen Download starten, ohne sich eines Angriffs bewusst zu sein, versuchen die Browser-Hersteller mit Filtermechanismen abzuwehren. Mit Hilfe dieser Filter können auch viele sogenannte „Drive-by-Download“-Angriffe erfolgreich abgewehrt werden.

Um von diesem Schutz zu profitieren, sollten Sie bei Nutzung des Internet Explorers unbedingt den SmartScreen-Filter aktivieren. Eine vergleichbare Funktion steht auch im Mozilla Firefox und in Google Chrome mit dem Phishing- und Malwareschutz zur Verfügung. Alle drei Filter können jedoch aufgrund der hohen Dynamik neuer Webseiten mit schädlichen Inhalten allein keine Garantie gegen eine ungewollte Infektion mit Schadsoftware bieten.

4.7 E-Mail

Für die weitgehend sichere Nutzung von E-Mails ist es nicht erforderlich, zusätzliche Software zu installieren. E-Mail-Provider bieten Webmail-Zugänge an, die Sie über den Internet-Zugang mit Ihrem Browser nutzen können. Wichtig ist, auf eine verschlüsselte Verbindung (https) zum Webmail-Zugang zu achten, um von den Schutzmechanismen Ihres Browsers zu profitieren. Achten Sie darauf, dass die verschlüsselte Verbindung nicht nur für den Login-Vorgang, sondern während der gesamten Webmail-Nutzung aktiviert ist.

Falls Sie erweiterte Anforderungen an Komfort und Funktionalität bei der Arbeit mit E-Mails haben, sollten Sie einen modernen E-Mail-Client installieren und sicher konfigurieren.

Insbesondere ist dabei auf die Verwendung verschlüsselter Übertragungsprotokolle (POP3S, IMAPS, SMTPS) zu achten.

Verzichten Sie zudem auf die Darstellung und Erzeugung von E-Mails im HTML-Format. Die Anzeige externer Inhalte, wie Bilder in HTML-E-Mails, sollten Sie unbedingt deaktivieren, da über diese eine zusätzliche Möglichkeit zur Ausführung von Schadcode besteht.

4.8 Java-Laufzeitumgebung

Einige Anwendungen benötigen unter Umständen die Java-Laufzeitumgebung[2], die nicht in einer Standard-Installation von Windows 7 enthalten ist. Um die Angriffsfläche Ihres Systems zu reduzieren, sollten Sie Java nur dann installieren, wenn Ihre Anwendungsprogramme diese Laufzeitumgebung tatsächlich benötigen. Beim Start einer entsprechenden Anwendung wird im Normalfall auf das Fehlen von Java hingewiesen. Nach der Installation sollten Sie darauf achten, dass Java über die automatische Updatefunktion auf einem aktuellen Stand gehalten wird. Empfehlenswert ist die Änderung der Standardeinstellung auf eine tägliche Überprüfung.

Wenn Sie die Java-Laufzeitumgebung installieren müssen, schalten Sie trotzdem die Java-Unterstützung in den Einstellungen Ihres Webbrowsers ab. Sie können Java dann fallweise aktivieren, wenn es von einer vertrauenswürdigen Website benötigt wird. Alternativ können Sie das Dienstprogramm „Java-Einstellungen“ verwenden, um Java systemweit ein- und auszuschalten.

2 http://java.com/de

4.9 Erzeugung eines Datenträgers zur Systemreparatur

Die meisten neuen Systeme werden heute ohne Installationsmedien, wie beispielsweise Programm-CDs, ausgeliefert. Wenn dies bei Ihrem neuen PC der Fall ist, sollten Sie nach der ersten Inbetriebnahme einen Systemreparaturdatenträger („Rescue Disk“) erzeugen. Im Falle eines Defekts oder Absturzes können Sie mit diesem Ihr Windows 7-Betriebssystem wiederherstellen. Näheres dazu kann unter
http://windows.microsoft.com/de-DE/windows7/Create-a-system-repair-disc nachgelesen werden.

5 Regelmäßiger Betrieb

Beachten Sie im täglichen Umgang mit Ihrem PC die folgenden Ratschläge für einen sicheren Betrieb:

5.1 Sicherheitsaktualisierungen

Wenn Sie während der Installation eingestellt haben, dass sowohl das Betriebssystem als auch alle installierten Anwendungen automatische Updates durchführen, dann achten Sie auf entsprechende Hinweise im laufenden Betrieb.

In manchen Fällen werden Sie aufgefordert, die Installation von Updates zu bestätigen. Andere Softwareprodukte, wie beispielsweise der Browser Google Chrome, installieren die Updates selbsttätig und ohne eine weitere Nachfrage.

5.2 Backups

Bei einem defekten System ist die Gefahr eines unwiederbringlichen Verlusts Ihrer Daten sehr hoch. Regelmäßige Datensicherungen (Backups) auf externen Speichermedien, wie externen Festplatten, DVDs oder USB-Sticks, bieten Abhilfe.

Die integrierten Funktionen von Windows 7 können für regelmäßige Backups verwendet werden, siehe:
http://windows.microsoft.com/de-DE/windows7/products/features/backup-and-restore

Sie sollten mindestens einmal wöchentlich ein Backup Ihrer Daten anfertigen. Ein vollständiges Systemabbild ist seltener erforderlich, etwa nach größeren Updates oder Installationen von Betriebssystem oder Anwendungssoftware, mindestens jedoch einmal jährlich.

Bedenken Sie stets, dass Sie im Ernstfall alle Daten verlieren können, die im Zeitraum nach der letzten Sicherung erstellt wurden.

5.3 Passwörter

Der Zugang zu Online-Services im Internet erfolgt häufig mittels der Abfrage eines Benutzernamens und Passworts. Wenn Sie verschiedene Online-Dienste nutzen, verwenden Sie dafür jeweils unterschiedliche, komplexe Passwörter. Um sich diese besser behalten zu können, sollten Sie Merkhilfen verwenden, etwa die Anfangsbuchstaben eines längeren Satzes. Notieren Sie Ihre Passwörter zudem auf Zetteln und bewahren Sie diese räumlich getrennt von Ihrem Rechner an einem sicheren Ort auf. Hinweise zur Passwort-Sicherheit finden Sie bei auf der BSI-Webseite „BSI für Bürger“.

Die empfohlenen Internet-Browser besitzen integrierte Funktionen, mit denen Sie Kennwörter für besuchte Webseiten verwalten können.

Zudem sind kostenlose technische Lösungen zum Erzeugen und Verwalten komplexer Passwörter verfügbar, z. B. *keepass* (http://keepass.info).

5.4 Notfallmaßnahmen

Bereiten Sie sich auf die skizzierten potenziellen Notfälle vor und überlegen Sie sich Ihre Reaktion in folgenden Situationen:

- Der Rechner startet nicht mehr.
- Sie können keine Verbindung mehr mit dem Internet herstellen.
- Sie können sich nicht mehr in Ihrem E-Mail-Postfach anmelden.
- Sie bemerken eine nicht von Ihnen vorgenommene Überweisung von Ihrem Bankkonto.

Microsoft gibt Ihnen verschiedene Hilfestellungen für solche Situationen unter:

http://windows.microsoft.com/de-DE/windows7/help/system-repair-recovery

Wenn Sie das Gefühl haben, dass Sie in diesen Situationen unsicher reagieren werden oder keine angemessenen Antworten finden, dann suchen Sie sich schon jetzt einen vertrauenswürdigen Ansprechpartner, der Sie bei der Bewältigung unterstützen kann.

6 PC-Entsorgung

Wenn Sie Ihren PC eines Tages entsorgen möchten, dann sollten Sie sicherstellen, dass alle Daten auf der Festplatte vernichtet sind. Ein einfaches Löschen in den „Papierkorb“ oder im Windows Explorer ist hierfür nicht ausreichend.

Zur sicheren Löschung der Daten sollten Sie Ihren PC von einer in das CD-ROM-Laufwerk eingelegten Live-CD starten (z. B. http://www.ubuntu.com/download/ubuntu/download), dann die Festplatte in das gestartete Live-System einbinden und schließlich in der Kommandozeile mit der Eingabe des Befehls

```
dd if=/dev/urandom of=/dev/GERAETENAME
```

löschen. Dabei steht der GERAETENAME für die erste Festplatte, die meistens mit „hda“ oder „sda“ bezeichnet wird. Sie sollten auf die Angaben der Kommandozeile achten.

Sie können Ihre Festplatte auch mit *BitLocker Drive Encryption* oder *TrueCrypt*, siehe Verschlüsselung der Festplatte, verschlüsseln und lediglich das Schlüsselmaterial vernichten.

Um Ihre Festplatte alternativ unbrauchbar zu machen, können Sie diese ausbauen und physisch zerstören. Ein Verkauf einer gebrauchten Festplatte lohnt sich in den meisten Fällen nicht, wenn man den möglichen Erlös ins Verhältnis zum Wert Ihrer Daten setzt.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **info@cyber-allianz.de** gesendet werden.

Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IM UNTERNEHMEN

Sichere Nutzung von PCs unter Ubuntu

Empfehlungen für kleine Unternehmen und Selbstständige

Ausgangslage

Viele nützliche und wichtige Dienstleistungen wie Online-Banking, E-Commerce oder E-Government werden heute über das Internet angeboten und genutzt. Auch in Zukunft wird sich die Anzahl der Online-Services noch weiter erhöhen. Hinzu kommt der verstärkte Einsatz mobiler Endgeräte wie Smartphones und Tablets, mit denen diese Dienste auch unterwegs genutzt werden können. Personal Computer (PCs) mit verschiedenen Betriebssystemen, wie Microsoft Windows, Apple Mac OS X oder einer Linux-Variante spielen derzeit jedoch noch die wichtigste Rolle.

Ziel

Die vorliegende BSI-Empfehlung zur Cyber-Sicherheit bietet Hilfestellungen für die sichere Konfiguration eines PCs unter der Linux-Distribution Ubuntu. Sinnvoll ist dabei die Betrachtung des Lebenszyklus eines solchen Linux-Systems:

- Anschaffung des Systems
- Installation und erste Inbetriebnahme
- Regelmäßiger Betrieb
- Entsorgung des Systems

Mit wenigen Maßnahmen kann ein PC unter dem Linux-Betriebssystem Ubuntu so abgesichert werden, dass eine weitgehend sichere Nutzung von Dienstleistungen über das Internet möglich ist.

Beachten Sie zusätzlich auch das Dokument „Sichere private Nutzung des Internets“, ebenfalls aus der Reihe „BSI-Empfehlungen zur Cyber-Sicherheit“.

Anschaffung des Systems

Bereits bei der Anschaffung des Systems gibt es wichtige Aspekte, die Sie für einen späteren sicheren Betrieb von Ubuntu beachten sollten.

Hardware und Betriebssystem

Achten Sie beim Kauf des PCs auf möglichst aktuelle PC-Hardware. Diese sollte zudem für einen reibungslosen Betrieb mit Ubuntu geeignet sein. Eine Übersicht von Systemen verschiedener

Hersteller, deren Eignung geprüft wurde, finden Sie auf der Internetseite von Ubuntu[1]. Falls Sie PC-Hardware ohne eine vorinstallierte Version von Ubuntu erwerben, sollten Sie die neueste Version von Ubuntu herunterladen[2] und installieren. Dabei können Sie sich zur Vermeidung häufiger Wechsel auf neue Betriebssystemversionen auch für eine sogenannte *LTS-Version* von Ubuntu (Long-Term Support) entscheiden, die Ihnen eine Langzeitunterstützung über fünf Jahre mit Updates und Sicherheitsaktualisierungen garantiert.

Virenschutzprogramm

Die Installation eines Virenschutzprogramms ist, basierend auf dem aktuellen Stand der Bedrohungslage in Bezug auf Schadsoftware für Linux, unter Ubuntu nicht notwendig.

Backups

Um Sicherungskopien Ihrer Daten zu erstellen, können Sie das in Ubuntu über die Dash-Startseite bereitgestellte Werkzeug *Datensicherung* verwenden. Diese Backups können Sie entweder in einem Online-Speicher im Internet wie dem voreingestellten *Ubuntu One* ablegen oder auf einem externen Speichermedium wie einer USB-Festplatte. Der Vorteil eines eigenen Speichermediums liegt in der vollen Kontrolle über Ihre Daten, die Sie bei einer Sicherung über einen Internetdienst zum Teil aufgeben.

Der Einsatz einer gesonderten Backup-Software ist für Ubuntu im Allgemeinen nicht erforderlich. Im geschäftlichen Einsatz von Ubuntu ist gegebenenfalls zu prüfen, ob ein professionelles Sicherungssystem eingesetzt werden sollte, welches spezifische Anforderungen – beispielsweise an Revisionssicherheit, Reporting oder Disaster Recovery – gewährleisten kann.

Anwendungen

Orientiert an Ihrem individuellen Bedarf werden Sie mit der Zeit verschiedene Anwendungsprogramme nutzen, die bei einer Installation von Ubuntu standardmäßig bereits vorhanden sind oder darüber hinaus auch neue Software hinzufügen. Dabei sollten Sie stets Software bevorzugen, die über das Ubuntu Software-Center zur Verfügung gestellt wird. So ist insbesondere auch die automatische Aktualisierung im späteren Betrieb gewährleistet. Darüber hinaus sind Software-Pakete aus dieser Quelle mit Prüfsummen versehen, um zu vermeiden, dass manipulierte Programme installiert werden.

Zur Bearbeitung von Texten, Tabellen oder Präsentationen ist in Ubuntu die kostenlose Bürosoftware *LibreOffice* enthalten, sodass hier keine zusätzliche Installation erforderlich ist.

Zur Darstellung von PDF-Dateien sowie vieler anderer Dokumenten- und Medienformate verfügt Ubuntu bereits über eingebaute Funktionalitäten wie die Anwendung *Dokumentenbetrachter*. Prüfen Sie im Einzelfall, ob Sie eine zusätzliche Anwendung zur Darstellung Ihrer Dateien benötigen oder ob die bereits vorhandenen Möglichkeiten ausreichend sind. Je weniger zusätzliche Anwendungen Sie nutzen, desto kleiner ist die Angriffsfläche des Systems.

Bei allen zusätzlichen Anwendungsprogrammen, die Sie etwa zur Bearbeitung von Fotos oder zum Komponieren und Abspielen von Musik nutzen, sollten Sie darauf achten, dass die Sicherheitsaktualisierungen vom Software-Hersteller auch tatsächlich automatisch installiert werden, ohne dass Sie bei den einzelnen Aktualisierungen aktiv werden müssen. Am einfachsten ist dies über das integrierte Paketverwaltungssystem von Ubuntu möglich. Bei Verwendung von Software aus dem Ubuntu Software-Center sind automatische Updates gewährleistet. Daher sollten Sie sich auf Anwendungen aus dieser Quelle beschränken, wenn Ihnen zu anderen Programmen keine Informationen vorliegen oder Sie unsicher sind, wie sich diese verhalten.

1 http://www.ubuntu.com/certification
2 http://www.ubuntu.com/download

Installation und erste Inbetriebnahme

Einen wichtigen Grundstein für die Systemsicherheit Ihres Systems können Sie bereits bei der Installation und ersten Inbetriebnahme von Ubuntu legen, wenn Sie folgende Punkte beachten.

Installation aller vorhandenen Sicherheitsaktualisierungen

Sofern Sie keine Hardware mit einem vorinstallierten Ubuntu einsetzen, können Sie eine Neuinstallation des Systems in wenigen Schritten selbst vornehmen. Installationsmedien erhalten Sie dabei über die Internetseiten von Ubuntu. Es ist einerseits möglich, Ubuntu als einziges Betriebssystem auf Ihrer PC-Hardware zu installieren, andererseits können Sie es aber auch parallel zu einem bereits vorhandenen Betriebssystem wie z. B. Microsoft Windows einrichten. Während des Installationsprozesses werden Ihnen die für einen solchen Parallelbetrieb relevanten Hinweise gegeben.

Bei einer Neuinstallation von Ubuntu sollten Sie das System mit dem Internet verbinden und die Option *Aktualisierungen während der Installation herunterladen* aktivieren. Bei der ersten Inbetriebnahme eines bereits vorinstallierten Ubuntu-Systems sollten Sie dieses ebenfalls mit dem Internet verbinden und die vom Betriebssystem angebotenen Softwareaktualisierungen herunterladen und installieren.

Um das Sicherheitsniveau von Ubuntu zu halten, ist es erforderlich, stets alle Sicherheitsaktualisierungen nach der Veröffentlichung zu installieren. Die automatische Softwareaktualisierung von Ubuntu ist im Auslieferungszustand bereits aktiviert und deckt sämtliche vorinstallierte Software sowie alle Anwendungen ab, die über das Ubuntu Software-Center hinzugefügt wurden.

Das Suchintervall für neue Updates ist in den Einstellungen der Aktualisierungsverwaltung auf *Täglich* voreingestellt. Hier sollten Sie nicht auf längere Zeiträume wechseln. Damit vorhandene Updates automatisch installiert werden, ohne dass Sie sich weiter darum kümmern müssen, sollten Sie zudem in den Einstellungen der Aktualisierungsverwaltung die Option *Wenn Sicherheitsaktualisierungen vorhanden sind* auf *Automatisch herunterladen und installieren* ändern.

Achten Sie bei der Installation von Drittanbieter-Software darauf, dass auch diese ebenfalls automatische Aktualisierungen vornimmt. Am besten ist dies durch Integration in die Paketverwaltung von Ubuntu möglich.

Benutzerkonten

Das bei der Erstkonfiguration von Ubuntu angelegte Benutzerkonto ist gleichzeitig auch ein Administrator-Konto mit umfassenden Berechtigungen zur Systemkonfiguration. Achten Sie darauf, dass nur solche Anwender administrative Aufgaben auf dem System wahrnehmen dürfen, die diese Funktionalität auch benötigen und beherrschen. Legen Sie für die tägliche Verwendung auf jeden Fall ein zusätzliches einfaches Benutzerkonto an. Sollte Ubuntu von mehreren Anwendern genutzt werden, sollten Sie für jeden Anwender ein eigenes Benutzerkonto anlegen.

Verwenden Sie neben Ihrem normalen Benutzerkonto, welches Sie für die tägliche Arbeit verwenden, ein zusätzliches Benutzerkonto, um transaktionsbezogene Aktivitäten wie Online-Banking durchzuführen oder um kritische Daten online zu versenden.

Verschlüsselung der Festplatte

Falls es sich bei Ihrem Ubuntu-System um ein Notebook handelt, das Sie auch unterwegs nutzen, sollten Sie unbedingt die Festplatte verschlüsseln, um Daten bei Verlust oder Diebstahl des Geräts zu schützen. Wenn Sie einen Desktop-PC besitzen, ist abzuwägen, ob ein möglicher Leistungsverlust Ihres Systems aufgrund der Verschlüsselung in einem angemessenen Verhältnis zum Schutz Ihrer Daten vor dem Zugriff unbefugter Dritter steht.

Wenn Sie Ihre Daten verschlüsseln möchten, dann sollten Sie bei der Installation von Ubuntu die Option *Meine persönlichen Daten verschlüsseln* auswählen. Gleiches gilt beim Anlegen zusätzlicher Benutzerkonten, deren Daten ebenfalls verschlüsselt werden sollten. Zur Entschlüsselung Ihrer Daten im Falle eines Verlusts des Passworts zeigt Ihnen Ubuntu dann einmalig eine zusätzliche *Passphrase* an, die Sie notieren und räumlich getrennt von Ihrem Rechner an einem sicheren Ort aufbewahren sollten.

Neben der Verschlüsselung Ihrer Daten können Sie auch das komplette System einschließlich Ihres Datenverzeichnisses auf der Festplatte verschlüsseln. Bei einer aktuellen Ubuntu-Version wählen Sie hierzu die Option *Die neue Ubuntu-Installation zur Sicherheit verschlüsseln* während des Installationsvorgangs aus und folgen den angezeigten Hinweisen. Zur vollständig verschlüsselten Installation der derzeitigen Version 12.04 mit Langzeitunterstützung durch den Hersteller (LTS) müssen Sie eine sogenannte Alternate-Installation durchführen[3]. Alternativ dazu können Sie bei der LTS-Version beispielsweise auch das kostenlose Produkt *TrueCrypt*[4] verwenden, dessen Einsatz auf den Internetseiten der Ubuntu-Community[5] im Detail beschrieben wird. Erstellen Sie während des Verschlüsselungsvorgangs unbedingt eine "TrueCrypt Rescue Disk". Diese hilft, wenn Probleme beim Entschlüsseln der Festplatte auftreten sollten.

Personal Firewall

Ubuntu bietet in seiner normalen Konfiguration keine Kommunikationsschnittstellen (genauer: keine Ports) nach außen an, die für Angriffe genutzt werden könnten. Daher ist der Einsatz einer Personal Firewall unter Ubuntu nicht erforderlich. Zur Absicherung des Einsatzes zusätzlicher Programme, die Ports nach außen öffnen, können Sie das Firewall-Werkzeug *Firestarter* über das Ubuntu Software-Center nachinstallieren. Dies ist jedoch eher für erfahrene Anwender zu empfehlen.

Internet-Browser

Ihr Internet-Browser ist die zentrale Komponente für die Nutzung von Online-Angeboten im Internet und stellt somit eines der beliebtesten Ziele für Cyber-Angriffe dar. Verwenden Sie daher möglichst einen Browser mit fortgeschrittenen Sicherheitsfunktionen, der regelmäßig über Sicherheitsaktualisierungen auf den neuesten Stand gebracht wird, wie beispielsweise Google Chrome (https://www.google.com/chrome).

Aktivieren Sie zudem den im Browser integrierten Filter zum Schutz vor Phishing und gefährlichen Websites. Bei Chrome finden Sie die entsprechende Option unter *Einstellungen / Erweiterte Einstellungen anzeigen... / Datenschutz*.

Durch den Einsatz eines sicheren Browsers in Verbindung mit den anderen aufgeführten Maßnahmen können Sie das Risiko eines erfolgreichen IT-Angriffs stark reduzieren.

E-Mail

Für die weitgehend sichere Nutzung von E-Mails ist es nicht erforderlich, zusätzliche Software zu installieren. Viele E-Mail-Provider bieten Webmail-Zugänge an, die Sie über den Internet-Zugang mit Ihrem Browser nutzen können. Wichtig ist, auf eine verschlüsselte Verbindung (HTTPS) zum Postfach zu achten, um von den Schutzmechanismen Ihres Browsers zu profitieren. Achten Sie darauf, dass die Verschlüsselung nicht nur für den Login-Vorgang, sondern während der gesamten Webmail-Nutzung aktiviert ist.

Falls Sie erweiterte Anforderungen an Komfort und Funktionalität bei der Arbeit mit E-Mails haben, sollten Sie einen aktuellen E-Mail-Client auswählen und sicher konfigurieren. Bereits in Ubuntu vorhanden ist der E-Mail-Client *Thunderbird*. Hinweise zur Konfiguration von *Thunderbird* finden Sie auf den Internetseiten von Mozilla[6]. Insbesondere ist auch hier auf die Verwendung verschlüsselter Übertragungsprotokolle (POP3S, IMAPS, SMTPS) zu achten.

3 http://wiki.ubuntuusers.de/System_verschl%C3%BCsseln/Alternate_Installation
4 http://www.truecrypt.org/downloads
5 http://wiki.ubuntuusers.de/TrueCrypt
6 http://support.mozillamessaging.com/de/home

Verzichten Sie zudem auf die Darstellung und Erzeugung von E-Mails im HTML-Format. Die Anzeige von externen Inhalten – beispielsweise Bilder in HTML-E-Mails – sollten Sie deaktivieren, da diese ein zusätzliches Einfallstor zur Ausführung von Schadcode auf Ihrem Rechner darstellen.

Java-Laufzeitumgebung

Einige Anwendungen benötigen unter Umständen die Java-Laufzeitumgebung[7]. Um die Angriffsfläche Ihres Systems zu reduzieren, sollten Sie Java nur dann installieren, wenn Ihre Anwendungsprogramme diese Laufzeitumgebung tatsächlich benötigen. Wenn Sie Java installieren müssen, schalten Sie es trotzdem standardmäßig in Ihrem Webbrowser ab. Sie können das Java-Plugin dann fallweise aktivieren, wenn es von einer vertrauenswürdigen Website benötigt wird.

Regelmäßiger Betrieb

Beachten Sie im täglichen Umgang mit Ubuntu die folgenden Ratschläge für einen sicheren Betrieb.

Sicherheitsaktualisierungen

Wenn Sie während der Installation berücksichtigt haben, dass sowohl das Betriebssystem als auch alle installierten Anwendungen automatische Updates durchführen, achten Sie auf entsprechende Hinweise dazu im laufenden Betrieb.

Standardmäßig werden Sie von Ubuntu dazu aufgefordert, die Installation von Updates stets zu bestätigen. Stellen Sie also wie weiter oben beschrieben sicher, dass in den Einstellungen der Aktualisierungsverwaltung die Option *Wenn Sicherheitsaktualisierungen vorhanden sind* auf den Wert *Automatisch herunterladen und installieren* konfiguriert ist.

Backups

Bei einem defekten System ist die Gefahr eines unwiederbringlichen Verlusts Ihrer Daten sehr hoch. Regelmäßige Datensicherungen (Backups) auf externen Speichermedien wie beispielsweise externen Festplatten, USB-Sticks oder DVDs bieten Abhilfe.

Die integrierte Backup-Funktion *Datensicherung* von Ubuntu kann für regelmäßige Backups verwendet werden. Diese Funktion sollten Sie so konfigurieren, dass Ihre Daten kontinuierlich im Hintergrund auf dem für diesen Zweck eingerichteten externen Speichermedium gesichert werden. Ist dieses nicht dauerhaft mit Ubuntu verbunden, sollten Sie mindestens einmal wöchentlich ein Backup Ihrer Daten anfertigen. Bedenken Sie stets, dass Sie im Ernstfall alle Daten verlieren können, die im Zeitraum nach der letzten Sicherung erstellt wurden.

Passwörter

Der Zugang zu Online-Services im Internet erfolgt häufig mittels der Abfrage eines Benutzernamens und Passworts. Wenn Sie verschiedene Online-Dienste nutzen, verwenden Sie dafür jeweils unterschiedliche, nicht erratbare Passwörter. Um solche komplexen Passwörter handhaben zu können, sollten Sie Merkhilfen verwenden, etwa die Anfangsbuchstaben eines längeren Satzes. Notieren Sie Ihre Passwörter zudem auf Zettel und bewahren Sie diese räumlich getrennt von Ihrem Rechner an einem sicheren Ort auf. Zudem können Sie den Passwortspeicher des Betriebssystems nutzen. Unter Ubuntu ist dies der *Schlüsselbund*. Hinweise zur Passwort-Sicherheit finden Sie bei „BSI für Bürger“[8].

7 http://java.com/de
8 https://www.bsi-fuer-buerger.de/Passwoerter

Notfallmaßnahmen

Auch Linux-Systeme können von Abstürzen oder Fehlfunktionen betroffen sein, die Auswirkungen auf Ihren Datenbestand oder die Nutzbarkeit Ihrer Anwendungen haben können. Bereiten Sie sich auf solche potenziellen Notfälle vor und überlegen Sie sich Ihre Reaktion in folgenden Situationen:

- Der Rechner startet nicht mehr.
- Sie können keine Verbindung mehr mit dem Internet herstellen.
- Sie können sich nicht mehr in Ihr E-Mail-Postfach einloggen.
- Sie bemerken eine nicht von Ihnen vorgenommene Überweisung von Ihrem Bankkonto.

Wenn Sie das Gefühl haben, dass Sie in diesen Situationen unsicher reagieren werden oder keine angemessenen Antworten finden, suchen Sie sich schon jetzt einen vertrauenswürdigen Ansprechpartner, der Sie bei der Bewältigung unterstützen kann.

Entsorgung

Wenn Sie Ihr Ubuntu-System eines Tages entsorgen möchten, sollten Sie sicherstellen, dass alle Daten auf der Festplatte vernichtet sind. Ein einfaches Löschen von Daten durch das Verschieben in den „Papierkorb“ ist hierfür nicht ausreichend.

Vielmehr sollten Sie Ihren PC von einer in das DVD-/CD-ROM-Laufwerk eingelegten Live-CD (z. B. *Ubuntu LiveCD*[9]) starten, dann die Festplatte in das gestartete Live-System einbinden und schließlich in der Kommandozeile mit der Eingabe des folgenden Befehls löschen:

```
sudo dd bs=1M if=/dev/urandom of=/dev/GERAETENAME
```

Dabei steht der GERAETENAME für die Festplatte, die meistens mit "hda" oder "sda" bezeichnet wird, wenn es sich um die erste oder einzige Festplatte in dem System handelt. Informationen darüber, wie Sie herausfinden können, welcher GERAETENAME im obigen Befehl zu verwenden ist, finden Sie im Internet[10].

Sie können Ihre Festplatte alternativ auch mit TrueCrypt – siehe Kapitel *Verschlüsselung der Festplatte* – schützen und lediglich das Schlüsselmaterial vernichten.

Um Ihre Festplatte alternativ unbrauchbar zu machen, können Sie diese ausbauen und physisch zerstören. Ein Verkauf einer gebrauchten Festplatte lohnt sich in den meisten Fällen nicht, wenn man den möglichen Erlös ins Verhältnis zum Wert Ihrer Daten setzt.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **info@cyber-allianz.de** gesendet werden.

9 http://www.ubuntu.com/download/ubuntu/download
10 http://wiki.ubuntuusers.de/Datenträger

Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IM UNTERNEHMEN

Sichere Nutzung von Macs unter Apple OS X Mountain Lion

Empfehlungen für kleine Unternehmen und Selbstständige

Ausgangslage

Viele nützliche und wichtige Dienstleistungen, wie Online-Banking, E-Commerce oder E-Government, werden heute über das Internet angeboten und genutzt. Auch in Zukunft wird sich die Anzahl der Online-Services noch weiter erhöhen. Hinzu kommt der verstärkte Einsatz mobiler Endgeräte, wie Smartphones und Tablets, mit denen diese Dienste auch unterwegs genutzt werden können. Personal Computer (PCs) mit verschiedenen Betriebssystemen, wie Apple Mac OS X, Microsoft Windows oder einer Linux-Variante, spielen derzeit jedoch noch die wichtigste Rolle.

Ziel

Die vorliegende BSI-Veröffentlichung zur Cyber-Sicherheit bietet Hilfestellungen für die Konfiguration eines Macs unter dem Gesichtspunkt der Sicherheit. Sinnvoll ist dabei die Betrachtung des Lebenszyklus eines Rechners:

- Anschaffung des Systems
- Installation und erste Inbetriebnahme
- Regelmäßiger Betrieb
- Entsorgung des Systems

Mit wenigen Maßnahmen können Macs unter dem aktuellen Betriebssystem OS X Mountain Lion so abgesichert werden, dass eine weitgehend sichere Nutzung von Dienstleistungen über das Internet möglich ist.

Beachten Sie zusätzlich auch das Dokument „Sichere private Nutzung des Internets“, ebenfalls aus der Reihe „BSI-Veröffentlichungen zur Cyber-Sicherheit“.

Anschaffung des Systems

Bereits bei der Anschaffung des Systems gibt es wichtige Aspekte, die Sie für einen späteren sicheren Betrieb Ihres Macs beachten sollten.

Hardware und Betriebssystem

Achten Sie beim Kauf eines Macs auf möglichst aktuelle Hardware mit der jeweils neuesten Version des Betriebssystems, derzeit also OS X Mountain Lion. Bei einem Neukauf eines Macs ist dieses üblicherweise bereits vorinstalliert. Beim Kauf eines gebrauchten Macs achten Sie darauf, dass dieser von OS X Mountain Lion unterstützt wird. Welche Modelle hier infrage kommen, können Sie einer Übersichtstabelle[1] entnehmen, die Apple im Internet bereitstellt.

Falls der Mac nur über eine ältere Version des Betriebssystems (mindestens Mac OS X 10.6 „Snow Leopard“) verfügt, erwerben Sie über den im Betriebssystem integrierten Mac App Store eine Lizenz für OS X Mountain Lion.

Virenschutzprogramm

Die Installation eines separaten Virenschutzprogramms ist, basierend auf dem aktuellen Stand der Bedrohungslage durch Schadsoftware für Macs, unter OS X Mountain Lion nicht notwendig.

OS X Mountain Lion enthält einen einfachen integrierten Schutz gegen bekannte, Mac-spezifische Schadsoftware, der durch Apple in unregelmäßigen Abständen aktualisiert wird und standardmäßig bereits aktiviert ist. Sie können den Status dieser Funktion in den Systemeinstellungen unter dem Punkt *Sicherheit* | *Weitere Optionen...* überprüfen. Die Option *Liste für sichere Downloads automatisch aktualisieren* sollte aktiviert sein.

Zusätzlich enthält OS X Mountain Lion mit dem sogenannten „Gatekeeper“ eine Funktion, welche die Ausführung von Anwendungen kontrolliert. Standardmäßig erlaubt Gatekeeper nur die Ausführung von solchen Programmen, die entweder über den Mac App Store bezogen wurden oder die von Entwicklern stammen, welche von Apple verifiziert wurden. Das bedeutet keine Garantie dafür, dass diese Anwendungen in jedem Fall harmlos sind. Allerdings ist ihr Urheber identifizierbar und nachträglich manipulierte Programme können ebenfalls erkannt werden.

Es wird empfohlen, Gatekeeper in der Standardkonfiguration zu betreiben. Möchten Sie bewusst eine Anwendung aus einer verlässlichen Quelle starten, bei der Gatekeeper die Ausführung nicht zulässt, können Sie dies über *CTRL+Klick* bzw. *Rechtsklick* und *Öffnen* tun. Gatekeeper merkt sich die Anwendung anschließend als vertrauenswürdig. Dieses Verfahren ist beispielsweise bei manchen Programmen notwendig, die vor der Veröffentlichung von OS X Mountain Lion erstellt wurden. Auch bestimmte Anwendungen aus dem Open-Source-Bereich, wie etwa OpenOffice, sind unter Umständen noch nicht für den Einsatz mit Gatekeeper vorbereitet. Prüfen Sie daher stets die Quelle und bevorzugen Sie die jeweilige Hersteller-Webseite für den Download der Anwendung.

Backups

Um Sicherungskopien sowohl des Systems als auch Ihrer Daten zu erstellen, können Sie die in OS X Mountain Lion eingebaute Funktionalität „Time Machine"[2] verwenden. Der Kauf einer gesonderten Backup-Software ist für OS X Mountain Lion im Allgemeinen nicht erforderlich. Im geschäftlichen Einsatz von OS X Mountain Lion ist gegebenenfalls zu prüfen, ob Time Machine als Ergänzung zu einem professionellen Sicherungssystem eingesetzt werden kann, welches spezifische Anforderungen – beispielsweise an Revisionssicherheit, Reporting oder Disaster Recovery – gewährleisten kann.

Beschaffen Sie beim Kauf des Macs für die Erstellung von Backups mittels Time Machine eine zusätzliche externe Festplatte mit ausreichend großem Speicherplatz (Richtwert: mindestens die doppelte Größe der internen Festplatte).

1 http://www.apple.com/de/osx/specs/
2 http://www.apple.com/de/macosx/apps/#timemachine

Anwendungen

Zur Darstellung von PDF-Dateien sowie vieler anderer Dokumenten- und Medienformate verfügt OS X Mountain Lion bereits über eingebaute Funktionalitäten, wie die Anwendung „Vorschau“ oder die Funktion „QuickLook“. Prüfen Sie im Einzelfall, ob Sie eine zusätzliche Anwendung zur Darstellung ihrer Dateien benötigen oder ob die bereits vorhandenen Möglichkeiten ausreichend sind. Je weniger zusätzliche Anwendungen Sie nutzen, desto kleiner ist die Angriffsfläche des Systems.

Bei allen zusätzlichen Anwendungsprogrammen, die Sie etwa zur Bearbeitung von Fotos oder zum Komponieren und Abspielen von Musik nutzen, sollten Sie darauf achten, dass die Produkte mit einer Funktion zur automatischen Aktualisierung ausgestattet sind. In der Regel lässt sich dies unter dem Menüpunkt *Einstellungen* in der jeweiligen Software überprüfen und konfigurieren. Updates sollten idealerweise ohne Ihr Zutun automatisch im Hintergrund installiert werden. Verbreiteter sind Aktualisierungsfunktionen, die Sie bei verfügbaren Updates benachrichtigen. Die Installation sollten Sie stets zeitnah durchführen. Für die im Folgenden beispielhaft genannten Produkte aus dem Bereich Bürosoftware gibt es solche Aktualisierungsmechanismen, die standardmäßig nach der Installation bereits aktiviert sind:

- kostenlos: LibreOffice (http://www.libreoffice.org)
- kostenpflichtig: Apple iWork (http://www.apple.com/de/iwork/)
- kostenpflichtig: Microsoft Office für Mac (http://www.microsoft.com/germany/mac)

Installation und erste Inbetriebnahme

Einen wichtigen Grundstein für die Systemsicherheit Ihres Macs können Sie bereits bei der Installation und ersten Inbetriebnahme des Rechners legen.

Installation aller vorhandenen Sicherheitsaktualisierungen

Üblicherweise ist OS X Mountain Lion im Auslieferungszustand eines neu erworbenen Macs bereits vorinstalliert. Ist dies – etwa bei einem Gebrauchtgerät – nicht der Fall, so führen Sie zunächst eine vollständige Neuinstallation von OS X Mountain Lion durch.

Um das Sicherheitsniveau des Macs zu halten, ist es erforderlich, stets alle Sicherheitsaktualisierungen nach deren Erscheinen zu installieren. Die automatische Softwareaktualisierung von OS X Mountain Lion ist in den Mac App Store integriert und im Auslieferungszustand bereits aktiviert. Sie sucht täglich nach Aktualisierungen für das Betriebssystem, alle Anwendungen von Apple sowie alle Drittanbieter-Anwendungen, die über den App Store auf dem Mac installiert wurden.

Die automatische Softwareaktualisierung benachrichtigt Sie, wenn Aktualisierungen verfügbar sind, und bietet sie zur Installation an. Führen Sie die Installation zeitnah durch.

Aktivieren Sie die Option *Systemdateien und Sicherheits-Updates installieren* in den *Systemeinstellungen* unter dem Punkt *Softwareaktualisierung*, um sicherheitsrelevante Aktualisierungen ohne Ihr Zutun installieren zu lassen.

Bei der ersten Inbetriebnahme sollten Sie alle zu diesem Zeitpunkt von Apple über die automatische Softwareaktualisierung angebotenen Software-Aktualisierungen unmittelbar herunterladen und installieren.

Benutzerkonten und Inhaltefilter

Das bei der Erstkonfiguration von OS X Mountain Lion angelegte Benutzerkonto (von Apple „Computer-Account“ genannt) ist ein Administrator-Konto mit umfassenden Berechtigungen zur Systemkonfiguration. Achten Sie darauf, dass nur solche Anwender administrative Aufgaben auf dem System wahrnehmen dürfen, die diese Funktionalität auch benötigen und beherrschen. Legen Sie für die tägliche Verwendung des Macs auf jeden Fall zusätzlich ein Standard-Benutzerkonto an. Sollte der Mac von mehreren Anwendern genutzt werden, sollten Sie für jeden Anwender ein eigenes Benutzerkonto anlegen.

Verwenden Sie neben dem Standard-Benutzerkonto, welches Sie für die tägliche Arbeit verwenden, ein zusätzliches Benutzerkonto, um transaktionsbezogene Aktivitäten wie Online-Banking durchzuführen oder um kritische Daten online zu versenden.

Für einfache Benutzerkonten erlaubt OS X Mountain Lion die Aktivierung der Inhaltefilter-Funktion „Kindersicherung“. Diese kann dazu genutzt werden, beispielsweise den Zugriff auf Anwendungen und Webseiten einzuschränken oder Nutzungszeiten für das Benutzerkonto festzulegen.

Verschlüsselung der Festplatte

Falls es sich bei Ihrem Mac um ein Notebook handelt, das Sie auch unterwegs nutzen, sollten Sie unbedingt die Festplatte verschlüsseln, um Daten bei Verlust oder Diebstahl des Geräts zu schützen. Wenn Sie einen Desktop-Mac besitzen, ist abzuwägen, ob ein möglicher Leistungsverlust Ihres Systems aufgrund der Verschlüsselung in einem angemessenen Verhältnis zum Schutz Ihrer Daten vor dem Zugriff unbefugter Dritter steht.

Das Betriebssystem OS X Mountain Lion verfügt über die eingebaute Festplattenverschlüsselung „FileVault“. Diese ist zur Verschlüsselung Ihrer Daten ausreichend, die Anschaffung einer separaten Verschlüsselungs-Software ist nicht erforderlich. Wenn Sie Ihre Daten mit FileVault verschlüsselt haben, können Sie darauf nur mittels Eingabe des Passworts Ihres Benutzerkontos zugreifen. Wählen Sie daher ein sicheres Passwort, welches Sie sich gut einprägen können. Schreiben Sie sich dieses Passwort zusätzlich auf und bewahren Sie den Zettel räumlich getrennt von Ihrem Mac an einem sicheren Ort auf. Hinweise zur Erstellung eines sicheren Passworts finden Sie bei „BSI für Bürger[3]“.

Bei Verlust Ihres persönlichen Passworts können Sie nur noch auf Ihre Daten zugreifen, wenn Sie einen Wiederherstellungsschlüssel haben. Notieren Sie sich daher auch den von FileVault bei der Aktivierung angezeigten Wiederherstellungsschlüssel und bewahren Sie ihn ebenfalls an einem sicheren Ort auf. FileVault bietet zusätzlich an, den Wiederherstellungsschlüssel verschlüsselt bei Apple zu hinterlegen. Entscheiden Sie, ob dies – abhängig von der Art Ihrer Daten – für Sie akzeptabel ist. Vor allem im privaten Umfeld ist der Verlust Ihrer Daten durch einen verlorenen Wiederherstellungsschlüssel oftmals gravierender als der theoretische Fall, dass ein Unbefugter Zugriff auf den bei Apple hinterlegten Schlüssel erlangt. Im Zuge der Speicherung des Schlüssels auf den Apple-Servern müssen Sie Sicherheitsfragen und dazu passende Antworten festlegen. Wählen Sie hier Sicherheitsfragen mit entsprechenden Antworten, die ausschließlich Ihnen bekannt sind.

Die Verschlüsselung durch FileVault erfolgt im Hintergrund. Sie können also nach der Aktivierung von FileVault normal weiterarbeiten.

Personal Firewall

OS X Mountain Lion besitzt eine integrierte Personal Firewall, die im Auslieferungszustand jedoch nicht aktiviert ist. Starten Sie daher die Firewall in den Systemeinstellungen unter dem Punkt Sicherheit. Die Installation einer zusätzlichen Firewall ist nicht erforderlich, da das System durch die eingebaute Firewall hinreichend gegen Angriffe über das Netz geschützt wird und zudem standardmäßig von OS X Mountain Lion keine aktivierten Netzwerkdienste wie Dateifreigaben oder Fernwartungsmöglichkeiten bereitgestellt

3 https://www.bsi-fuer-buerger.de/Passwoerter

werden. Aktivieren Sie solche Dienste nur, wenn Sie diese tatsächlich benötigen und sicher konfigurieren können.

Internet-Browser

Ihr Internet-Browser ist die zentrale Komponente für die Nutzung von Online-Angeboten im Internet und stellt somit eins der beliebtesten Ziele für Cyber-Angriffe dar. Verwenden Sie daher möglichst einen Browser mit Sandbox-Technologie. Unter OS X Mountain Lion sind dies:

- Apple Safari (im Betriebssystem integriert)
- Google Chrome (https://www.google.com/chrome)

Vorteilhaft sind bei Google Chrome die kurzen Update-Intervalle sowie die Funktion zur automatischen Aktualisierung, die auch den integrierten Adobe Flash Player umfasst. Dadurch wird auch der Adobe Flash Player stets auf dem neuesten Stand gehalten. Wenn Sie ausschließlich Google Chrome verwenden, sollten Sie einen eventuell zusätzlich installierten Adobe Flash Player von Ihrem Mac entfernen.

Aktivieren Sie zudem den im Browser integrierten Filter zum Schutz vor Phishing und gefährlichen Websites. Bei Chrome finden Sie die entsprechende Option unter *Einstellungen* | *Erweiterte Einstellungen anzeigen...* | *Datenschutz*, bei Safari unter *Einstellungen* | *Sicherheit*.

Durch den Einsatz eines dieser Browser in Verbindung mit den anderen aufgeführten Maßnahmen können Sie das Risiko eines erfolgreichen IT-Angriffs stark reduzieren.

E-Mail

Für die weitgehend sichere Nutzung von E-Mails ist es nicht erforderlich, zusätzliche Software zu installieren. Viele E-Mail-Provider bieten Webmail-Zugänge an, die Sie über den Internet-Zugang mit Ihrem Browser nutzen können. Wichtig ist, auf eine verschlüsselte Verbindung (HTTPS) zum Postfach zu achten, um von den Schutzmechanismen Ihres Browsers zu profitieren. Achten Sie darauf, dass die Verschlüsselung nicht nur für den Login-Vorgang, sondern während der gesamten Webmail-Nutzung aktiviert ist.

Falls Sie erweiterte Anforderungen an Komfort und Funktionalität bei der Arbeit mit E-Mails haben, sollten Sie einen aktuellen und verbreiteten E-Mail-Client auswählen und diesen sicher konfigurieren, wie zum Beispiel:

- Apple Mail (im Betriebssystem integriert)
- Thunderbird (http://mozilla.org/de/thunderbird)

Hilfestellungen zur Konfiguration finden Sie auf den Webseiten der Anbieter:

- Apple Mail (http://www.apple.com/de/support/mail/)
- Thunderbird (http://support.mozillamessaging.com/de/home)

Auch bei der Nutzung von E-Mail-Programmen ist auf die Verwendung verschlüsselter Übertragungsprotokolle (POP3S, IMAPS, SMTPS) zu achten.

Verzichten Sie zudem auf die Darstellung und Erzeugung von E-Mails im HTML-Format. Die Anzeige von externen Inhalten – beispielsweise Bilder in HTML-E-Mails – sollten Sie deaktivieren, da diese ein zusätzliches Einfallstor zur Ausführung von Schadcode auf Ihrem Rechner darstellen.

Java-Laufzeitumgebung

Einige Anwendungen benötigen unter Umständen die Java-Laufzeitumgebung[4], die nicht in einer Standard-Installation von OS X Mountain Lion enthalten ist. Um die Angriffsfläche Ihres Systems zu reduzieren, sollten Sie Java nur dann installieren, wenn Ihre Anwendungsprogramme diese Laufzeitumgebung tatsächlich benötigen. Beim Start einer entsprechenden Anwendung weist OS X Mountain Lion

4 http://java.com/de

auf das Fehlen von Java hin und bietet einen automatischen Download einer von Apple bereitgestellten Version von Java 6 an. Nach der Installation wird diese über die im Betriebssystem integrierte Softwareaktualisierung automatisch auf einem aktuellen Stand gehalten. Für ein manuell installiertes Java 7 der Firma Oracle können die Updates über die „Systemeinstellungen“ von OS X Mountain Lion konfiguriert werden.

Wenn Sie die Java-Laufzeitumgebung installieren müssen, sollten Sie trotzdem die Java-Unterstützung in den Einstellungen Ihres Webbrowsers abschalten. Sie können Java dann fallweise aktivieren, wenn es von einer vertrauenswürdigen Website benötigt wird. Alternativ können Sie das Dienstprogramm „Java-Einstellungen“ verwenden, um Java systemweit ein- und auszuschalten.

Erzeugung eines Datenträgers zur Systemreparatur

Macs mit OS X Mountain Lion werden ohne ein Installationsmedium für das Betriebssystem ausgeliefert. Mit der vorinstallierten Funktion OS X Wiederherstellung können Sie jedoch im Falle eines Defekts oder Absturzes Wartungsarbeiten oder eine Neuinstallation durchführen. Nähere Informationen zur Nutzung stellt Apple im Internet bereit[5].

Ebenfalls sind auf der oben genannten Apple-Webseite Informationen darüber zu finden, wie Sie für den Fall eines Festplattendefekts ein externes Wiederherstellungsmedium erstellen können.

Regelmäßiger Betrieb

Beachten Sie im täglichen Umgang mit Ihrem Mac die folgenden Ratschläge für einen sicheren Betrieb:

Sicherheitsaktualisierungen

Wenn Sie während der Installation eingestellt haben, dass sowohl das Betriebssystem als auch alle installierten Anwendungen automatische Updates durchführen, dann achten Sie auf entsprechende Hinweise im laufenden Betrieb.

In manchen Fällen werden Sie aufgefordert, die Installation von Updates zu bestätigen. Dies trifft etwa auf die integrierte Softwareaktualisierung von OS X Mountain Lion zu. Andere Softwareprodukte, wie beispielsweise der Browser Google Chrome, installieren die Updates selbsttätig und ohne eine weitere Nachfrage.

Backups

Bei einem defekten System ist die Gefahr eines unwiederbringlichen Verlusts Ihrer Daten sehr hoch. Regelmäßige Datensicherungen (Backups) auf externen Speichermedien, wie externen Festplatten, DVDs oder USB-Sticks, bieten Abhilfe.

Die integrierte Backup-Funktion „Time Machine“ von OS X Mountain Lion sichert das Betriebssystem und Ihre Daten kontinuierlich im Hintergrund auf eine für diesen Zweck eingerichtete externe Festplatte. Ist diese nicht dauerhaft mit dem Mac verbunden, sollten Sie mindestens einmal wöchentlich ein Backup Ihrer Daten anfertigen. Bedenken Sie stets, dass Sie im Ernstfall alle Daten verlieren können, die im Zeitraum nach der letzten Sicherung erstellt wurden.

Passwörter

Der Zugang zu Online-Services im Internet erfolgt häufig mittels der Abfrage eines Benutzernamens und Passworts. Wenn Sie verschiedene Online-Dienste nutzen, verwenden Sie dafür jeweils unterschiedliche, nicht erratbare Passwörter. Um solche komplexen Passwörter besser behalten zu können, sollten Sie Merk-

5 http://www.apple.com/de/macosx/recovery/

hilfen verwenden, etwa die Anfangsbuchstaben eines längeren Satzes. Notieren Sie Ihre Passwörter zudem auf Zetteln und bewahren Sie diese räumlich getrennt von Ihrem Rechner an einem sicheren Ort auf. Hinweise zur Passwort-Sicherheit finden Sie bei „BSI für Bürger“.

Die empfohlenen Browser Safari und Chrome besitzen integrierte Funktionen, mit denen Sie Kennwörter für besuchte Webseiten verwalten können. Beide verwenden dazu den in OS X Mountain Lion integrierten Zertifikats- und Passwort-Manager „Schlüsselbund“, auf den auch über das Dienstprogramm „Schlüsselbundverwaltung“ zugegriffen werden kann. Hier werden unter anderem auch alle Kennwörter gespeichert, die Sie etwa für den Zugriff auf WLANs verwenden. Standardmäßig wird der Schlüsselbund mit dem Anmeldepasswort des Benutzers vor einer unbefugten Einsichtnahme oder Verwendung der Passwörter geschützt. Zur Erhöhung der Sicherheit kann über das Dienstprogramm auch ein separates Kennwort für den Anmelde-Schlüsselbund vergeben werden.

Notfallmaßnahmen

Auch Macs können von Abstürzen oder Fehlfunktionen betroffen sein, die Auswirkungen auf Ihren Datenbestand oder die Nutzbarkeit Ihrer Anwendungen haben können. Bereiten Sie sich auf solche potenziellen Notfälle vor und überlegen Sie sich Ihre Reaktion in folgenden Situationen:

- Der Rechner startet nicht mehr.
- Sie können keine Verbindung mehr mit dem Internet herstellen.
- Sie können sich nicht mehr in Ihrem E-Mail-Postfach anmelden.
- Sie bemerken eine nicht von Ihnen vorgenommene Überweisung von Ihrem Bankkonto.

Wenn Sie das Gefühl haben, dass Sie in diesen Situationen unsicher reagieren werden oder keine angemessenen Antworten finden, suchen Sie sich schon jetzt einen vertrauenswürdigen Ansprechpartner, der Sie bei der Bewältigung unterstützen kann. Hierbei können Sie auch auf Angebote von Händlern oder Apple selbst zurückgreifen.

Entsorgung

Wenn Sie Ihren Mac eines Tages entsorgen möchten, dann sollten Sie sicherstellen, dass alle Daten auf der Festplatte vernichtet sind. Ein einfaches Löschen von Daten durch das Verschieben in den „Papierkorb“ ist hierfür nicht ausreichend.

Zur sicheren Löschung der Daten sollten Sie den Mac über die Funktion „OS X Wiederherstellung“ oder von einem externen Installationsmedium für OS X Mountain Lion starten und die Festplatte über das Festplatten-Dienstprogramm sicher löschen. Wählen Sie dazu Ihre Festplatte aus und bewegen Sie unter *Löschen* in den *Sicherheitsoptionen* den entsprechenden Regler nach rechts, um ein sicheres Löschen durchzuführen. Das einmalige Überschreiben aller Daten ist üblicherweise ausreichend. Mehrfaches Überschreiben kann die Sicherheit zusätzlich erhöhen, erfordert aber einen entsprechend größeren Zeitaufwand.

Um Ihre Festplatte alternativ unbrauchbar zu machen, können Sie diese ausbauen und physisch zerstören. Ein Verkauf einer gebrauchten Festplatte lohnt sich in den meisten Fällen nicht, wenn man den möglichen Erlös ins Verhältnis zum Wert Ihrer Daten setzt.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **info@cyber-allianz.de** gesendet werden.

Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IM UNTERNEHMEN

iOS

Konfigurationsempfehlung auf Basis betriebssystemeigener Mittel für eine Nutzung mit erhöhter Sicherheit

1 Einleitung

Smartphones und Tablet-Computer werden heute zunehmend im Arbeitsumfeld eingesetzt und sind vielfach zum wichtigsten Arbeitsgerät für Mitarbeiter geworden. Mittlerweile gibt es eine nicht mehr zu überschauende Anzahl an Geräten mit unterschiedlichen Betriebssystemen. Smartphones und Tablet-Computer mit iOS, Android oder Windows Phone sind mit modernen, einfachen Bedienkonzepten eher auf den Consumer-Markt ausgerichtet und weniger für den geschäftlichen Einsatz mit hohem Schutzbedarf. Damit unterscheiden sie sich grundlegend von anderen Konzepten mobiler Endgeräte, die speziell für den Unternehmenseinsatz konzipiert wurde. Trotzdem finden Geräte mit iOS und Android zunehmend in der Geschäftswelt Verwendung und verdrängen etablierte Lösungen.

Die Innovation bei mobilen Endgeräten hat in den letzten Jahren viele Neuerungen hervorgebracht und viele Funktionen explizit für den Unternehmenseinsatz und insbesondere die Verwaltung der Endgeräte integriert. Zur Nutzung dieser Funktionen werden vergleichbar zum Desktop Einsatz zentrale Management Dienste benötigt. Diese unterstützen im Gegensatz zu klassischen PCs die Verwaltung der mobilen Endgeräte, auch wenn diese „im Feld“ unterwegs sind. Hierdurch werden speziell die Anforderungen für den Unternehmenseinsatz angesprochen.

In diesen Konfigurationsempfehlungen für iOS, die in Zusammenarbeit mit dem Hersteller Apple erstellt wurden, soll gezeigt werden, welche betriebssystemeigenen Mittel zur Verfügung stehen und wie diese zur Erhöhung der Datensicherheit beitragen. Aufgrund der Herkunft der Geräte aus dem Consumer-Bereich reichen die Konfigurationseinstellungen jedoch nicht aus, um Geschäftsprozesse abzusichern, sodass weitere Maßnahmen erforderlich sind. Zusätzlich soll daher aufgezeigt werden mit welchen Mitteln einer Geräteverwaltung erhöhte Sicherheit umgesetzt werden kann.

In der aktuellen Version von iOS wurden maßgebliche Erweiterungen für den Datenschutz und die Verwaltung in Unternehmen eingeführt, welche in diesem Dokument einbezogen wurden.

In den Empfehlungen wird im Folgenden als mobiles Endgerät immer "iPhone" genannt. Dies ist beispielhaft zu sehen. Gemeint sind die iOS-basierten Geräte iPhone, iPad und iPod touch, jeweils in den Versionen, für die die Empfehlungen zutreffen.

Ebenso werden vom Leser gewisse Vorkenntnisse bezüglich der verwendeten Begriffe erwartet. Beispiele sind hier "App", "Safari" oder "App Store".

2 Einsatzszenarien

Bei der Verwendung von Smartphones und Tablets für berufliche Zwecke können grundsätzlich drei Einsatzszenarien unterschieden werden. Das erste Szenario ist ein rein dienstlicher Gebrauch, bei dem keinerlei private Daten und Zugriffe existieren, das Gerät durch sein Passwort und die verwendete Verschlüsselung geschützt ist und nur definierte Apps verwendet werden können. Das zweite Szenario behandelt eine gemischte Verwendung von dienstlich und privat. Dabei können durch eine Systemkonfiguration private Daten von dienstlichen Daten getrennt werden. Im dritten Fall werden sämtliche beruflichen Belange in einer abgeschlossen, gesicherten Einheit bearbeitet, dem sogenannten "Secure Container". Das Smartphone kann außerhalb dieses Containers normal, das heißt ohne spezielle, restriktive Konfiguration verwendet werden. Mit dem Secure Container können weitere besondere technische Anforderung implementieren werden, wie beispielsweise Mehrfaktorauthentifizierung. Hiermit können besonders schützenswerte Daten zusätzlich abgesichert werden.

In iOS wurden zuletzt Verwaltungsfunktionen zur Trennung von privaten und dienstlichen Daten eingeführt. Ein Beispiel hierfür ist die Funktion „Managed Open-In". Hierdurch wird eine Trennung der Daten möglich, obwohl dem Nutzer in einigen Anwendungen diese gleichzeitig konsolidiert dargestellt werden können.

Für die bestmögliche Verwaltung und Prüfung der Compliance ist der Einsatz einer Mobile Device Management- Lösung (MDM) in Verbindung mit dem Device Enrollment Program (DEP) vorgesehen.

Je nach Schutzbedarf ist abzuwägen, wie die mobilen Endgeräte eingesetzt und verwaltete werden. Für einen niedrigen bis normalen Schutzbedarf reicht der Einsatz der nativen Programme. Für einen erhöhten bis hohen Schutzbedarf sollte eine MDM-Lösung, eventuell in Verbindung mit einem DEP eingesetzt werden. Bei hohem Schutzbedarf und in der Bundesverwaltung empfiehlt das BSI den Einsatz des Secure Containers, weil nur damit eine Wechselwirkung zwischen privater und beruflicher Verwendung des mobilen Endgerätes weitestgehend vermieden werden kann und dienstlichen Daten sicher gespeichert werden können. Siehe dazu auch die Empfehlungen zur Cyber-Sicherheit "Mobile Device Management"[1] der Allianz für Cyber-Sicherheit.

3 Sicherheitsrichtlinien

Bevor mobile Endgeräte in eine Unternehmensstruktur eingebunden werden können, müssen klare Regeln für die Integration festgelegt werden. Mit diesen Sicherheitsrichtlinien, den sogenannten Security Policies, werden
u. a. die Rahmenbedingungen bezüglich Auswahl der Geräte, Auswahl der Daten, die auf den Geräten verarbeitet werden dürfen, Einschränkungen der Benutzer und Limitierung der Möglichkeiten der Geräte (Hardware wie Software) festgelegt.

Neben den Sicherheitsrichtlinien ist auch eine Dienstvereinbarung mit einer klaren Darstellung der Rahmenbedingungen für die Verwendung der mobilen Endgeräte notwendig.

Die Durchsetzung der technischen Anforderungen der Sicherheitsrichtlinien ist bei der steigenden Vielzahl der mobilen Endgeräte nur noch mit entsprechenden Tools erreichbar. Dazu wird eine MDM-Lösung verwendet. Mit dieser können sowohl die Einstellungen auf den Geräten vorgenommen und geprüft, als auch ein Lizenzmanagement institutionell erworbener Apps durchgeführt werden.

Apple hat zusätzlich das Programm "Apple Configurator"[2] veröffentlicht, das für die initiale Konfiguration von iOS-Geräten verwendet werden kann und das weitere Einstellungsmöglichkeiten bietet.

1 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_052.html
2 https://itunes.apple.com/de/app/apple-configurator/id434433123?mt=12

4 Restrisiken

Selbst bei der Verwendung von sicheren Einstellungen auf dem mobilen Endgerät, die sowohl den Benutzer als auch die Apps weitgehend in ihren Freiheiten einschränken, bleibt ein Restrisiko. Dieses Restrisiko beruht in erster Linie darauf, dass die Geräte außerhalb einer gesicherten Umgebung eingesetzt werden, oft auch in Umgebungen, in denen man einen Laptop nicht einsetzen würde. Es besteht immer die Gefahr, dass die Geräte (und damit die darauf befindlichen Daten) abhandenkommen. In einem solchen Fall kann man nur darauf vertrauen, dass die eingesetzten Mechanismen zum Schutz der Daten noch wirksam greifen und nachträglich initiierte Aktionen (beispielsweise Remote Wipe) funktionieren.

Sogar beim Einsatz eines Secure Containers verbleiben Restrisiken, denen nicht ohne weiteres begegnet werden kann. Als Beispiel sei die unerlaubte Verwendung des Gerätemikrofons zum Abhören genannt.

Grundsätzlich muss Herstellern proprietärer Lösungen ein hohes Maß an Vertrauen entgegengebracht werden. Auch iOS ist ein solches proprietäres mobiles Betriebssystem, dessen Sourcecode nicht offengelegt und nicht überprüfbar ist. Das gesamte "iOS-Ökosystem", inklusive nativen Apps, App-Store, Push-Mechanismen und Clouddiensten unterliegt vollständig der Kontrolle des Herstellers.

Außerdem muss beachtet werden, dass sichere Konfigurationen immer auch Beschränkungen für den Benutzer bedeuten. Dies führt nicht nur zu Akzeptanzproblemen, sondern fördert auch die Fantasie der Benutzer, Grenzen und Beschränkungen zu überwinden.

5 Allgemeine Empfehlungen

5.1 Hardware

Bei der Neuanschaffung von iPhones sollte auf aktuelle Hardware geachtet werden. Geräte, die vom Betriebssystemhersteller nicht mehr unterstützt werden, sollten durch neue ersetzt werden.

Beim Übergang vom iPhone 4S auf das iPhone 5 hat Apple einen Wechsel beim Kabelanschluss vom 30-poligen Dock Connector auf den sogenannten "Lightning Connector" vollzogen. Ältere Hardwareerweiterungen (einschließlich Sicherheitsprodukte, wie beispielsweise Smartcard-Reader) können ab dem iPhone 5 nicht mehr ohne spezielle Adapter verwendet werden.

5.2 Aktualisierungen

Apple stellt in unregelmäßigen Abständen Aktualisierungen beziehungsweise neue Versionen des iOS-Betriebssystems zur Verfügung. Vor dem Umstieg auf eine neue Version von iOS sollte geprüft werden, ob die vorhandenen Geräte noch unterstützt werden und die verwendeten Apps auch mit dem Update einwandfrei funktionieren. Aktualisierungen des installierten Betriebssystems sollten in jedem Fall zeitnah auf die Geräte ausgerollt werden, um bekannte Sicherheitslücken zu schließen.

Informationen zum Sicherheitsinhalt einer iOS-Version sowie Informationen, welche Apple-Geräte durch ein Update unterstützt werden, liefert die Apple-Datenbank[3]. Die Datenbank enthält Updateinformationen zu allen Apple-Produkten, u.a. auch zu iOS. IOS Betaversionen können durch ein kostenpflichtiges Entwicklerprogramm für iOS[4] heruntergeladen und getestet werden. Grundsätzlich ist es empfehlenswert für den Test von Beta Versionen keine Produktivgeräte zu verwenden. Für den Test müssen dediziert iPhones im Apple-Entwicklerprogramm registriert werden. In der Regel ist ein Downgrade von der Betaversion nur auf die aktuelle Version möglich.

3 http://support.apple.com/kb/HT1222?viewlocale=de_DE&locale=de_DE
4 https://developer.apple.com/programs/ios/

Nach einer Aktualisierung sollte überprüft werden, dass die Einstellungen nach der Installation weiterhin unverändert vorliegen und den Anforderungen entsprechen. Durch Updates werden gegebenenfalls neue Funktionen integriert oder aktiviert, welche in der Vorgängerversion nicht enthalten waren. Damit können Konfigurationsänderungen auftreten. Beispiel: Aktivierung der Bluetooth-Funktion mit Einführung von Continuity.

5.3 Synchronisation

Die Synchronisation von Inhalten findet in den meisten Fällen zwischen einem iPhone und einem Desktop-Computer oder mit zentralen Diensten statt. Zentrales Hilfsmittel für den Abgleich mit einem Computer ist das Programm iTunes. Es hält alle Daten vor, die mit dem mobilen Endgerät abgeglichen werden. Synchronisiert werden können Programme, Medieninhalte, Lesezeichen, Bücher, Kontakte, Kalender, Fotos, Notizen, Dokumente und Klingeltöne. Eine Synchronisation kann mittels USB oder im selben WLAN stattfinden. Zusätzliche Informationen finden Sie im Apple-Supportartikel[5].

Wenn Sie in iTunes die Option "Automatisch synchronisieren, wenn dieses iPhone verbunden ist" aktivieren, findet eine Synchronisation statt, sobald das iPhone an den Computer angeschlossen wird. Um das zu verhindern, muss diese Option deaktiviert werden. Zu beachten ist, dass es sich hierbei um keine globale Einstellung in iTunes handelt, die für jedes zu synchronisierende iPhone einzeln vorgenommen werden muss.

Standardmäßig wird jedes iPhone, das an einen Mac oder PC angeschlossen wird, in die dortige iTunes-Bibliothek aufgenommen. Das heißt, dass beispielsweise ein beruflich genutztes Gerät mit einem privaten iTunes-Computer synchronisiert werden kann. Um dies zu verhindern, muss das iPhone in den sogenannten "Supervised Mode" versetzt werden. In diesem Modus geht das Gerät nur mit einem bestimmten Mac eine Synchronisations-Beziehung ein. Näheres dazu siehe Kapitel "Supervised Mode".

5.4 Backup

Damit die Daten des iPhones im Bedarfsfall wiederhergestellt werden können, sollten Sie regelmäßige Backups anlegen. Diese Backups können lokal über iTunes oder in der iCloud angelegt und wiederhergestellt werden. Für das iCloud-Backup benötigen Sie keinen lokalen iTunes-Computer und auch keine Kabelverbindung mehr, sondern nur eine WLAN-Verbindung und eine Apple-ID. Eine Sicherung wird automatisch erstellt, wenn das Gerät gesperrt, mit einem WLAN-Netzwerk sowie einer Stromverbindung verbunden ist. Die Übertragung der Daten, wie auch das Backup selbst auf den iCloud-Servern, ist verschlüsselt. Die Daten werden nach ihrer Verschlüsselungsklasse im verschlüsselten Zustand vom Gerät übertragen und nochmals auf den iCloud-Servern verschlüsselt. Der Verschlüsselungs-Schlüssel dazu wird nicht vom Benutzer, sondern von Apple vergeben. Daten mit der Klasse „No Protection“ werden lediglich für den Transport verschlüsselt und liegen auch im Backup unverschlüsselt vor. Keychain-Inhalte (Passwörter, E-Mail-Accounts, WLAN-Accounts, usw.) werden mithilfe eines Hardwareschlüssels (UID) des Gerätes verschlüsselt und können somit immer nur auf dem Original-Gerät wiederhergestellt werden.

Apple stellt den iCloud-Backup-Dienst unter Vorbehalt zur Verfügung. Hierbei wird weder eine dauerhafte Speicherung der Backup-Daten gewährleistet noch ,dass die Daten "...NICHT VERSEHENTLICH BESCHÄDIGT ODER VERFÄLSCHT WERDEN, VERLOREN GEHEN ODER ENTFERNT WERDEN". Lesen Sie dazu Kapitel "iCloud" und folgen Sie dem Link zu den Nutzungsbedingungen für die iCloud.

Sollten Sie sich dennoch für ein iCloud-Backup entscheiden, können Sie festlegen, welche Daten in der iCloud gesichert werden sollen (Einstellung - iCloud). Wie bei anderen Lösungen

5 http://support.apple.com/kb/HT1386?viewlocale=de_DE&locale=de_DE

auch müssen Sie sich aber bewusst sein, dass Sie keinen Einfluss auf den Schutz der Backup-Daten haben. Der einzige "Schutz"-Mechanismus, der in Ihrem Einflussbereich liegt, ist das Kennwort für die verwendete Apple-ID. Verwenden Sie für die iCloud eine andere Apple-ID als beispielsweise für den Apple Store und verwenden Sie ein ausreichend langes und komplexes Kennwort. Siehe dazu auch Kapitel "Zwei-Faktor-Authentifizierung für Apple-ID" unten.

Das BSI empfiehlt, lokale Backups auf einem externen Datenträger (beispielsweise einer externen Festplatte) in regelmäßigen Zeitintervallen. Sichern Sie diese Backups mit einem Kennwort. In diesem Fall werden die Backups mit dem Passwort verschlüsselt. Bei der Verwendung einer MDM- Lösung oder des „Apple Configurator“ kann die Eingabe eines Kennworts erzwungen werden.

Werden Apps durch ein MDM auf dem iPhone installiert, kann das Backup für die Daten der App deaktiviert werden, insofern das MDM System diese Funktion unterstützt. Das heißt, dass die Einstellungen für eine App, die über ein MDM installiert wird, dahingehend verändert werden, dass die Inhalte der App nicht in ein Backup übernommen werden. Vergleichen Sie hierzu auch den Abschnitt „Managed Open-In”.

5.5 iCloud

Über Apples iCloud können Daten zwischen verschiedenen Apple-Geräten automatisch synchronisiert werden. Damit stehen die Daten automatisch auf allen angemeldeten Geräten zur Verfügung. Es handelt sich um E-Mails, Kontakte, Kalenderdaten, Erinnerungen, Lesezeichen, Notizen, Passbook-Daten, Fotos und Schlüsselbund-Daten, mit denen Zugangsdaten synchronisiert werden. Außerdem können Backups und Dokumente in der iCloud abgelegt werden. Daneben gibt es Apps, welche die Daten vollständig in der iCloud ablegen. Weitere Dienste wie "Mein iPhone suchen" werden auch über die iCloud realisiert.

Bei der Verwendung der iCloud-Dienste wissen Sie nicht, wo Ihre Dokumente, Backups und sonstigen Daten gespeichert werden und ob ihre Daten auf den Servern wieder gelöscht werden, wenn Sie die entsprechenden Optionen auf allen iPhones deaktivieren. Lesen Sie auch die Nutzungsbedingungen[6] für die iCloud.

Trotz der Annehmlichkeiten, die die iCloud mitbringt, empfiehlt das BSI für die berufliche Verwendung von iPhones auf Synchronisierungsdienste über die iCloud zu verzichten. Ebenso empfiehlt das BSI keine dienstlichen Dokumente und Backups in der iCloud zu speichern. Auch sollte kein iCloud-E-Mail-Account verwendet werden.

5.6 Geräteverschlüsselung / Code-Sperre

Mit der Aktivierung der Code-Sperre wird das iPhone automatisch verschlüsselt (Data Protection). Das Schlüsselmaterial wird aus einer Kombination von geräteeigenen Daten (UID - Unique Identification Key) und dem Sperr- Code selbst erzeugt. Die UID ist fest in das iPhone eingebrannt und kann nicht verändert werden. Angreifer, die die Code-Sperre knacken wollen, brauchen demnach zur Entschlüsselung der Daten das Gerät selbst, weil auf einem baugleichen Gerät eine andere UID eingebrannt ist.

Benutzer können nur über die Qualität der Code-Sperre das Schutzniveau der Verschlüsselung beeinflussen. Bei Geräten, die abhandenkommen, braucht ein Angreifer, der im Besitz des Gerätes ist, zurzeit etwa 15 Minuten, um einen 4-stelligen nummerischen Code zu knacken. Bei einem 6-stelligen alphanumerischen Code würden laut Hersteller dagegen fünfeinhalb Jahre benötigt[7].

6 http://www.apple.com/legal/internet-services/icloud/de/terms.html
7 http://images.apple.com/privacy/docs/iOS_Security_Guide.pdf

Aktivieren Sie die Code-Sperre unter *Einstellungen - Allgemein - Code-Sperre* und verwenden Sie einen mindestens 6-stelligen alphanumerischen Code. Stellen Sie den Wert für „Automatische Sperre“ auf einen möglichst niedrigen Wert ein. Mit iOS 9 wird auf einem iOS Gerät mit integrierter „Touch ID“ automatisch ein mindestens 6-stelliger numerischen Code verlangt.

Lesen Sie in diesem Zusammenhang auch den Absatz "Application Data Encryption".

5.7 Zwei-Faktor-Authentifizierung für Apple-ID

Die Apple-ID ist der zentrale Zugang zu den Apple-Diensten iTunes, App Store, iCloud, iMessage, FaceTime usw. Die Account-Daten sind in der Vergangenheit öfter Ziel von Angriffen gewesen. In dem entsprechenden Account werden u. a. auch die Kreditkartendaten gespeichert.

Als neue Sicherheitsfunktion hat Apple die Zwei-Faktor-Authentifizierung für die Verwaltung des Apple-ID-Accounts und für den Einkauf mit einem neuen Gerät im iTunes Store, App Store oder iBookstore sowie iMessage und FaceTime eingeführt. Sie wird über die Internet-Seite zur Apple-ID[8] eingerichtet.

Bei dem Zwei-Faktor-Authentifizierungsverfahren muss neben dem Kennwort eine zusätzliche PIN eingegeben werden. Diese PIN erhält der Benutzer über einen alternativen Weg auf ein registriertes Gerät - entweder als SMS oder über ein anderes iPhone, welches über dieselbe iCloud-ID angemeldet wurde. Diese Geräte werden automatisch als vertrauenswürdige Geräte hinterlegt. Bei der Anmeldung wählt der Nutzer aus, auf welches registrierte Gerät oder welche Telefonnummer der Code gesendet werden soll.

Bei der Wiederherstellung eines Geräts aus einem iCloud-Backups werden alle Apps wieder aus dem App Store geladen und neu installiert. Mit der Einführung von iOS 9 wird dazu für jede dabei verwendete Apple-ID der zweite Faktor abgefragt.

5.8 Wi-Fi (WLAN)

Smartphones, wie das iPhone, sind nur sinnvoll einsetzbar, wenn sie Zugang zum Internet haben. Die hauptsächlichen Kommunikationskanäle sind dabei das Mobilfunknetz über die SIM-Karte des Providers sowie im Nahbereich Wi-Fi (WLAN). Problematisch sind unverschlüsselte WLANs, etwa an öffentlichen Orten. In diesen Netzen kann potentiell jeder den Netzwerkverkehr mitlesen.

In solchen Netzen werden Ihre Daten durch den Einsatz eines Virtual Private Networks[9] (VPN) im sonst unverschlüsselten Netzwerkverkehr verschlüsselt, sodass ein Angreifer die Daten zwar noch mitlesen kann, sie aber nicht mehr versteht. Die Verwendung von VPN ist jedoch mit Aufwand verbunden, da die Gegenseite der Kommunikationsstrecke ebenso VPN unterstützen muss. Im dienstlichen Umfeld ist dieser Aufwand aber in jedem Fall gerechtfertigt.

Obwohl für den Nutzer ein Komfortfaktor, kann es aus Sicherheitssicht kritisch sein, dass sich ein iPhone die WLANs, in die es einmal eingebucht war, anhand des WLAN-Namens (SSID) merkt. Kommt das Gerät zu einem späteren Zeitpunkt wieder in den Funkbereich eines solchen WLANs, verbindet sich das iPhone automatisch. Um diese Komforteinrichtung auszunutzen, muss ein Angreifer nur wissen, dass Ihr iPhone einmal in einem bestimmten unverschlüsselten öffentlichen WLAN eingebucht war und kann dem iPhone dann ein eigenes WLAN mit der gleichen SSID präsentieren. Das iPhone verbindet sich automatisch. Dies ist besonders an öffentlichen Plätzen wie Flughäfen kritisch.

8 https://appleid.apple.com/
9 http://de.wikipedia.org/wiki/Virtual_Private_Network

Um ein WLAN aus der Merkliste des iPhones zu entfernen, klickt man in Einstellungen - WLAN bei dem entsprechenden WLAN auf "Dieses Netzwerk ignorieren". Das geht aber nur, wenn das iPhone momentan in dem Netzwerk eingebucht ist. Alternativ kann man in Einstellungen - Allgemein - Zurücksetzen - alle Netzwerkeinstellungen zurücksetzen. Damit werden alle gespeicherten WLANs gelöscht. Anschließend verbindet man sich erneut mit den bekannten und gesicherten WLANs.

Generell sollten Sie die WLAN-Funktion in unsicheren Umgebungen nur bei gleichzeitiger Verwendung eines VPN aktivieren oder komplett deaktivieren (Einstellungen – WLAN). Gleiches gilt, wenn sie überhaupt nicht gebraucht wird.

WLAN-Unterstützung
Mit iOS 9 wurde die neue Funktion WLAN-Unterstützung oder im englischen „Wi-Fi Assist“ integriert. Mit dieser wird es ermöglicht, bei einer schlechten WLAN-Verbindung anstatt des WLANs - automatisch - das Mobilfunknetz zur Datenverbindung verwendet wird. Diese Funktion belastet allerdings den genutzten Datentarif, teilweise können hohe Kosten entstehen. Die Funktion wird nicht verwendet, wenn sich das iPhone im Roaming befindet.

WLAN-Unterstützung kann man in *Einstellungen - Mobiles Netz* deaktivieren. In diesem Fall verhält sich das iPhone wie unter iOS 8 und früher.

Weitere Informationen zu den Einstellungen und zur Nutzung von mobilen Daten auf iPhone und iPad (Cellular-Modell) entnehmen Sie dem Apple Support Artikel[10].

5.9 Persönlicher Hotspot

Eine weitere Verbindungsart per WLAN ist die Einstellung "Persönlicher Hotspot" (*Einstellungen - Persönlicher Hotspot*). Bei Aktivierung auf Ihrem Gerät stellen Sie anderen Nutzern Ihren Internetzugang (UMTS/LTE über die SIM-Karte) zur Verfügung. Die Verbindung selbst ist sowohl passwortgeschützt als auch verschlüsselt (WPA2) und sicherheitstechnisch eher unkritisch; die Daten werden im iPhone einfach durchgereicht. Für Sie fallen höchstens zusätzliche Verbindungskosten an. Als zusätzliche Sicherheitsmaßnahme sollten Sie das voreingestellte Kennwort durch ein eigenes, komplexes ersetzen.

Anders herum gesehen können Sie Ihr iPhone aber auch mit einem Ihnen angebotenen Hotspot verbinden. Hier ist Vorsicht geboten. Ihr iPhone "sieht" nur einen WLAN-Zugang. Theoretisch muss die Verbindung dazu nicht verschlüsselt sein, was zur Problematik des oben genannten öffentlichen WLANs führt. Auch wissen Sie nicht, was auf dem anderen mobilen Endgerät passiert. Werden Ihre Daten dort auch nur durchgereicht oder sind eventuell "Zwischenschichten" eingebaut, die Ihre Daten mitlesen?

Verzichten Sie daher weitgehend auf die Verbindung zu "Persönlichen Hotspots" beziehungsweise akzeptieren Sie diese im Ausnahmefall nur von vertrauenswürdigen Personen.

Der Persönliche Hotspot kann auch durch die neue Funktion Continuity im Hintergrund aktiviert und verwendet werden. Siehe dazu auch das Kapitel "Continuity".

Hinweis: Die Verbindung zu einem persönlichen Hotspot funktioniert nicht nur über WLAN, sondern auch per Bluetooth und USB-Kabel. Bei der Verbindung über Bluetooth ist zu beachten, dass bei Deaktivierung des persönlichen Hotspots die Kopplung (Pairing) der Bluetooth-Verbindung nicht immer automatisch beendet wird. Dieses Phänomen ist geräteabhängig. Prüfen Sie daher nach der Deaktivierung des persönlichen Hotspots die Bluetooth-Verbindung.

10 https://support.apple.com/en-us/HT201299

5.10 Bluetooth

Die im Abschnitt Wi-Fi erwähnte Merkliste für bekannte WLANs existiert in ähnlicher Form auch bei Bluetooth. Zu beachten ist, dass der Mechanismus zum allgemeinen Löschen der Merkliste von Netzverbindungen (*Einstellungen - Allgemein - Zurücksetzen - Netzwerkeinstellungen*) für Bluetooth nicht wirkt. Erst wenn man in *Einstellungen - Bluetooth - Devices* auf *"Dieses Gerät ignorieren"* klickt, wird das spezielle Gerät entkoppelt und aus der Merkliste entfernt.

Die Bluetooth-Schnittstelle ist immer wieder Ziel von Angriffsversuchen. Deaktivieren Sie die Bluetooth-Funktion, wenn Sie sie nicht benötigen. Sollte Ihr iPhone oder ein gekoppeltes Bluetooth-Gerät verloren gehen, denken Sie daran, die Verbindungsschlüssel in den verbleibenden Geräten zu löschen.

5.11 Schutzprogramme

Aus Sicht des BSI ist ein gesondertes Virenschutzprogramm auf mobilen Endgeräten zurzeit nicht erforderlich.

Betriebssysteme, wie iOS, sind über die Rechtestruktur für Apps verhältnismäßig gut abgesichert. Das Sandbox- Prinzip verhindert den Zugriff auf Daten außerhalb der Ablaufumgebung, den Zugriff von außen auf App-Daten sowie zwischen Apps. Bei den verschiedenen mobilen Plattformen ist der Grad der Abschottung insgesamt jedoch durchaus unterschiedlich. iOS gibt sich innerhalb des Apple-Ökosystems geschlossener als andere mobile Betriebssysteme, die Programmierern mehr Freiheiten lassen und teilweise auch alternative App-Stores zulassen.

Wegen der genannten Abschottung durch die Sandbox können Schutzprogramm-Apps weder auf andere Apps, noch auf das Betriebssystem zugreifen. Die verbleibenden Datenbestände reichen jedoch nicht für eine umfassende Schutzwirkung wie sie auf Desktop-Computer stattfindet.

Schutzprogramme (AV-Apps) bieten neben der Erkennung von Malware oft weitere Funktionen, wie zum Beispiel Diebstahlschutz, "Parental Control", Verschlüsselung, "Safe Browsing", usw. Im Unternehmensumfeld werden diese Funktionen überwiegend durch die sowieso notwendige Mobile Device Management-Lösung erbracht und können dort durch den Administrator zentral gesteuert werden. Für den Bereich „Safe Browsing“ und Phishing-Schutz lesen Sie bitte das Kapitel "Internet-Browser".

Wichtig ist aus Sicht des BSI, dass die Anwender auf die Risiken hingewiesen werden, die durch sogenanntes "Jailbreaken" bzw. "unsichere" App-Stores entstehen. Beim Jailbreak werden die durch die Rechtestruktur des Betriebssystems gegebenen Sicherheitsmechanismen außer Kraft gesetzt. Programme können mit Root-Berechtigung ablaufen und sind nicht mehr kontrollierbar. Sie könnten sich im System auch jenseits einer Erkennungsmöglichkeit von AV-Apps festsetzen.

Die Anzahl schadhafter Apps in "sicheren" App-Stores ist gering. Taucht im App-Store ein Malware-Paket auf, ist der Anbieter des Stores, d. h. im Falle von iOS Apple gefordert, um betroffene Anwender zu warnen. Der Anbieter könnte sogar eine schadhafte App wieder von den Geräten deinstallieren.

5.12 Supervised Mode / Betreuung

Der "Supervised Mode" bietet erweiterte Verwaltungsmöglichkeiten über eine MDM-Lösung auf einem iPhone, welche im Normalfall nicht verfügbar sind. Der Modus kann ausschließlich bei Aktivierung des iPhones aktiviert bzw. deaktiviert werden. Erweiterte Möglichkeiten sind zum Beispiel die Unterbindung der Kopplung mit Host Systemen, Deaktivierung des Menüs

Einschränkungen und der Möglichkeit ein iPhone über *Alle Inhalte und Einstellungen löschen* zurückzusetzen und einige mehr.

Der „Supervised Mode“ kann entweder über das Programm "Apple Configurator" oder das DEP (vgl. Device Enrollment Program) aktiviert werden. Der „Apple Configurator“ kann in kleineren Unternehmen auch als Konfigurations-Tool und für die Grundeinstellung neuer Geräte eingesetzt werden und iPhones weitgehend über die USB Schnittstelle konfigurieren. Das Tool kann sowohl Konfigurationsprofile als auch Apps installieren. Es ist kostenlos, setzt aber einen Mac-Rechner voraus.

Wie oben beschrieben, bietet der „Supervised Mode“ auch den Vorteil, dass iPhones gefahrlos an fremde Ladestationen angeschlossen werden können.

Hinweis 1: Beim Einstellen des "Supervised Mode" über den „Apple Configurator“ wird das iPhone vollständig gelöscht. Vorhandene Daten sollten erst gesichert werden, bevor der Supervised Mode eingeschaltet wird.

Hinweis 2: Bei Mac-Rechner mit deutscher Spracheinstellung wird der „Apple Configurator“ auch in deutschsprachiger Übersetzung installiert. Im Programm heißt der Reiter "Supervise" dann "Betreuen".

5.13 AirDrop

Über AirDrop können Daten zwischen Apple-Geräten ausgetauscht werden. Die Kommunikation geschieht über ein temporäres ad-hoc Netzwerk (WLAN und Bluetooth) von Gerät zu Gerät. Für die Zeit der Datenübertragung wird eine verschlüsselte Datenverbindung, unabhängig von den bestehenden Verbindungen, aufgebaut. Mit Beendigung der Übertragung wird die Verbindung automatisch wieder abgebaut.

Mit iOS 9 wurde eine neue Einschränkung eingeführt, welche AirDrop als nicht verwalteten Zielort behandelt. Diese Einschränkung muss als Profil bei verwalteten Geräten installiert werden. Wenn diese Einschränkung aktiviert wurde und zusätzlich die Funktion „Managed Open-In“ verwendet wird, können Dokumente aus verwalteten Apps nicht mehr über AirDrop verteilt werden.

Wie auch bei anderen Schnittstellen sollte auch AirDrop abgeschaltet werden, wenn es nicht benötigt wird.

5.14 Vertrauenswürdige Verbindung

Zum Schutz vor unautorisiertem Zugriff über die USB-Schnittstelle auf ein iPhone hat Apple ein Kopplungsmodell eingeführt, welches den Zugriff von einem Hostrechner auf ein iPhone steuert. In der Vergangenheit war es möglich, dass, solange das iPhone entsperrt war, Hostsysteme über USB ungehindert auf ein iPhone zugreifen konnten. Seit iOS 7 überprüft das iPhone die Verbindung zum Host, ob dieser vom Nutzer als vertrauenswürdig definiert wurde. Handelt es sich beim Verbindungsaufbau um einen unbekannten Host, wird der Nutzer explizit darauf hingewiesen. Der Nutzer muss dem Zugriff auf sein iPhone zustimmen. Durch diese Funktion wird der Zugriff auf das iPhone durch beispielsweise ein manipuliertes Ladegerät unterbunden und die Sicherheit maßgeblich erhöht.

Bei Supervised-Geräten bestand hier bereits die Möglichkeit diese Kopplung komplett zu unterbinden und den Datenaustausch zu einem Host zu verbieten.

Benutzer sollten dahingehend geschult werden, dass sie keine vertrauenswürdige Verbindung mit einem fremden, nicht autorisierten Host eingehen.

5.15 Continuity

Mit Continuity besteht die Möglichkeit, dass alle Geräte, die mit derselben iCloud-ID konfiguriert wurden, Inhalte direkt miteinander austauschen können, sofern sie sich im selben WLAN und in unmittelbarer Entfernung befinden. Hierbei kommt neben WLAN auch Bluetooth zum tragen. Unterstützt werden hierbei die Übertragung von Dokumenten innerhalb unterstützter Apps, wie zum Beispiel Mails, welche Sie auf dem iPhone begonnen haben und auf dem Mac fortführen wollen, als auch umgekehrt. Auch können Telefonate am Mac oder einem anderen iOS Gerät angenommen, bzw. initiiert werden. Zudem kann auch der „Personal Hotspot“ des iPhones automatisch verwendet werden, auch wenn dieser in *Einstellungen - Persönlicher Hotspot* deaktiviert ist. Diese Funktionalität wird als "Instant Hotspot" bezeichnet.
Steht ein entsprechendes Dokument zur Fortführung bereit, wird dies entweder mit einem entsprechendem Icon im iOS Lock Screen (oder im OS X Dock) angezeigt. Bei Verwendung des Icons wird das entsprechende Dokument auf das andere Gerät übertragen.

Wie auch bei anderen Schnittstellen sollte auch Continuity abgeschaltet werden, wenn es nicht benötigt wird. Die Funktion kann über *Einstellungen - Allgemein - Handoff & App-Vorschläge - Handoff* deaktiviert werden.

5.16 Per App-VPN

„Per App VPN“ steht für verwaltete Apps zur Verfügung, vgl. auch „Managed Open-In”. Mit dieser Option kann einer verwalteten App ein dedizierter VPN-Tunnel zugewiesen werden, welcher automatisch bei Verwendung der App initiiert und nach Inaktivität beendet wird. Im Gegensatz zu einer klassischen VPN-Konfiguration terminiert nicht das gesamte iPhone den Tunnel, welcher allen darauf installiert Apps Zugriff auf das Intranet des Unternehmens bietet, sondern nur die definierten Apps. Hierdurch wird ein verbesserter Schutz des Unternehmensnetzwerkes gegenüber unautorisierten Zugriffen bei privater Verwendung des iPhones geboten.

Neben den verwalteten Apps kann „Per App VPN“ auch für Safari-Domänen konfiguriert werden. Wird in Safari eine entsprechende Domäne geöffnet, wird automatisch der VPN-Tunnel aufgebaut und der Browser kann die Intranet Dienste des Unternehmens nutzen. Da Safari auf der Sandboxing-Technologie beruht, kann nur der aktive Tab des Browsers auf das Unternehmens-Intranet zugreifen.

Da die VPN Verbindung nicht auf Geräteebene sondern auf App Ebene aufgebaut wird, wird im Unternehmen hierfür eine SSL/TLS-VPN oder seit iOS 9 eine IKEv2 VPN-Infrastruktur mit Unterstützung von „Per App VPN“ benötigt. Gegebenenfalls ist die Installation eines entsprechenden Clients auf dem iPhone notwendig. Weitere Informationen dazu im Support-Artikel des Herstellers[11].

5.17 VPN Always-on

Soll sämtlicher Datenverkehr eines iPhones über das unternehmenseigene Netzwerk laufen, bietet sich die Funktion *„VPN* always-on“ in Verbindung mit dem Protokoll IKEv2[12] an. Diese Funktion bietet die Tunnelung sämtlichen Datenverkehrs des Gerätes, unabhängig von WLAN oder Mobilfunknetz, über das VPN-Gateway des Unternehmens.

Weitere Informationen dazu im entsprechenden Apple-Dokument[13].

11 https://help.apple.com/deployment/ios/#/apdfbf6f529b
12 Internet Key Exchange: siehe: http://en.wikipedia.org/wiki/Internet_Key_Exchange
13 https://help.apple.com/deployment/ios/#/iore8b083096

5.18 Auto-Updates

Apps und ihre Updates können bei iOS automatisch installiert werden. Diese Funktion muss explizit für die verwendete „Apple ID“ aktiviert werden. Damit sind die Programmversionen nicht mehr unter der Kontrolle des Unternehmens oder Benutzers. Dieses Feature sollte abgeschaltet werden (*Einstellungen - iTunes und App* Store - *Automatische Downloads*). Updates sollten vor der Verteilung durch den Administrator getestet werden.

Zusätzlich besteht für Apps die Möglichkeit, ihre Inhalte automatisch im Hintergrund über das Mobilfunknetz oder WLAN zu aktualisieren, um dem Nutzer bei der nächsten Nutzung aktuelle Informationen anbieten zu können (*Einstellungen - Allgemein - Hintergrundaktualisierung*). Auch diese Funktion sollte nur im begründeten Bedarfsfall aktiviert werden.

5.19 iOS Update durch die IT-Administration

Mit iOS 9 und einem MDM kann seitens der IT-Administration ein Update für iOS für die verwalteten iPhones angestoßen werden. Dieser Prozess gewährleistet, dass alle iPhones denselben Versionsstand haben, beziehungsweise kritische Sicherheitsupdates installiert werden.

Die aktuelle Implementierung erfordert für eine automatische Installation des Updates, dass das iPhone über keinen PIN-Code verfügt. Wurde es mit einem PIN-Code versehen, wird der Nutzer zur Installation aufgefordert und anschließend nach dem PIN-Code gefragt, um die Installation durchführen zu können.

Mit dieser neuen Funktion ist eine Aktualisierung der iPhones durch die IT-Administration möglich, die nicht verhindert werden kann.

Für eine automatische Installation ohne Nutzeraktion wäre ein Gerät ohne PIN-Sperre notwendig. Diese Installationsart sollte in keinem Falle verwendet werden, da damit eine elementare Sicherheitsfunktion außer Kraft gesetzt wird.

5.20 Activation Lock

Die Aktivierungssperre greift für die Aktivierung eines iPhones für die Ersteinrichtung. Ein Gerät, bei dem die Aktivierungssperre eingerichtet ist, kann nur mit Hilfe der genutzten iCloud-Anmeldedaten reaktiviert und damit genutzt werden.

Hat der Nutzer ein iCloud Konto auf dem iPhone konfiguriert und die Funktion “Mein iPhone suchen” aktiviert, wird automatisch die Aktivierungssperre für das Gerät aktiviert. Wird ein iPhone auf den Auslieferungszustand zurückgesetzt (*Allgemein - Zurücksetzen sowie Remote-Funktion*), ist für die Neu-Aktivierung des Gerätes sowohl der Accountname als auch das Passwort der iCloud ID notwendig, um die Aktivierung durchzuführen. Gestohlene iPhones ab iOS 7 sind damit für den Dieb im Prinzip wertlos.

Die Aktivierungssperre wird durch Deaktivierung der Funktion “Mein iPhone suchen” ebenfalls deaktiviert. Außerdem wird die Funktion deaktiviert, wenn das Gerät durch “*Alle Dokumente und Einstellungen löschen*” in den Auslieferungszustand versetzt wird.

Bei der Rücknahme eines dienstlichen iPhones sollte daher darauf geachtet werden, dass das iPhone nicht durch die Funktion „Remote Wipe” gelöscht wird, sondern in den Auslieferungszustand zurückgesetzt wird. Im Zweifelsfall kann dies auch über das iCloud-Konto[14] geschehen.

Weitere Information zur Aktivierungssperre im entsprechenden Apple-Dokument[15].

14 http://icloud.com/
15 http://support.apple.com/kb/PH13695?viewlocale=de_DE

5.21 Enterprise Single Sign-On

Gerade bei Smartphones mit relativ kleinen Tastaturen ist die Eingabe von komplexen Kennwörtern schwierig. Bei mehreren Enterprise-Apps, die alle passwortgeschützt sind, führt dies dazu, dass der Benutzer kurze, einfache Zugangscodes verwendet. Bei Single Sign-On authentifiziert sich der Benutzer nur einmal gegenüber den Unternehmensservern. Das Betriebssystem übernimmt dann für alle "registrierten" Apps die weitere Anmeldung. Durch den Wegfall der lästigen Mehrfacheingabe steigt auch die Akzeptanz für ein komplexes Kennwort. Neben der Verwendung von Passwörtern können auch Zertifikate genutzt werden.

Weitere Information zur Aktivierungssperre im entsprechenden Apple-Dokument[16].

5.22 Notification Sync

Bei „Notification Sync“ handelt es sich um einen iCloud-Dienst, der dafür sorgt, dass Mitteilungen (Notifications) auf die verschiedenen iPhones des Benutzers synchronisiert werden. Auf allen Geräten erscheint die gleiche Mitteilung und verschwindet auch wieder von allen Geräten, wenn der Benutzer sie auf seinem aktuellen Gerät löscht. Da es sich um einen Cloud-Dienst handelt, sollten Sie genau abwägen, ob Sie einen solchen Dienst in Anspruch nehmen.

5.23 SMS Weiterleitung

Verwenden mehrere iOS Geräte und Macs dieselbe „Apple ID“ für den iMessage-Dienst, kann unter iOS 8 die Weiterleitung von SMS dediziert für weitere Geräte aktiviert werden. In diesem Falls werden am iPhone eingehende SMS auf allen aktivierten Geräten angezeigt. (*Einstellungen - Nachrichten - Weiterleiten von SMS*)

Diese Einstellung sollte nur im Bedarfsfall aktiviert werden.

5.24 Managed Open-In

Eine App kann sich in iOS als Kandidat für die Bearbeitung bestimmter Dateitypen (beispielsweise zur Anzeige von PDF-Dokumenten) registrieren. Wählt der Benutzer in einer anderen App - etwa im Browser - bei einem solchen Dokument die Option "Öffnen in", wird die registrierte App in einem Auswahlmenü aufgelistet. Dies kann zu einem Sicherheitsproblem führen, wenn sensible Daten unbedacht mit ungeeigneten Apps (beispielsweise soziale Netzwerke oder Clouddienste) geöffnet werden.

Unter iOS werden Apps, welche über ein MDM installiert wurden, automatisch als verwaltete Apps gekennzeichnet. Hierzu stehen Enterprise-Apps oder über das sogenannte Volume Purchase Program[17], kurz VPP, bezogene Apps zur Verfügung. Dem gegenüber werden die durch den Nutzer installierten Apps als nicht verwaltet gehandhabt. Innerhalb einer MDM-Lösung bietet sich die Möglichkeit, dass das Öffnen von Dokumenten aus verwalteten Apps in nicht verwaltete Apps und das Öffnen von Dokumenten aus nicht verwalteten Apps in verwaltete Apps, unterbunden werden kann. Der “Öffnen in” Dialog bietet in diesem Fall nur die entsprechend konfigurierten Apps an.

Hierdurch wird eine Trennung von dienstlichen und privaten Daten erreicht und eine Abwanderung von einem Bereich in den anderen unterbunden. Wurde ein E-Mail-Account über das MDM konfiguriert gelten dieselben Regeln und E-Mailanhänge können nur in verwalteten Apps geöffnet werden.

Neben den verwalteten Apps werden verwaltete Bücher, Document Provider, Tastaturen und Domänen unterstützt.

16 https://help.apple.com/deployment/ios/#/apdf5b35aad2Sync
17 https://www.apple.com/de/business/programs/

Hinweis 1: Mit iOS 9 können Apps und deren Updates über MDM mittels VPP auch installiert werden, wenn der App-Store auf dem iPhone deaktiviert wurde.

Hinweis 2: Mit iOS 9 besteht die Möglichkeit, über ein MDM nicht verwaltete Apps in verwaltete Apps zu migrieren. Da es sich um vom Nutzer installierte Apps handelt, ist dieser über diese Änderung zu informieren, da seine privaten Daten nicht mehr mit seinen eigenen Apps ausgetauscht werden können.

Weitere Information zur „Managed Open-In“ siehe hier[18].

5.25 Application Data Encryption

Grundsätzlich sind alle Daten eines iPhones verschlüsselt gespeichert. Das hierfür benötigte Schlüsselmaterial ist in einem Hardwarebaustein fest eingebrannt. Die Frage ist, in welchem Zustand des Geräts auf die Daten zugegriffen werden kann, das heißt, wann das Schlüsselmaterial für die Entschlüsselung der Daten zur Verfügung steht. Apple definiert verschiedene Klassen, denen die Daten zugeordnet werden.

Complete Protection
Das Schlüsselmaterial steht zur Verfügung, wenn das Gerät entsperrt ist. Nach dem Sperren des Geräts wird das Schlüsselmaterial wieder vernichtet.

Protected Unless Open
Solange eine Datei geöffnet ist, steht ein individueller Dateischlüssel zur Verfügung. Wird die Datei geschlossen, wird auch der Schlüssel vernichtet. Diese Klasse wird beispielsweise für Downloads im Hintergrund verwendet.

Protected Until First User Authentication
Nach einem Reboot sind die Daten dieser Klasse bis zum ersten Entsperren nicht zugreifbar. Nach der ersten Benutzer-Authentisierung (über die Code-Sperre) bleibt das Schlüsselmaterial bis zum Herunterfahren im Speicher.

No Protection
Das Schlüsselmaterial steht bei eingeschaltetem Gerät ständig zur Verfügung. Sinn dieser Klasse ist im Prinzip nur die Funktion "Remote Wipe", bei der die Schlüssel im Bedarfsfall einfach gelöscht werden. Damit sind die Daten nicht mehr zugreifbar.

In iOS sind die Daten von Drittanbieter-Apps - bei Verwendung der Code-Sperre - bis zum ersten Unlock nicht zugreifbar. Das heißt, dass der Benutzer sich am Gerät mit der PIN erst authentifizieren muss, bevor die Daten zugreifbar sind.

Unabhängig davon haben Programmierer die Möglichkeit, Daten mithilfe dieser Schutzklassen zu sichern. Je nach Schutzbedarf sollte bei eigen-entwickelten Apps auf die Verwendung der geeigneten Schutzklasse geachtet werden.

5.26 Sicheres Löschen

Eine wichtige Frage im Rahmen des Life Cycle Management von iOS Geräten ist das sichere Löschen eines Endgerätes im Falle einer Außerbetriebsetzung oder eines Reparaturfalles. Grundsätzlich ist in beiden Fällen anzuraten zuvor ein Backup des Gerätes vorzunehmen, um die Daten auf einem neuen Gerät wieder herstellen zu können. Nähere Informationen hierzu liefert ein Artikel des Herstellers[19].

18 https://help.apple.com/deployment/ios/#/iorf4d72eded
19 http://support.apple.com/de-de/ht4946

Vor Außerbetriebnahme ist das iPhone sicher zu löschen. Gehen Sie hierzu in die *Einstellungen* des iOS und wählen Sie unter *Allgemein* die Option *Zurücksetzen*. Mit *Alle Inhalte und Einstellungen löschen* werden sämtliche Inhalte gelöscht. Da die Daten des Dateisystems verschlüsselt sind, reicht zum Löschen der Daten, das Schlüsselmaterial zu entfernen.

5.27 Device Enrollment Program / DEP

Das „Device Enrollment Program[20]", kurz DEP, bietet für Unternehmen die Möglichkeit, dass neue iPhones einem MDM Servern zugewiesen und somit automatisch verwaltet werden können, ohne das eine Interaktion mit der IT-Administration oder durch den Nutzer notwendig ist.

Dazu muss sich ein Unternehmen für das DEP-Programm registrieren[21] und autorisierte Handelspartner, über welche die Geräte bezogen werden, benennen. Der Handelspartner wird über eine sogenannte DEP-Reseller-ID identifiziert. Das Unternehmen benötigt eine DEP-Customer-ID.

Durch das DEP wird eine erhöhte Sicherheit für die Anwendung im Unternehmen erreicht. Einstellungen werden automatisch auf das iPhone ausgerollt und entsprechend der Compliance-Regeln umgesetzt. Ein Abweichen von diesem Prozess ist dem Nutzer nicht möglich, da selbst bei Zurücksetzen des iPhones der Prozess wieder von vorne beginnt. In diesem Sinne wird ähnlich der Aktivierungssperre auch ein erhöhter Diebstahlschutz erreicht, da das iPhone ohne Nutzerauthentifizierung nicht verwendet werden kann.

Weitere Information zu „Device Enrollment Program" im Support-Artikel des Herstellers[22].

Hinweis 1: Werden iPhones über das DEP entsprechend verwaltet, ist es nicht möglich, das iPhone über den Apple Configurator oder iTunes zu aktivieren.

Hinweis 2: Mit iOS 9 ist das iPhone erst betriebsbereit, wenn alle Konfigurationen auf das Gerät aufgespielt wurden. Zwischenzeitlich verweilt das iPhone im Setup Assistenten.

5.28 S/MIME

iOS verfügt über eine integrierte Unterstützung von S/MIME in iOS auf Basis von Zertifikaten. Unter iOS 7 werden sämtliche Mails des Postfaches verschlüsselt, sobald S/MIME aktiviert wurde. Ab iOS 8 hat der Nutzer die Möglichkeit bei jeder einzelnen Mail zu entscheiden, ob diese verschlüsselt werden soll oder nicht.

5.29 Touch ID

Alle aktuellen iOS Geräte verfügen über eine „Touch ID". Diese ermöglicht es dem Nutzer anstatt des Passwortes seinen Fingerabdruck für das Entsperren des Gerätes, Einkäufe in den Apple Stores oder, insofern vom App Entwickler integriert, die Öffnung von Apps, zu verwenden. Hierbei wird nicht der Fingerabdruck des Nutzers als Passwort verwendet. Der Nutzer muss ein Passwort hinterlegt haben um „Touch ID" aktivieren zu können.

Zur Erhöhung der Sicherheit wird vom iPhone dennoch das Passwort verlangt, wenn das iPhone neu eingeschaltet, das Gerät seit mehr als 48 Stunden nicht mehr verwendet, per Fernzugriff gesperrt, fünfmal kein autorisierter Fingerabdruck erkannt wurde, oder aber ein neuer Fingerabdruck hinterlegt werden soll. Insgesamt können bis zu 5 Fingerabdrücke hinterlegt werden.

20 https://www.apple.com/de/business/programs/
21 http://deploy.apple.com/
22 https://www.apple.com/de/business/docs/VPP_Business_Guide_DE_Aug14.pdf

Biometrische Sensoren können grundsätzlich getäuscht werden, wie dies bei „Touch ID“ schon der Fall war. Der Aufwand einer qualifizierten Täuschung ist dennoch sehr hoch und ein entsprechend hochwertiger Fingerabdruck muss vorhanden sein. Dennoch bietet die Verwendung von „Touch ID“ eine höhere Akzeptanz komplexere Passwörter oder überhaupt einen PIN-Code zu verwenden. Außerdem kann durch Verwendung von „Touch-ID“ in öffentlichen Bereichen kein PIN-Code mitgelesen werden.

Grundsätzlich sollte von einem Unternehmen geprüft werden, ob das Restrisiko bei Verwendung von solchem Mechanismen getragen werden kann. Die Verwendung von „Touch ID“ kann unterbunden werden.

5.30 Siri

Apples Sprachassistent Siri ist zentraler Bestandteil von iOS. Bereits bei der initialen Konfiguration wird der Nutzer gefragt, ob diese Funktion aktiviert werden soll. Mittels langem Drücken des Home Buttons kann Siri aufgerufen werden, um beispielsweise Textnachrichten zu erstellen oder aktuelle Termine abzufragen. Siri erhält dabei weitreichenden Zugriff auf zentrale Daten, wie Mail, Nachrichten, Kontakte, Kalender und weitere. Siri ist zudem in der Standardkonfiguration im Sperrbildschirm verfügbar.

Zur Erkennung der Sprache werden Teile der Kommandos an Apple-Server zur Analyse geschickt, um diese auf dem iPhone ausführen zu können. Hierbei werden laut Apple jedoch keine Nutzerdaten vom iPhone selbst übertragen.

In der aktuellen iPhone Generation iPhone 6s und iPhone 6s plus kann Siri auch mittels des Kommandos „Hey Siri“ ohne Betätigung des Home-Buttons aktiviert werden. Das iPhone reagiert auf das Kommando und aktiviert Siri zur Kommandoeingabe. Diese Komfortfunktion kann aus Sicherheitssicht kritisch sein. Bei älteren iPhone Modellen ist ein analoges Verhalten möglich, wenn das iPhone am Strom angeschlossen wird. In beiden Fällen muss die Funktion explizit aktiviert werden.

Trotz der Annehmlichkeiten, die Siri mitbringt, empfiehlt das BSI für die berufliche Verwendung von iPhones auf Siri zu verzichten oder zumindest Siri für den Sperrbildschirm und die Funktion „Hey Siri“ zu deaktivieren. Die Einstellungen zu Siri finden sich unter *Einstellungen - Allgemein - Siri*.

5.31 TLS 1.2

iOS 9 setzt durchgehend auf die empfohlene Version von TLS 1.2 zur Datenverschlüsselung. Zur Erhöhung der Datensicherheit fordert Apple ab iOS 9 TLS 1.2 als Mindeststandard. Das kann zur Folge haben, dass Safari oder App Store Apps in Verbindung mit einer älteren Version von TLS einen Dienst nicht mehr erwartungsgemäß aufrufen.

Entwickler, die in den Apps weiterhin TLS 1.1 verwenden wollen, können dazu Ausnahmen definieren.

5.32 Suche / Spotlight-Suche

Apple bietet unter iOS verschiedene Möglichkeiten an, Inhalte zu suchen. Dabei handelt es sich um die sogenannte Schnellsuche (Spotlight), Vorschläge von Siri und Siri selbst. (Unabhängig davon kann mit Safari über eine klassische Suchmaschine gesucht werden.)

Das generelle Suchverhalten von Spotlight kann unter *Einstellungen - Allgemein - Spotlight-Suche* beeinflusst werden. Hier können Sie die Vorschläge von Siri deaktivieren sowie auswählen, welche Apps in die Suchen einbezogen werden sollen. Die Verwendung von Spotlight sollte

auf eine lokale Suche beschränkt sein. Schalten Sie dazu in *Einstellungen - Allgemein - Spotlight-Suche* Bing-Suchergebnisse sowie Spotlight-Vorschläge ab.

Zudem können Suchanfragen über Spotlight und Safari auch ortsbezogene Ergebnisse liefern. Um dies zu verhindern, müssen Safari- & Spotlight-Vorschläge unter *Einstellungen - Datenschutz - Ortungsdienste - Systemdienste* deaktiviert werden.

Weitere Informationen dazu finden Sie im Apple-Supportartikel[23].

6 Apps

Parallel zu den allgemeinen Einstellungen des Betriebssystems müssen natürlich auch die Apps in sicherheitstechnischer Hinsicht betrachtet werden. Primär geht es dabei um die "nativen" Apps, die in die iOS-Versionen integriert sind.

6.1 Mail

iOS bietet Assistenten für die Einrichtung von E-Mail-Konten für Postfächer in der iCloud, in Microsoft Exchange, Gmail, Yahoo, AOL und Outlook an. Darin sind verschiedene Felder, beispielsweise die Servernamen, bereits vorbelegt. Daneben gibt es einen allgemeinen Einrichtungs-Assistenten für andere E-Mail-Serverdienste.

Die Einrichtungs-Assistenten für die vordefinierten Serverdienste richten automatisch verschlüsselte Übertragungsprotokolle ein. Achten Sie bei dem Assistenten für sonstige E-Mail-Server selbst auf die Verwendung der verschlüsselten Protokolle (POP3S, IMAPS, SMTPS).

Über Profile kann eingeschränkt werden, dass Mails von Unternehmensaccounts nicht über einen anderen Account weitergeleitet werden können, um die Datenabwanderung zu unterbinden.

6.2 Internet-Browser

Der Internet-Browser ist sicherlich auch bei mobilen Endgeräten eine der am meisten verwendeten Apps. Verwenden Sie einen sicheren Internet-Browser, der innerhalb der Browser-Tabs nach dem Sandbox-Prinzip arbeitet. Dazu können Sie den in iOS integrierten Browser "Mobile Safari" verwenden. Achten Sie bei der Verwendung von sonstigen Browsern auch auf das Sandbox-Verfahren.

Der Browser verfügt über einen "Privatmodus", in dem die aufgerufenen Webseiten nicht zum "Verlauf" (Historie) hinzugefügt werden. Cookies, Lesezeichen sowie Leselisten werden nicht gespeichert, usw. Beim Chrome Browser heißt dieser Modus "Incognito-Tab", bei Mobile Safari "Privates Surfen".

Verwenden Sie diese Modi, wenn Sie keine Spuren ihres Surf-Verhaltens hinterlassen wollen und Ihre Eingaben und Downloads nicht temporär gespeichert werden sollen.

Internet-Browser auf mobilen Endgeräten haben im Vergleich zu Browsern auf Desktop Computern keinen effektiven Schutz vor Phishing-Seiten. Dies liegt hauptsächlich an dem großen Update-Bedarf der Phishing-Seiten-Datenbank. Eine Schutzmöglichkeit besteht darin, einen zentralen Proxy-Server einzurichten, über den der Internetverkehr geleitet wird. Auf dem Proxy wird dann ein Phishing-Filter eingerichtet.

Dennoch hat der Browser von iOS einen einfachen Phishing-Filter, der eingeschaltet werden sollte (Einstellungen - Safari - Betrugswarnungen).

23 https://support.apple.com/de-de/HT201285

6.3 3rd-Party-Apps / Drittanbieter-Apps

Apps von Drittanbietern werden bei Apple ausschließlich über den „App Store" vertrieben. Einzige Ausnahme sind die eigen-entwickelten sogenannten Enterprise-Apps, die auch über einen „Enterprise App Store" (in Verbindung mit einer MDM-Lösung) verteilt werden können.

Wählen Sie 3rd-Party-Apps für berufliche Belange mit Bedacht aus. Wenn mit diesen Apps dienstliche Daten verarbeitet werden sollen, sollten die Kommunikationskanäle verschlüsselt sein. Außerdem dürfen die verarbeiteten Daten nur auf dem Firmenserver, oder direkt in der App, also durch die Sandbox geschützt, gespeichert werden. Achten Sie daher darauf, dass keine Daten in der Cloud (iCloud oder auch andere Clouddienste) gespeichert werden.

6.4 Enterprise-Apps

Nicht alle Anforderungen einer Organisation können durch „App Store"- Apps abgedeckt werden. Dabei kann es sich um spezielle Prozesse oder sensible Daten handeln. Zu diesem Zweck bietet Apple das sogenannte „iOS Developer Enterprise Programm", kurz iDEP an. Hiermit kann eine Organisation Apps entwickeln und mit einem iDEP Zertifikat signieren, um diese unter iOS ausführbar zu machen. Die Apps können den betrieblichen Bedingungen entsprechend entwickelt werden und werden unabhängig vom „App Store" bereitgestellt. Dies kann entweder durch ein MDM oder aber über eine Portalseite geschehen. Die Bereitstellung der Enterprise- oder auch In-house- Apps darf nur an Organisationsmitglieder erfolgen. Beachten Sie daher die aktuell gültigen Lizenzbedingungen zum Programm.

Insofern ein Nutzer die entsprechenden Zertifikate noch nicht auf seinem iPhone hinterlegt hat, muss er das Zertifikat zunächst als vertrauenswürdig akzeptieren. Erst dann ist die App lauffähig. Der Nutzer erhält bei erstmaligem Start der App einen Warndialog, den er bestätigen kann. Alternativ kann dies unter *Einstellungen - Allgemein - Profile* vorgenommen werden. Wurde ein Zertifikat als vertrauenswürdig akzeptiert, sind alle weiteren Apps, welche mit demselben Zertifikat signiert wurden, automatisch lauffähig.

Da eine „Enterprise App" ohne den „App Store" auf jedem iPhone installiert werden kann, können manipulierte - mit einem iDEP Zertifikat signierte - Apps auch über unsichere Quellen verteilt werden. Mit iOS 9 kann die Installation von organisationsfremden „Enterprise Apps" auf Basis ihrer Zertifikate verhindert werden. Deaktivieren Sie hierzu die Einschränkung *Einstufen neuer Entwickler firmenweiter Apps als vertrauenswürdig erlauben*. Anschließend hat der Nutzer nicht mehr die Möglichkeit, die Zertifikate fremder Enterprise-Entwickler zu akzeptieren und nur die hausinternen Apps sind lauffähig.

7 iOS Einstellungen / Settings

In den vorangegangenen Kapiteln wurden bereits mehrfach Konfigurations-Menüs von iOS genannt. Diese befinden sich alle in der "Einstellungen"-App. Bis auf einige Ausnahmen besteht die Möglichkeit, die Konfigurationen lokal in der "Einstellungen"-App zu machen, den bereits beschriebenen „Apple Configurator" zu verwenden sowie eine „Mobile Device Management"-Lösungen ein zusetzen.

Viele Einstellmöglichkeiten sind in der "Einstellungen-App" einfach zu finden und selbsterklärend, wie beispielsweise das Menü Einstellungen - WLAN. Andere Menüs sind mitunter komplexer und liegen teilweise in Untermenüs versteckt. An dieser Stelle sollen die zentralen Menüs Einstellungen - *Datenschutz* und Einstellungen - *Allgemein - Einschränkungen* sowie die Einstellungen zur Mitteilungszentrale beschrieben werden.

7.1 Datenschutz

Über das Menü *Einstellungen - Datenschutz* können Sie steuern, welche Apps auf Ihre persönlichen Daten (Kontakte, Kalender, Fotos, usw.) zugreifen dürfen. Sie sind in verschiedene Kategorien unterteilt. Beispiel: Ortungsdienste. In diesem Menüpunkt werden alle installierten Apps aufgelistet, die auf die Ortungsdienste (GPS und Netzwerkstandort) zugreifen wollen. Sie können für jede App entscheiden, ob sie dieses Recht bekommen soll oder nicht.

In der Vergangenheit kam es immer wieder vor, das Apps den Zugriff auf persönliche Daten missbraucht haben, um beispielsweise an Kontaktdaten zu gelangen. Gehen Sie nach dem Minimalprinzip vor und stellen Sie sich bei jeder Kategorie kritisch die Frage, ob die angezeigten Apps tatsächlich das entsprechende Recht zum Zugriff auf diese persönlichen Daten bekommen sollen. Im Zweifel sollten Sie das Recht verweigern. Apps für iOS müssen so programmiert sein, dass sie bei einem verweigerten Recht im Funktionsumfang zwar eingeschränkt sind, aber weiterhin funktionieren, also nicht abstürzen.

Zugriffsberechtigungen zu den personenbezogenen Daten werden bei der Installation von neuen Apps abgefragt. Kontrollieren Sie nach der Installation neuer Apps, ob Ihre Entscheidung zum Zugriff richtig konfiguriert wurde.

7.2 Einschränkungen

Das Menü E*instellungen - Allgemein - Einschränkungen* wird durch einen vierstelligen nummerischen PIN-Code geschützt. Administratoren sollten hier einen PIN-Code verwenden, der nicht oder nur bei Bedarf an den Benutzer weitergegeben wird. Alternativ lässt sich ab iOS 8 die manuelle Konfiguration der Einschränkungen auf „Supervised Devices“ pro Profile deaktivieren.

Im Bereich *Erlauben* können bestimmte - von Apple vorgegebene - Apps beziehungsweise Dienste erlaubt oder verboten werden; voreingestellt ist alles erlaubt. Legen Sie hier insbesondere fest, ob der Benutzer den App Store benutzen, Apps löschen, aber auch, ob er den iCloud-basierten Spracherkennungsdienst "Siri" verwenden darf.

Im Bereich *Zulässiger Inhalt* werden zunächst die Altersbeschränkungen für Medieninhalte und Apps konfiguriert. Hier wird aber auch festgelegt, ob der Benutzer sogenannte In-App-Käufe tätigen darf. Apps von Drittanbietern werden häufig in einer Basisversion kostenlos angeboten, interessante Funktionen soll der Benutzer dann zusätzlich erwerben. Bei Geräten, die ein Administrator vorkonfiguriert, wird diese Funktion nicht benötigt und sollte deaktiviert werden.

In dem Menü findet sich auch das Menü Datenschutz (s.o.) wieder, so dass die dort gemachten Einstellungen gesperrt werden können. Das bedeutet, dass der Benutzer die gewählten Einstellungen nicht verändern kann und neue Apps die gesperrten Funktionen nicht nutzen können. Bei der Installation wird dann eine Warnmeldung ausgegeben. Dies führt allerdings häufig zu Unverständnis bei den Benutzern und Nachfragen beim Support, insbesondere dann, wenn Sie dem Benutzer den „App Store” erlauben - Apps aufgrund der hier gemachten Einschränkungen aber nicht vollständig funktionieren. Legen Sie in den eingangs genannten Security Policies fest, welche Funktionalitäten gesperrt werden und kommunizieren Sie diese deutlich an die Benutzer.

Hinweis: Bei den unterschiedlichen iOS-Versionen sind die Inhalte in dem Menü Allgemein - Einschränkungen durchaus unterschiedlich. Bei neueren Versionen kommen neue Einträge hinzu, teilweise sind die Einträge aber auch umsortiert. Außerdem können Einträge in Menüs unveränderlich ausgegraut sein, wenn eine MDM-Lösung eingesetzt wird.

7.3 Mitteilungszentrale / In der Zentrale / Notification Center

Ein weiterer Menüpunkt in der "Einstellungen"-App ist Mitteilungen ("In der Zentrale", "Notification Center"). Mitteilungen werden in der Mitteilungszentrale - den Touch-Screen von oben nach unten streichen - angezeigt. Sie können aber auch im Sperrbildschirm dargestellt werden. In dem Menüpunkt können Sie konfigurieren, welche Apps Mitteilungen anzeigen. In den Untermenüs der einzelnen Apps legen Sie dann fest, ob Mitteilungen im Sperrbildschirm angezeigt werden sollen. Schalten Sie diese Funktion für solche Apps ab, die berufliche Daten mitteilen könnten.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an info@cyber-allianz.de gesendet werden.

Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IM UNTERNEHMEN

Android

Konfigurationsempfehlung auf Basis betriebssystem-eigener Mittel für eine Nutzung mit erhöhter Sicherheit

1 Einleitung

Android ist ein weitgehend quelloffenes Betriebssystem für mobile Geräte, wie Smartphones und Tablet-Computer, das von der "Open Handset Alliance"[1] unter der freien Apache-Lizenz sowie der GNU General Public License (GPL) entwickelt wird. Federführend ist dabei die Firma Google. Basis ist ein Linux-Kernel, auf dem das Betriebssystem Android als Mittelschicht läuft. Darauf werden in einer kontrollierten Ablaufumgebung Applikationen (Apps) von Drittanbietern installiert und ausgeführt. Das Betriebssystem verfolgt dabei mit dem sogenannten *Sandbox-Prinzip* den Ansatz der kontrollierten Trennung von Apps vom Betriebssystem und auch von App zu App.

Aufgrund der Quelloffenheit haben Gerätehersteller die Möglichkeit, die Android-Mittelschicht an eigene Bedürfnisse anzupassen und sie um – z. T. proprietäre – Komponenten zu erweitern. Einige Hersteller unterstützen so Besonderheiten der verwendeten Hardware, andere Hersteller ändern beispielsweise die komplette Bedienoberfläche in ihren Geräten. Diese Veränderungen beziehungsweise Ergänzungen führen in der "Android-Landschaft" zu einer mittlerweile unüberschaubaren Vielzahl von angepassten Android-Versionen (Android-Fragmentierung), die durch den Einsatz von Android auf verschiedenartigen Geräteklassen über klassische Smartphones hinaus, z. B. Uhren, Unterhaltungssysteme und insbesondere Tablets, enorm an Komplexität gewinnt. Die Pflege dieser angepassten Versionen sowie die Versorgung der Geräte mit Betriebssystem-Updates wird von den Herstellern allein schon in dem schnelllebigen Smartphone-Markt nur unzureichend geleistet. Neue Betriebssystem-Versionen, die von Google herausgegeben werden, müssen dann durch die Gerätehersteller, wiederum an die eigenen Bedürfnisse angepasst werden. Aufgrund der sehr schnellen Produktzyklen im Bereich mobiler Endgeräte kann man oft beobachten, dass ein neues Android-Gerät, früher auf dem Markt erscheint, als dass es neue und angepasste Betriebssystem-Updates für die etablierten Geräte gibt.

Durch den hohen Grad der Fragmentierung der Android-Landschaft ist es unmöglich, Konfigurationsempfehlungen für alle möglichen Android-basierten Geräte zu geben. Die vorliegende Empfehlungen beschränken sich daher auf die von Google herausgegebene Grundversion von Android. Es soll gezeigt werden, welche betriebssystemeigenen Mechanismen zur Verfügung stehen und wie diese mit geeigneten Maßnahmen zur Erhöhung der Datensicherheit beitragen. Viele Empfehlungen sind jedoch allgemeingültig auch auf angepassten Android-Versionen anderer Hersteller sowie weitere Geräteklassen anwendbar.

1 http://www.openhandsetalliance.com/

Gefährdungen durch konzeptionelle Schwächen, systembedingte Mängel oder ausgenutzte Schwachstellen im Betriebssystem können mit den empfohlenen Konfigurationen und Maßnahmen höchstens gemildert, jedoch nicht vollständig beseitigt werden. Solchen Gefährdungen kann im PC-Bereich z. B. unter Microsoft Windows mit zusätzlichen Schutzprogrammen begegnet werden, die Angriffe tief im Betriebssystem auf Kernel- und Prozessebene abwehren. Im Betriebssystem Android unterliegen Schutzprogramme jedoch den gleichen Einschränkungen wie "normale" Apps von Drittanbietern und sind demzufolge nicht in der Lage, Verteidigungslinien „vor der Schadsoftware“ aufzubauen und so ein vergleichbares Schutzniveau zu gewährleisten. Mehr dazu im Kapitel "Schutzprogramme".

Für einen sicheren Einsatz im Unternehmensumfeld mit einem hohen und sehr hohen Schutzbedarf reichen die empfohlenen Konfigurationen alleine nicht aus. Ohne weitere Maßnahmen sollten auf Android-Geräten **keine vertraulichen Daten verarbeitet werden**. Solche Maßnahmen werden im nächsten Kapitel "Einsatzszenarien" beschrieben.

2 Einsatzszenarien

Bei der Verwendung von Smartphones und Tablets für berufliche Zwecke sind grundsätzlich drei Einsatzszenarien denkbar:

1. Der Gebrauch der im Betriebssystem integrierten Apps (Kontakte, Kalender, E-Mail-Client, Webbrowser) und/oder vergleichbaren Apps von Drittanbietern. Dabei kommt es oft zu einer Vermischung von geschäftlicher und privater Benutzung.
2. Sämtliche geschäftlichen Belange werden in einer abgeschlossen, gesicherten Einheit bearbeitet, dem sogenannten "Secure Container". Es handelt sich dabei um Drittanbieter-Apps. Das Smartphone kann außerhalb dieses Containers normal, das heißt ohne spezielle, restriktive Konfiguration verwendet werden.
3. Private und geschäftliche Bereiche werden als unterschiedliche virtuelle Maschinen auf einem Gerät zu betrieben. Hierbei werden der private und geschäftliche Bereich nicht auf Anwendungsebene, sondern auf Betriebssystemebene getrennt. Ein Datenaustausch zwischen beiden virtuellen Maschinen ist nur über die tiefer liegende Virtualisierungsschicht in Form des Hypervisors (auch Virtual Machine Monitor, VMM genannt) möglich.

Das BSI empfiehlt, sofern aus wirtschaftlichen oder organisatorischen Gründen keine umfassende Lösung verwendet werden kann, die eine Trennung geschäftlicher und privater Bereiche mittels Virtualisierungstechniken umsetzt, mindestens den Einsatz des Secure Containers, weil damit Wechselwirkungen zwischen privater und geschäftlicher Verwendung des mobilen Endgerätes verhindert werden und alle geschäftlichen Daten sicher gespeichert werden können. Eine ungeregelte Nutzung der im Betriebssystem integrierten Apps sowie die Vermischung geschäftlicher und privater Daten ist in jedem Fall zu vermeiden. Siehe dazu auch die Empfehlungen zur Cyber-Sicherheit "Mobile Device Management"[2] der Allianz für Cyber-Sicherheit.

Für den Fall, dass dieser Empfehlung nicht gefolgt werden kann, werden in diesem Dokument Konfigurationsempfehlungen für den Gebrauch der "nativen" Apps (Szenario 1) gegeben.

3 Sicherheitsrichtlinien

Bevor mobile Endgeräte in eine Unternehmensstruktur eingebunden werden können, müssen klare Regeln für die Integration festgelegt werden. Mit diesen Sicherheitsrichtlinien, den sogenannten Security Policies, werden u. a. die Rahmenbedingungen bezüglich Auswahl der Geräte, Auswahl der Daten, die auf den Geräten verarbeitet werden dürfen, Einschränkungen der Benutzer, Limitierung der Möglichkeiten der Geräte (Hardware wie Software), festgelegt. Die BSI

2 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_052.html

Publikation „Überblickspapier Smartphone“[3] liefert dazu weitere Aspekte.

Neben den Sicherheitsrichtlinien ist auch eine Betriebsvereinbarung mit einer klaren Darstellung der Rahmenbedingungen für die Verwendung der mobilen Endgeräte notwendig.

Die Durchsetzung der technischen Anforderungen der Sicherheitsrichtlinien ist bei der steigenden Anzahl der mobilen Endgeräte nur noch mit entsprechenden Tools erreichbar. Dazu wird eine Mobile Device Management-Lösung (MDM) verwendet.

4 Aktualisierungen

Durch die Popularität des Betriebssystems Android und den damit verbundenen Marktanteilen ist die Wahrscheinlichkeit relativ hoch, dass Schwachstellen gefunden und aktiv ausgenutzt werden. Daher ist die zeitnahe Verfügbarkeit sowie das Einspielen von Updates beim Auftreten von Schwachstellen wichtig. Es sollten nur Geräte von solchen Herstellern verwendet werden, die eine nachvollziehbare und schnelle Updatepolitik haben und ihre Geräte langfristig mit Aktualisierungen versorgen[4]. Geräte, die keine Betriebssystem-Updates mehr erhalten, sollten ausgesondert werden. Das Restrisiko für die Ausnutzung gegebenenfalls bestehender Sicherheitslücken wird entsprechend größer.

Neue Versionen von Apps sollten vor der Installation auf neue oder veränderte Funktionalitäten geprüft werden. Man kann sich über neue Versionen von Apps benachrichtigen lassen. Die Einstellungen dazu werden in der *Google Play* App im Menü Einstellungen vorgenommen. Neuen Versionen können auch Veränderungen in den Berechtigungen (Permissions) aufweisen. Lesen Sie dazu auch das Kapitel "Permissions".

Automatische App-Updates sollten deaktiviert werden (Google *Play Store* App - Einstellungen - 'Keine automatischen App-Updates').

5 Bluetooth und NFC

Nicht benötigte Schnittstellen sollten grundsätzlich abgeschaltet werden. Beispiele hierfür könnten sein: Bluetooth oder NFC.

6 WLAN und Mobilfunknetze

Smartphones sind nur sinnvoll einsetzbar, wenn sie Zugang zum Internet haben. Die derzeit hauptsächlichen Kommunikationskanäle sind dabei das Mobilfunknetz des Providers sowie im Nahbereich WLAN. Problematisch sind unverschlüsselte WLANs, etwa in öffentlichen Plätzen, in Hotel-WLANs oder großen Handelsketten. Hier kann praktisch jeder den Netzwerkverkehr mitlesen.

Generell sollte die WLAN-Funktion in unsicheren – das heißt unverschlüsselten sowie fremd kontrollierten – Umgebungen deaktiviert werden. Ebenso, wenn sie überhaupt nicht gebraucht wird.

Die Kommunikation außerhalb eines WLAN geschieht über das Mobilfunknetz des Providers mittels der Standardprotokolle GSM, UMTS (3G) und LTE (4G). GSM gilt als unsicher und kann mit wenig Aufwand abgehört werden[5]. Mit UMTS wurden verbesserte Authentifizierungs-Mechanismen eingeführt, Sicherheitsprobleme sind aber auch bei dieser Technik nicht ausgeschlossen[6]. Demgegenüber verkürzt der neuste Standard (LTE) die Akkulaufzeit etwas mehr. Dieser Nachteil sollte jedoch aufgrund der besseren Absicherung der Kommunikation in Kauf genommen werden. LTE basiert vollständig auf einem IP-Übertragungssystem. Die Datenüber-

3 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzUeberblick/itgrundschutzUeberblick_node.html
4 The state of Android updates: http://arstechnica.com/gadgets/2014/08/the-state-of-android-updates-whos-fast-whos-slow-and-why/
5 BSI Dokument "Öffentliche Mobilfunknetze und ihre Sicherheitsaspekte" (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Oeffentl-Mobilfunknetze.pdf)
6 Lücke im SS7 bei UMTS: http://heise.de/-2503376

tragung erfolgt also (wie schon im Internet allgemein üblich) datenpaketorientiert auf Basis des IP-Protokolls. Für alle Verbindungen wird AES als Verschlüsselung eingesetzt.

Bei einigen Android-basierten Geräten kann der unsichere Standard GSM sogar deaktiviert werden, was irreguläre Abhörmaßnahmen auf der Luftschnittstelle erschwert.

In allen ungesicherten Netzen sollten die Daten durch den Einsatz eines Virtual Private Networks[7] (VPN) verschlüsselt werden. Die Verwendung von VPNs ist jedoch mit Aufwand verbunden, da die Gegenseite der Kommunikationsstrecke ebenso das VPN unterstützen muss. Im geschäftlichen Bereich ist dieser Aufwand aber in jedem Fall gerechtfertigt.

7 Rooten

Beim sogenannten Rooten wird das Sicherheits-Konzept von Android außer Kraft gesetzt. Apps können mit Root-Berechtigung ablaufen und haben so alle Möglichkeiten, das Betriebssystem zu kontrollieren.

Im Unternehmenseinsatz sollten Android-basierte Geräte nicht "gerootet" sein.

Daneben gibt es für eine Vielzahl von Android-basierten Geräten alternative Android-Versionen, sogenannte Custom ROMs, die nicht vom Hersteller selbst stammen. Als Beispiel sei das weit verbreitete CyanogenMod[8] genannt. Mit diesen Custom-ROMs erhält der Benutzer in der Regel mehr Möglichkeiten der Einflussnahme auf das Betriebssystem. Zu beachten ist, dass durch die Manipulation des originalen Betriebssystems die Herstellergarantie möglicherweise verloren geht. In jedem Fall wird der Nachweis, dass ein aufgetretener Schaden nicht durch die Betriebssystemmanipulation hervorgerufen wurde, schwierig. Custom-ROMs sollten für geschäftliche Zwecke nicht eingesetzt werden.

8 App-Stores

Im Auslieferungszustand ist üblicherweise nur Googles eigener App-Store über die App *Google Play* erreichbar. Apps aus anderen Quellen können nicht installiert werden. Dies verhindert eine Systemeinstellung (*Einstellungen - Sicherheit - Unbekannte Herkunft*). Wird diese Einstellung deaktiviert, können Apps aus beliebigen Quellen installiert werden. Dies können alternative App-Stores sein, Internet-Seiten, auf denen ein Installationspaket einer App verlinkt ist, aber beispielsweise auch ein solches Paket im Anhang einer E-Mail. Grundsätzlich gilt, dass Apps nicht ohne Nutzerinteraktion, nämlich durch Bestätigung der App-Berechtigungen, installiert werden können.

Wie im Kapitel "Schutzprogramme" erläutert wird, bestehen schädliche Apps (Malware) bei Android technisch gesehen aus vollkommen normalen Programmen, d. h. Apps, die der Benutzer selbst installiert. Diese maliziösen Apps kommen fast ausschließlich aus "unsicheren Quellen", App-Stores, die keine ausreichende Sicherheitskontrolle haben oder Installationspakete aus sonstigen Quellen. Im Gegensatz dazu wird der Play Store von Google überwacht, gegenüber den sonstigen Quellen sind hier bisher kaum Fälle bekannt geworden.

Das BSI empfiehlt, keine Apps aus unsicheren und nicht vertrauenswürdigen Quellen zu installieren. Ob und welche Apps installiert werden dürfen, sollte durch eine spezifische Unternehmens-Richtlinie geregelt werden.

Mit der Systemeinstellung *Einstellungen - Sicherheit - Unbekannte Herkunft* werden aber auch alternative, seriöse App-Stores deaktiviert. Als ein Beispiel für eine ebenfalls professionell betreute Alternative zu Google Play sei der Amazon-App-Store genannt. Bei diesem werden, wie auch bei Google Play, die von der ENISA empfohlenen Maßnahmen zur Absicherung von App-Stores[9] umgesetzt.

7 http://de.wikipedia.org/wiki/Virtual_Private_Network
8 http://www.cyanogenmod.org/
9 http://www.enisa.europa.eu/media/press-releases/app-store-security2013-the-five-lines-of-defence-new-report-by-eu-cyber-security-agency-enisa

Das BSI empfiehlt, die Option abzuschalten und für Apps aus solchen App-Stores nur im Bedarfsfall kurzfristig einzuschalten.

9 Apps verifizieren

Google bietet mit der Option *Einstellungen - Sicherheit - Apps verifizieren* die Möglichkeit, Apps vor der Installation mithilfe einer Reputationsdatenbank auf schädliche Apps zu prüfen. Dies betrifft Apps aus unbekannten Quellen. Zudem sucht der Google-Dienst dann regelmäßig auf dem Gerät nach schädlichen Apps. Werden Apps als schädlich erkannt, wird eine entsprechende Warnung angezeigt und die Installation abgebrochen.

Zu beachten ist, dass *Apps verifizieren* ein Cloud-Dienst ist und Daten über die Apps sowie über das Gerät an Google gesendet werden[10].

Im Unternehmens-Einsatz ist es empfehlenswert, die zu verwendenden Apps vorab von einem unabhängigen Prüfinstitut tiefgehend auf mögliche schädliche Funktionalitäten untersuchen zu lassen.

Die Option *Apps verifizieren* ist eine der effektivsten Schutzmaßnahmen gegen schädliche Apps – Das BSI empfiehlt die Nutzung daher.

10 Schutzprogramme

Schädliche Apps im Android-Umfeld sind Apps, die neben gewollten, sinnvollen auch ungewollte, bösartige Funktionen enthalten. Es handelt sich dabei meist nicht um Programme, die sich tief im Betriebssystem einnisten, wie z. B bei Standard Desktop-Computer, sondern um Apps, die der Benutzer (oder das Unternehmen) selbst installiert. Meist handelt es sich bei 'infizierten' Apps um Programme aus unsicheren Quellen.

Betriebssysteme, wie Android, sind über die Rechtestruktur für Apps verhältnismäßig gut abgeschottet. Das Sandbox-Prinzip verhindert sowohl den unkontrollierten Zugriff auf Daten außerhalb der Ablaufumgebung als auch den Zugriff von außen auf die App.

Derzeitige Schutzprogramme für mobile Endgeräte erkennen Malware-Apps anhand von statischen Signaturen. Eine auf Desktop-Systemen eingesetzte echte Hintergrundüberwachung der laufenden Prozesse, die für eine gute Schutzwirkung notwendig ist, ist auf mobilen Betriebssystemen, wie Android und iOS, für Drittanbieter-Apps nicht möglich. Beim Virentest findet demnach eine Prüfung statt, ob eine App in einer Malware-Datenbank enthalten ist – Auch hierbei, wie bei Google, als Cloud-Dienst. Dieser Vorgang geschieht vor der Installation der App automatisch, kann aber auch auf alle bereits installierten Drittanbieter-Apps angewendet werden.

Schutzprogramme (AV-Apps) bieten oft neben der Erkennung von Malware weitere Funktionen, wie zum Beispiel Diebstahlschutz, "Parental Control" (Kinderschutz), Verschlüsselung, "Safe Browsing" (Blockieren von unsicheren Websites), usw.

Aus Sicht des BSI ist Virenschutz auf mobilen Endgeräten aus grundsätzlichen Erwägungen zurzeit nicht erforderlich. Die von Google im offiziellen Play Store umgesetzten Mechanismen sowie die ohnehin vor einer Verteilung über MDM vorzunehmenden Prüfungen sind in der Lage, ein hinreichendes Schutzniveau zur Abwehr von Schadprogramm zu gewährleisten. Zudem sind am Markt verfügbare Virenschutzlösungen mit technischen Einschränkungen verbunden, insbesondere erfolgt wie oben beschrieben keine Überwachung im Hintergrund. Lediglich für Nutzer, die Apps auch aus alternativen Quellen beziehen oder die die oben genannten Zusatzfunktionen nutzen wollen, können AV-Apps neben dem Google-Dienst *Apps verifizieren* eine sinnvolle Ergänzung darstellen. Eine Übersicht über Android-Sicherheits-Apps liefern die einschlägigen Testinstitute, wie beispielsweise AV-TEST.

10 https://support.google.com/accounts/answer/2812853?hl=de

Bei der ausschließlichen Nutzung von Apps aus vertrauenswürdigen, sicheren App-Stores sowie geprüften Apps, kann zurzeit auf zusätzliche AV-Programme verzichtet werden.

11 Datenschutz und Privatsphäre

Der Verlust von Daten und der Privatsphäre stellt ein großes Problem für den Benutzer dar. Die Erfassung und Auswertung von Nutzerdaten (Kontakte, Geopositionen, Surfverhalten, E-Mail-Inhalte usw.) ist häufig intransparent und nur schwer nachvollziehbar.

11.1 Permissions

Permissions sind die Berechtigungen, die eine App im Android-Betriebssystem hat. Mit Berechtigungen kann eine App auf Objekte außerhalb der eigenen Sandbox zugreifen. Beispiele sind *Kontakte lesen oder Zugriff auf Mikrofon, Kamera oder Geopositionsdaten.* Es gibt Einzel- und Gruppenberechtigungen, unterteilt in kritische, unkritische und systemrelevante Berechtigungen.

Die Berechtigungen werden dem Benutzer vor der Installation einer App angezeigt und er muss sie explizit bestätigen. Er kann nur alle Berechtigungen gleichzeitig bestätigen. Verweigert er das, wird die App nicht installiert.

App-Berechtigungen sollten kritisch geprüft werden. Dies ist die einzige Einflussmöglichkeit, die ein Anwender hat. Im Zweifelsfall sollte er eine App nicht installieren.

Weitere Informationen zu Android-Berechtigungen findet man auf BSI-FUER-BUERGER[11].

11.2 Cloud-Dienste

Aus Sicht des Datenschutzes sollte sorgfältig abgewogen werden, welche (persönlichen oder geschäftlichen) Daten wo verarbeitet und gespeichert werden. Eine Vielzahl von Apps verwenden externe Dienste und Speicherkapazitäten für diese Aktionen. Insbesondere die Speicherkapazitäten und die Möglichkeit der Synchronisation der Daten über mehrere Geräte sind bei den Benutzern beliebt. Oft werden solche Dienste verwendet, ohne dass den Benutzern klar ist, dass es sich dabei um Cloud-Technik handelt und wichtige Daten extern gespeichert werden. Nutzer sollten bei der Auswahl von Apps darauf achten, ob die Daten der App lokal oder in der Cloud gespeichert werden.

11.3 Backups

Backups sind Sicherheitskopien, aus denen die Nutzerdaten im Bedarfsfall wieder hergestellt werden können. Diese Daten sollten nur lokal gespeichert werden und zusätzlich verschlüsselt sein. Die Ablage von Nutzerdaten in Cloud-Speichern oder die automatische Synchronisation zwischen Mobilgerät und Cloud-Speicher stellt keine ausreichende Sicherung der Daten dar. Nutzer müssen bei solchen Diensten damit rechnen, dass diese Daten unverschlüsselt vorliegen und die Anbieter diese Daten ggf. für ihre Zwecke nutzen. In Google Play gibt es Apps, die Backups auch von nicht-gerooteten Geräten anfertigen können[12].

11.4 Widgets

Widgets sind kleine Programme, die im Homescreen des Smartphones ablaufen. Sie sind im Betriebssystem schon teilweise vorhanden, können aber auch aus dem App Store nachinstalliert werden. Typische Widgets sind Kalender, Notizen, E-Mail oder Wetter.

Diese Widgets können auch im Sperrbildschirm angezeigt werden.

Es ist darauf zu achten, dass im Sperrbildschirm durch Widgets keine sensitiven Daten angezeigt werden, beispielsweise SMS (die z. B. mTANs für Bank-Transaktionen enthalten können), E-Mail-Nachrichten oder Kalendereinträge.

11 https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/BasisschutzGeraet/EinrichtungMobileGeraete/EinrichtungMobileGeraete_node.html
12 Beispiel: MyPhoneExplorer (Desktop-Programm) und zugehörige MyPhoneExplorer Client (Android App)

11.5 Google Apps und Google Dienste

Es gibt eine Vielzahl von Apps und Diensten von Google; dazu gehören Apps, die bereits mit dem Android-Gerät ausgeliefert werden sowie Apps, die man nachträglich installieren kann. Beispiele sind:

- Gmail
- Chrome
- Hangout
- Google Kalender
- Google Drive
- YouTube
- Picasa
- Google Play
- Google+
- Google Now

Alle Google-Apps und Google-Dienste sind u. a. auch über Google Now miteinander verzahnt und bilden ein Ökosystem, das die Verwendung von Android-Geräten bequem macht. So wird beispielsweise bei Google Maps die aktuelle Position in der Karte angezeigt, wenn man sich orientieren will, oder tageszeit- oder ortsabhängige Ereignisse werden automatisch im Bildschirm eingeblendet. Seit der Android-Version 4.4 enthält Google Now die Sprachsteuerungsfunktion 'always-listening'. Ist diese Funktion aktiviert, reagiert das Mobilgerät auf die Worte 'OK Google' und führt den gesprochenen Befehl aus oder beantwortet die gesprochene Anfrage. Dabei ist das Mikrofon des Gerätes immer aktiviert, wenn sich das Gerät im eingeschalteten Zustand befindet.

Nutzer erkaufen sich diese Bequemlichkeit jedoch mit der Übertragung ihrer Daten an Google, die Google gemäß der Nutzungsvereinbarung zur Bereitstellung des Dienstes weiter auswerten und nutzen kann. Anwender sollten daher überlegen, welche Apps beziehungsweise Dienste sie verwenden wollen. Über die App *Google Einstellungen* hat der Benutzer Möglichkeiten, den Abfluss von Daten durch Google-Dienste zu steuern. Zudem kann man im Menü *Einstellung - Apps* nicht benötigte System-Apps deaktivieren[13]. Mit weitergehenden Maßnahmen ist es sogar möglich, ein Android-basiertes Mobilgerät weitgehend auch ohne Google-Apps und Google-Dienste zu betreiben[14].

An dieser Stelle sei deutlich darauf hingewiesen, dass Google zwar eine umfassende Integration seiner Apps und Dienste in Android vorgenommen hat, Anbieter anderer Apps deren Nutzerdaten aber ebenso erfassen, speichern und (oft für Werbezwecke) auswerten.

12 E-Mail

Bei E-Mail-Programmen ist bei der Einrichtung des Accounts darauf zu achten, dass die Übertragung von empfangenen und gesendeten E-Mails verschlüsselt geschieht). Bei der Verwendung von Web-Mailern muss das HTTPS-Protokoll verwendet werden.

13 Internet-Browser

Der Internet-Browser ist sicherlich auch bei mobilen Endgeräten eine der am meisten verwendeten Apps. Es ist ein Internet-Browser zu verwenden, der nach dem Sandbox-Prinzip arbeitet.

Der Standardbrowser in Google Nexus-Geräten ist der Chrome-Browser. Der Browser verfügt über einen "Inkognito-Modus", in dem die aufgerufenen Webseiten nicht zum "Verlauf" (Historie) hinzugefügt werden. Cookies, Lesezeichen, Leselisten, usw. werden nicht gespeichert. Dieser Modus ist zu verwenden, wenn man keine Spuren des Surf-Verhaltens auf dem Endgerät hinterlassen will und Eingaben und Downloads nicht registriert werden sollen. Der Inkognito-Modus kann jedoch prinzipiell nicht einer ggf. Server-seitig implementierten Überwachung entgegenwirken. Insofern ist die Bezeichnung "Inkognito" irreführend, da gegenüber dem Anbieter der Webseite keine Anonymisierung erfolgt.

Enthält der verwendete Browser einen Phishing-Filter, sollte dieser auch verwendet werden.

13 https://support.google.com/googleplay/answer/3123922?hl=de
14 http://heise.de/-2070519

14 Android Debugging Bridge

Android-basierte Mobilgeräte verfügen mit der sogenannten Android Debugging Bridge (ADB, auch USB-Debugging) über eine Schnittstelle, die weitgehenden Zugriff auf das Gerät erlaubt. Diese Schnittstelle besteht standardmäßig aus einer Kabelverbindung zwischen Mobilgerät und Desktop-Computer, es gibt aber auch Erweiterungen, die eine Verbindung über WLAN erlauben. Die Schnittstelle ist primär für den Entwicklungsprozess von Apps gedacht, wird aber auch für diverse andere Datenzugriffe auf dem Gerät verwendet. Die Schnittstelle ist standardmäßig deaktiviert, kann aber durch den Benutzer aktiviert werden (bei einigen Geräten durch versteckte Kommandos im Menü *Einstellungen).*

Diese Schnittstelle ist für den normalen Gebrauch von Android-basierten Geräten nicht notwendig und sollte in jedem Fall deaktiviert werden.

15 Display-Sperre

Im Menü *Einstellung - Sicherheit - Display-Sperre* kann man wählen, ob das Gerät über eine Display-Sperre verfügen und mit welcher Methode die Entsperrung erfolgen soll. Zur Wahl stehen:

- keine
- Finger bewegen
- PIN
- Passwort
- Muster
- Face Unlock

Die Wahlmöglichkeit *keine* und *Finger bewegen* bieten keinerlei Schutz vor unberechtigtem Zugriff. Eine *PIN* kann aus mindestens 4 und maximal 16 Ziffern bestehen. Das Gleiche gilt für ein *Passwort* aus alphanumerischen Zeichen. Ein mit dem Finger abzufahrendes *Muster* hat Werte zwischen 4 und 9 Punkte. *Face Unlock* ist als Zugangsschutz ungeeignet, da Personen, die sich ähnlich sehen, das Smartphone entsperren können. Teilweise reicht schon ein ausgedrucktes Foto zur Entsperrung.

Der beste Zugangsschutz bietet ein ausreichend langer PIN-Code beziehungsweise ein entsprechend komplexes alphanumerisches Passwort.

Über das Menü *Einstellung – Display -Ruhezustand* kann die Zeit bis zur automatischen Aktivierung einer Displaysperre zwischen 15 Sekunden und 30 Minuten eingestellt werden. Es wird empfohlen, dort keine Zeiten über fünf Minuten zu wählen.

16 Geräteverschlüsselung

Mit dem Menü *Einstellung - Sicherheit - Telefon verschlüsseln* kann man die Daten des Smartphones verschlüsseln. Es handelt sich um eine Verschlüsselung der Datenpartition des Benutzers. Dazu ist die Eingabe einer PIN oder eines Passworts beim Gerätestart notwendig, die beliebte Wischgeste (Finger bewegen) funktioniert damit nicht.

Zu beachten ist, dass bisher nur der interne Gerätespeicher verschlüsselt wird, Daten auf einer eventuell vorhandenen externen Speicherkarte oder Daten die in der Cloud gespeichert werden jedoch nicht. Ist dies der Fall, kann zur Verschlüsselung der Daten der SD-Karte oder Daten in der Cloud auf Drittanbieter-Apps aus dem App Store zurückgegriffen werden.

Weiterhin ist zu beachten, dass gegebenenfalls eine Verschlüsselung nur durch das Zurücksetzen des Geräts auf Werkseinstellung rückgängig gemacht werden kann. Dabei gehen alle Daten auf dem internen Speicher des Geräts verloren. Zur Datenwiederherstellung muss vor dem Zurücksetzen ein Backup erstellt werden.

17 Geräteadministrator-Apps

Als "Geräteadministratoren"werden in Android Apps bezeichnet, die Sicherheitsrichtlinien durchsetzen. Die Apps tragen sich im Menü *Einstellungen - Sicherheit - Geräteadministratoren* ein und müssen vom Nutzer dort auch aktiviert werden.

Die Richtlinien betreffen:

- Passwortregeln
- Aufforderung für ein neues Passwort
- Automatische Bildschirmsperrung
- Datenlöschung (Werkseinstellung) aus der Ferne
- Geräteverschlüsselung
- Abschalten der Kamera

Sie können in der jeweiligen App fest enthalten sein oder von einem entfernten Server gesendet werden[15]. Oft werden solche Apps mit einer entsprechenden Infrastruktur angeboten.

Da es sich um normale Apps handelt, sollten Nutzer während der Installation auf die Berechtigungen achten, die solche Apps fordern. Bei bereits installierten Geräteadministrator-Apps kann über das Menü *Einstellungen - Sicherheit - Geräteadministratoren* die Administrator-Funktionalität abgeschaltet werden.

18 Restrisiken

Selbst bei der Verwendung von sicheren Einstellungen auf dem mobilen Endgerät, die sowohl den Benutzer als auch die Apps weitgehend in ihren Freiheiten einschränken, bleibt ein Restrisiko. Dieses Restrisiko beruht in erster Linie darauf, dass die Geräte außerhalb einer gesicherten Umgebung eingesetzt werden, oft auch in Umgebungen, in denen man einen Laptop nicht einsetzen würde. Es besteht immer die Gefahr, dass die Geräte (und damit die darauf befindlichen Daten) durch Verlust oder Diebstahl abhandenkommen. In einem solchen Fall kann man nur darauf vertrauen, dass die eingesetzten Mechanismen zur Datenabsicherung wirksam greifen und nachträglich initiierte Aktionen (beispielsweise eine Fernlöschung) funktionieren. Hierbei ist aber auch abzuwägen, ob Fernlöschmechanismen oder Geräteortung nicht anderen Datenschutzaspekten widersprechen.

Bei allen Varianten des Einsatzes von Android verbleiben Restrisiken unterschiedlicher Tragweite, denen nicht ohne Weiteres begegnet werden kann. Als Beispiel seien die unerlaubte Verwendung des Gerätemikrofons zum Abhören oder die unerlaubte Nutzung der GPS-Funktion zum systematischen Tracking des Benutzers genannt.

Darüber hinaus liegen weitere Restrisiken in der Sprach-, SMS- und Datenkommunikation über das Internet, die ohne zusätzliche Maßnahmen nicht Ende-zu-Ende gesichert sind.

Zu beachten ist auch, dass sichere Konfigurationen immer auch Beschränkungen für den Benutzer bedeuten. Dies führt nicht nur zu Akzeptanzproblemen, sondern fördert auch die Fantasie der Benutzer, Grenzen und Beschränkungen zu überwinden.

15 Supportartikel zu Device Administrator API (englisch): http://developer.android.com/guide/topics/admin/device-admin.html

19 Fazit

Mobile Geräte mit dem Betriebssystem Android sind sowohl im Privat- wie im Geschäftsbereich weit verbreitet. Diese Verbreitung liegt im Wesentlichen an der Offenheit des Systems, an vergleichsweise günstiger Hardware und an der Vielzahl kostenfreier Apps. Diese Offenheit führt jedoch einerseits zu einer komplexen Betriebssystem-Struktur, andererseits aber auch zu einer unüberschaubaren Vielzahl von Geräten mit unterschiedlichen Android-Versionen. Dadurch ergeben sich ebenso heterogene wie komplexe Anforderungen beim Versuch einer abgesicherten Nutzung der Geräte.

Für den beruflichen Einsatz von Android-basierten Geräten sind mindestens die oben empfohlen Konfigurationen durchzuführen. Beim Einsatz dieser Geräte in größeren Umgebungen und Stückzahlen ist die Verwaltung mittels einer Mobile Device Management-Lösung[16] unumgänglich.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **info@cyber-allianz.de** gesendet werden.

16 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_052.pdf

Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IM UNTERNEHMEN

Einsatz und Konfiguration des Adobe Readers X und XI

Durch manipulierte PDF-Dokumente können Sicherheitslücken in PDF-Readern ausgenutzt werden, um Schadprogramme auf einem Zielsystem zur Ausführung zu bringen. Aufgrund seiner weiten Verbreitung steht dabei insbesondere der Adobe Reader für das Betriebssystem Microsoft Windows im Fokus von Angreifern. Seit Ende 2010 verfügt die Version X („Zehn“) des Adobe Readers mit dem *Geschützten Modus* (Protected Mode) über eine Sandbox, die diesen Angriffen entgegenwirken soll. In der aktuellen Version XI ist der Sandboxmechanismus durch ein weiteres Feature, die *Geschützte Ansicht* (Protected View), erweitert worden. Seit dem Einsatz des Adobe Readers X und XI konnten PDF-gestützte Angriffsformen weitgehend abgewehrt werden. Der Aufwand für Angreifer, wirksame Schadsoftware zu erzeugen, erhöht sich um ein Vielfaches, da zusätzlich die Sandbox umgangen werden muss.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt Anwendern, die zur Betrachtung und Bearbeitung von PDF-Dokumenten den Adobe Reader verwenden, die aktuelle Version Adobe Reader XI einzusetzen und den *Geschützten Modus* sowie die *Geschützte Ansicht* zu nutzen. Die Erfolgsaussichten weitverbreiteter Angriffe über manipulierte PDF-Dokumente werden dadurch deutlich reduziert. Zusätzlich zu dem erforderlichen Einspielen sämtlicher (Sicherheits-)Aktualisierungen sollten daher folgende Punkte beachten werden:

1 Der Geschützte Modus

Mit dem *Geschützten Modus* ab dem Adobe Reader X hat der Hersteller die Architektur der Software unter Microsoft Windows um eine wesentliche Sicherheitskomponente erweitert.

Die technischen Grundlagen des *Geschützten Modus* hat das Secure Software Engineering Team des Herstellers in einer Serie von Artikeln detailliert dargestellt:

http://blogs.adobe.com/security/2010/10/inside-adobe-reader-protected-mode-part-1-design.html

http://blogs.adobe.com/security/2010/10/inside-adobe-reader-protected-mode-part-2-the-sandbox-process.html

http://blogs.adobe.com/security/2010/11/inside-adobe-reader-protected-mode-part-3-broker-process-policies-and-inter-process-communication.html

https://blogs.adobe.com/security/2010/11/inside-adobe-reader-protected-mode-part-4-the-challenge-of-sandboxing.html

1.1 Voraussetzungen und Einschränkungen für den Einsatz des Geschützten Modus

In größeren, administrierten Umgebungen muss grundsätzlich vor jedem Einsatz einer neuen Software deren Verträglichkeit mit der bereits bestehenden Umgebung sowie den dort vorhandenen Arbeitsabläufen sichergestellt werden. Dies gilt auch für den Adobe Reader X und XI. Da die Aktivierung des *Geschützten Modus* im Adobe Reader aus sicherheitstechnischer Sicht umgesetzt werden sollte, müssen die erforderlichen Tests vor der Installation auf Produktivsystemen auch *diesen Modus* umfassen. Hier ist speziell auf die Funktionsfähigkeit von Plug-Ins oder Zusatzmodulen des Adobe Readers bei aktiviertem *Geschützten Modus* zu achten, die möglicherweise in der individuellen Umgebung eingesetzt werden.

1.2 Aktivierung des Geschützten Modus

Nach einer Installation des Adobe Readers ist der *Geschützte Modus* bereits aktiviert. Über das Menü „*Datei → Eigenschaften*“ kann nach dem Start des Adobe Readers und dem Öffnen eines PDF-Dokuments unter dem Reiter „*Erweitert*“ überprüft werden, ob der *Geschützte Modus* aktiviert ist (Geschützter Modus: Ein).

Die Aktivierung und Deaktivierung des *Geschützten Modus* wird in den Menüs des Adobe Readers XI über „*Bearbeiten → Voreinstellung*“ und dort im Bereich „***Sicherheit (erweitert)***“ vorgenommen: „*Geschützten Modus beim Start aktivieren*“.

Die Aktivierung/Deaktivierung im Adobe Reader X erfolgt unter „*Bearbeiten → Voreinstellung*“ und dort im Bereich „*Allgemein*“: „*Geschützten Modus beim Start aktivieren*“.

In administrierten Umgebungen sollte diese Einstellmöglichkeit für den Nutzer blockiert werden. Die dafür notwendigen Konfigurationsschritte werden im Folgenden beschrieben.

1.3 Administration des Geschützten Modus

***Geschützten Modus* einschalten**

Sofern der Adobe Reader mit *Geschütztem Modus* in einer Testumgebung keinen Konflikt mit den etablierten Arbeitsabläufen erzeugt hat, sollten Administratoren in größeren Umgebungen auf Nutzersystemen die Aktivierung über die Registry von Microsoft Windows vornehmen. Dazu muss unter dem Schlüssel:

HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\<version>\FeatureLockDown[1]

ein DWORD-Wert mit dem Namen „bProtectedMode“ angelegt werden.

Achtung: Wenn Sie ein 32-Bit Adobe Reader-Plug-In (z.B. als Plug-In über einen 32-Bit-Browser) auf einem 64-Bit Windows Betriebssystem laufen haben, so müssen sämtliche (auch die folgenden) Einträge in diesem Pfad geändert werden:

HKEY_LOCAL_MACHINE\Software\Wow6432Node\...

Sowohl mit dem Wert „0“ (geschützter Modus aus), als auch mit dem Wert „1“ (geschützter Modus an) blockiert diese Einstellung jegliche Änderungen des *Geschützten Modus* über die Benutzeroberfläche des Adobe Readers X und XI. Die entsprechende Option wird in der Folge innerhalb der Benutzeroberfläche ausgegraut dargestellt.

Falls der Benutzer selbst entscheiden darf, ob er den *Geschützten Modus* aktivieren oder deakti-

1 <version> muss für Adobe Reader X mit „10.0“ und für Adobe Reader XI mit „11.0“ ersetzt werden.

vieren darf und eine Voreinstellung administrativ gemacht werden muss, sollte unter dem Schlüssel:

HKEY_LOCAL_USER\Software\Adobe\Acrobat Reader\<version>\Privileged

ein neuer DWORD-Wert mit dem Namen „bProtectedMode“ angelegt werden. Den Wert kann wie oben entsprechend gesetzt werden.

Geschützten Modus ausschalten

Für den Fall, dass wegen eines Konflikts mit den Arbeitsabläufen der Adobe Reader ohne den *Geschützten Modus* eingesetzt werden soll, ist der DWORD-Wert „bProtectedMode“ des Schlüssels:

HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\<version>\Feature-LockDown

zu löschen, um die Blockade aufzuheben. Wenn der *Geschützte Modus* im Menü ausgeschaltet und ausgegraut sein soll, ist der Wert nicht zu löschen, sondern auf „0“ zu setzen.

Sollte es beim Einsatz des *Geschützten Modus* zu Problemen mit Plug-Ins oder Arbeitsabläufen kommen, kann zur weiteren Analyse unter *„Bearbeiten → Voreinstellung“* im Bereich *„Sicherheit (erweitert)“* die Erstellung einer speziellen Protokoll-Datei aktiviert werden.

Unter Adobe Reader X findet man diese Einstellung unter *„Bearbeiten → Voreinstellung → Erweitert“*.

In größeren Umgebungen kann die Protokollerstellung auch über die Registry veranlasst werden. Details dazu sowie zu den anderen Konfigurationsmöglichkeiten des Adobe Reader in administrierten Umgebungen wird vom Hersteller im „Acrobat Development Center“ bereitgestellt unter: http://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/protectedmode.html

2 Geschützte Ansicht des Adobe Reader XI

Bei der *Geschützten Ansicht* wird davon ausgegangen, dass alle Adobe PDF-Dokumente schädlich sind. Daher sind alle Features deaktiviert, außer diejenigen, die nur für das Betrachten einer PDF-Datei wichtig sind (Zoom, Navigation, Links, Finden, ...). Wenn der Benutzer z. B. eine PDF-Datei öffnet und aktive Inhalte dieser Datei nutzen möchte, muss er auf den Hinweistext *„Alle Funktionen aktivieren“* klicken.

Die *Geschützte Ansicht* ist nur aktiv, wenn der *Geschützte Modus* aktiviert ist.

Die technischen Grundlagen der *Geschützten Ansicht* hat das Product Security Incident Response Team des Herstellers in folgendem Artikel dargestellt:

http://blogs.adobe.com/security/2011/06/inside-adobe-acrobat-protected-view.html

Da die Aktivierung der *Geschützten Ansicht* im Adobe Reader XI aus sicherheitstechnischer Sicht umgesetzt werden sollte, müssen die erforderlichen Tests vor der Installation auf Produktivsystemen auch die *Geschützte* Ansicht umfassen.

Nach Installation des Adobe Readers ist die *Geschützte Ansicht* deaktiviert (Option „Aus“). Das BSI empfiehlt diese Standardeinstellung zu ändern und die Option „Dateien mit potenziell unsicherem Ursprung“ oder die Option „Alle Dateien“ zu wählen.

2.1 Aktivierung der Geschützten Ansicht

Wie bereits oben erwähnt, ist nach einer Installation des Adobe Readers der *Geschützte Modus* schon aktiv. Die *Geschützte Ansicht* dagegen ist ausgeschaltet und sollte erst aktiviert werden. Die Aktivierung und Deaktivierung der *Geschützten Ansicht* wird in den Menüs des Adobe Readers über *„Bearbeiten → Voreinstellung“* und dort im Bereich „*Sicherheit (erweitert)*“ vorgenommen. Es gibt folgende Optionen:

1. *„Aus“* : Deaktiviert die *Geschützte Ansicht.*

2. *„Dateien mit potenziell unsicheren Ursprung“*: Aktiviert die *Geschützte Ansicht* und zeigt für alle Dateien Warnungen an, die von einer nicht vertrauenswürdigen Quelle stammen. Dateien, die vom Benutzer als vertrauenswürdig markiert werden, sind ab diesem Zeitpunkt von der *Geschützten Ansicht* ausgenommen und werden in der Liste „*vertrauenswürdiger Sites*“ unter *„Bearbeiten → Voreinstellung“ → „Sicherheit (erweitert)“* gelistet (siehe Punkt 3 – „Festlegen der vertrauenswürdigen Seiten“).

3.*„Alle Dateien“*: Aktiviert die *Geschützte Ansicht* in allen PDF, die geöffnet werden, über den Reader selbst oder über das Browser Plug-In. Auch hier werden Dateien, die vom Benutzer als vertrauenswürdig markiert werden, ab diesem Zeitpunkt von der *Geschützten Ansicht* ausgenommen und unter „*vertrauenswürdige Sites*“ gelistet.

2.2 Administration der Geschützten Ansicht

Sofern der Adobe Reader mit *Geschützter Ansicht* in einer Testumgebung keinen Konflikt mit den etablierten Arbeitsabläufen erzeugt hat, sollten Administratoren die Aktivierung auf Nutzersystemen in größeren Umgebungen über die Registry von Microsoft Windows vornehmen. Dazu muss unter dem Schlüssel:

HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\11.0\FeatureLockDown

ein DWORD-Wert mit dem Namen „iProtectedView“ und einem Wert angelegt werden. Folgende Werte können gesetzt werden:

Wert „0“: „Aus“

Wert „1“: „Dateien mit potenziell unsicherem Ursprung“

Wert „2“: „Alle Dateien“

Über die Benutzeroberfläche des Adobe Readers ist die Einstellung blockiert. Die entsprechende Option wird in der Folge innerhalb der Benutzeroberfläche ausgegraut dargestellt.

2.3 Geschützte Ansicht ausschalten

Für den Fall, dass wegen eines Konflikts mit den Arbeitsabläufen der Adobe Reader ohne *Geschützte Ansicht* eingesetzt werden soll, ist das DWORD „iProtectedView“ des Schlüssels:

HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\11.0\FeatureLockDown

mit einem anderen Wert zu belegen. Wenn der Benutzer dies zu entscheiden hat, so muss dieses DWORD gelöscht werden.

Weitere Details und Infos zu der Protokollerstellung finden Sie im Detail unter:

http://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/protectedview.html

3 Erweiterte Sicherheit

Erweiterte Sicherheit, die es schon seit dem Adobe Reader 8 und 9 gibt, schränkt generell Verhaltensweisen des PDFs und das Ausführen von Inhalten ein.

Wenn die *Erweiterte Sicherheit* aktiviert ist und die Datei noch nicht als vertrauenswürdig eingestuft worden ist, erscheint eine Warnung, sobald diese Datei versucht, folgende riskante Aktionen durchzuführen: domänenübergreifende Zugriffe aufrufen, Javascript ausführen, Skripte oder Daten einfügen, Multimedia-Elemente wiedergeben, etc.

Nach einer Installation des Adobe Readers ist die *Erweiterte Sicherheit* bereits standardmäßig aktiviert. Die Aktivierung und Deaktivierung der *Erweiterten Sicherheit* wird in den Menüs des Adobe Readers über *„Bearbeiten → Voreinstellung“* und dort im Bereich ***„Sicherheit (erweitert)“*** vorgenommen: *„Erweiterte Sicherheit aktivieren“*.

Administratoren in größeren Umgebungen auf Nutzersystemen sollten die Aktivierung über die Registry von Microsoft Windows vornehmen. Dazu muss unter dem Schlüssel:

HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\<version>\FeatureLockDown

ein neuer DWORD-Wert mit dem Namen „bEnhancedSecurityStandalone“ und „bEnhancedSecurityInBrowser“ angelegt werden.

Sowohl mit dem Wert „0“ (Erweiterte Sicherheit aus), als auch mit dem Wert „1“ (Erweiterte Sicherheit an) blockiert dieser DWORD-Wert jegliche Änderungen der Erweiterten Sicherheit über die Benutzeroberfläche des Adobe Readers X und XI. Die entsprechende Option wird in der Folge innerhalb der Benutzeroberfläche ausgegraut dargestellt. Dies ist jedoch nicht zu empfehlen.

Festlegen der *Vertrauenswürdigen Sites*

Vertrauenswürdige Sites können Dateien, Dateien in bestimmten Ordnern oder URLs sein. Wenn diese aufgelistet sind, wird das Laden von Daten im Adobe Reader zugelassen.

Wenn der Benutzer ein PDF-Dokument öffnet und diesem vertraut (durch entsprechenden Klick auf den Sicherheitshinweis), wird dieses unter den *Vertrauenswürdigen Sites* gelistet. Der Benutzer kann auch vorher selbst bestimmen, welche Quellen er als vertrauenswürdig ansieht. Um diese einzutragen, müssen Sie unter *„Bearbeiten → Voreinstellung“* und dort im Bereich ***„Sicherheit (erweitert)“*** *Datei hinzufügen, Verzeichnispfad hinzufügen* oder *Host hinzufügen* wählen und die gewünschte Quelle angeben. Die Sicherheitseinstellungen von diesen Quellen können nun umgangen werden.

Auch können die *Vertrauenswürdigen Sites*, die bereits in den Internetoptionen von Windows unter dem Reiter *„Sicherheit →Vertrauenswürdige Sites“* eingetragen worden sind, mit der Option *„Unter meinen Windows-Sicherheitszonen aufgeführten Sites automatisch Vertrauen“* auch für den Adobe Reader genutzt werden.

Die Option *„Dokumenten mit gültigem Zertifikat automatisch vertrauen“* kann gewählt werden, um Dokumente mit entsprechender digitaler Signatur auszuführen. Diese Option gibt es seit dem Adobe Reader XI.

Erweiterte Sicherheit und *Vertrauenswürdige Sites* können auch in administrierten Umgebungen konfiguriert werden. Details dazu finden Sie auf folgender Seite:
http://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/enhanced.html

4 Adobe PDF Whitelisting Framework

Das ***Adobe PDF Whitelisting Framework*** erlaubt die selektive Aktivierung von Javascript für vertrauenswürdige PDF-Dateien oder für PDF-Dokumente an bestimmten Speicherorten.

Unter *„Bearbeiten → Voreinstellungen → Javascript“* gibt es folgende Optionen:

- Falls Javascript nicht benötigt wird, sollte *„Acrobat JavaScript aktivieren“* **deaktiviert** werden. Das automatische Ausführen von Javascript wird dadurch deaktiviert oder über APIs beschränkt.

Falls Javascript benötigt wird, sollten folgende Optionen gewählt werden:

- *„Menübefehlen Berechtigung zur Ausführung von JavaScript erteilen“* **aktivieren**: Wenn ein PDF geöffnet ist, wird durch Klicken auf einen Hinweistext in der Benutzeroberfläche die Ausführung von JavaScript aktiviert.
- *„Sicherheitsrichtlinie für globale Objekte aktivieren“* **aktivieren**: Javascript wird global über APIs zugelassen oder es wird bestimmten Dokumenten vertraut (siehe *Vertrauenswürdige Sites*).

Diese Einstellungen können auch in administrierten Umgebungen vorgenommen werden. Mehr dazu finden Sie unter:

http://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/javascript.html

5 Support

Der Produktsupport für den Adobe Reader 9 wurde am 26.06.2013 eingestellt. Unter Windows sollte der Adobe Reader X (Support bis 18.11.2015) oder besser der Adobe Reader XI (Support bis 15.10.2017) verwendet werden. Unter Linux empfiehlt das BSI, einen alternativen PDF-Reader zu benutzen.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **info@cyber-allianz.de** gesendet werden.

Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IM UNTERNEHMEN

Drucker und Multifunktionsgeräte im Netzwerk

Bürogeräte – wie Drucker, Scanner, Kopierer, Faxgeräte oder die Kombination dieser als Multifunktionsgeräte – sind heutzutage üblicherweise fester Bestandteil der Office-IT und anderer IT-Infrastrukturen. Im Gegensatz zu anderen Komponenten der Infrastruktur, beispielsweise Anwender-PCs oder Server, wird der Sicherheit dieser Geräte jedoch meist kaum Beachtung geschenkt.

1 Bedrohungslage

Moderne Drucker oder Multifunktionsgeräte bieten zunehmend Dienste an, die einen Zugriff über das Netzwerk mithilfe von Protokollen, wie HTTP, FTP, TELNET oder SNMP, ermöglichen. Gleichzeitig eröffnen sich hierüber prinzipiell auch Möglichkeiten für Angriffe. Zudem sind diese Dienste mitunter nicht sicher implementiert, wohl aber in der Standardkonfiguration aktiviert oder sie können gar nicht deaktiviert werden. Insbesondere Geräte, die durch externe Netzzugänge über das Internet erreicht werden können, sind in besonderem Maße durch Angriffe bedroht.

Zusätzlich zu diesen Diensten sind gerätespezifische Protokolle (z. B. Printer Control Language, PCL oder Printer Job Language, PJL) und möglicherweise undokumentierte Zugangsmöglichkeiten (Debugging-Schnittstellen) implementiert. Diese können für unberechtigte Zugriffe verwendet werden. Auch Cross Site Scripting und ähnliche Angriffe über bzw. auf die Webschnittstelle sind ggf. möglich. Somit kann ein Angreifer durch eine manipulierte E-Mail oder Webseite über einen lokalen Client unberechtigten Zugriff auf den Drucker erlangen.

Analog zu Betriebssystemen und Anwendungen für PCs existieren auch Exploits[1] für Drucker und Multifunktionsgeräte und die darauf implementierten Dienste und Schnittstellen. Diese reichen von Denial-of-Service Angriffen bis hin zur Ausführung von fremdem Code auf dem Gerät. Erforderliche Patches zur Behebung von solchen Schwachstellen werden häufig nicht durch die Betreiber eingespielt. Mitunter werden auch keine Patches durch die Hersteller zur Verfügung gestellt.

Authentisierungsmechanismen können evtl. umgangen werden, da die Geräte i. d. R. nicht gegen Brute Force Angriffe geschützt sind und somit ein automatisiertes Ausprobieren von Passwörtern oder den Missbrauch von Standardpasswörtern möglich ist. Zudem ermöglichen es insbesondere ältere SNMP-Versionen und andere Schnittstellen, Passwörter in Erfahrung zu bringen.

Aufgrund dieser Schwachstellen kann ein Angreifer beispielsweise:

1 Printer Exploitation Toolkit (PRET), http://hacking-printers.net

- Gescannte oder gedruckte Dokumente herunterladen (Verlust von Intellectual Property, Verletzung von Datenschutzbestimmungen),
- Eigene Dokumente zum Drucken hochladen,
- Änderungen an der Gerätekonfiguration vornehmen (z. B. IP-Adresse ändern, Zugriffsberechtigungen bzw. ACLs modifizieren, Druckeinstellungen ändern, Manipulation der Firmware, Herbeiführen von Verschleißerscheinungen, etc.),
- Missbrauch von Druckern als Einfallstor für Angriffe auf das lokale Netzwerk.

Insbesondere der erste der genannten Punkte kann einen signifikanten Schaden verursachen, da gerade größere Bürogeräte in der Regel über einen nicht-flüchtigen Speicher verfügen und dort sämtliche gedruckten oder gescannten Dokumente speichern. Dies muss sowohl bzgl. des (externen) Wartungspersonals als auch bei der Entsorgung von Geräten berücksichtigt werden. Darüber hinaus könnten durch Innentäter, Wartungspersonal oder Lieferanten Manipulationen an der Hardware vorgenommen oder die Festplatten in Geräten ausgetauscht werden.

2 Empfohlene Maßnahmen

Zusätzlich zu allgemeinen Maßnahmen im Rahmen des IT-Sicherheitsmanagements sollten die folgenden Maßnahmen bzgl. der Geräte selbst ergriffen werden, sofern diese vom jeweiligen Produkt unterstützt werden:

- Drucker sollten nicht aus dem Internet heraus erreichbar sein
- Beschränkung des Zugriffs von Druckern in das Internet
- Verwendung eines von Clients und Servern separierten Netzbereichs für Drucker. Falls möglich sollte der Zugriff auf Drucker nicht direkt von Clients aus möglich sein, sondern nur über Druckerserver erfolgen können.
- Änderung sämtlicher Standardpasswörter. Dabei ist zu beachten, dass ggf. für verschiedene Zugriffsmöglichkeiten mehrere separate Passworte verwendet und entsprechend geändert werden müssen.
- Aktivieren der sicheren Kommunikation zu den Geräten oder anderen Komponenten, wie Druckerservern, sowohl für Dokumente als auch für Authentisierungsdaten. Hierzu bietet sich die Nutzung von IPP (Internet Printing Protocol) an, welches eine Absicherung mittels SSL/TLS ermöglicht.
- Nutzung von Zugangsberechtigungen (Access Control List, ACL)
- Aktivieren der Verschlüsselung des eingebauten Dateisystems (Harddrive, Ramdisk)
- Aktivieren des sicheren Löschens der internen Datenträger / Speicher nach Abarbeitung von Aufträgen
- Deaktivieren unsicherer bzw. nicht-benötigter Dienste (z. B. FTP, SNMP, TELNET, etc.)
- Sicherstellung der Aktualität der Firmware. Einige Hersteller bieten Tools an, um die Versionsstände der Drucker von zentraler Stelle aus zu überwachen und zu aktualisieren. Im Falle von Beschränkungen des Zugriffs auf das Internet ist zu gewährleisten, dass Patches manuell eingespielt werden.
- Nutzung weiterer Features, wie z. B. vertrauliches Drucken (Ausgabe von Dokumenten nur nach PIN-Eingabe)
- Beachtung der Hersteller-Dokumentation bzw. -Empfehlungen zu Sicherheitsaspekten

Die genannten Punkte sollten auch bei der Auswahl bzw. Beschaffung von Geräten berücksichtigt werden. Zudem sollten weitere Kriterien geprüft werden, wie beispielsweise fest-codierte Passwörter oder Passwort-Policies (z. B. Mindestlängen).

Weiterführende Informationen zur Absicherung von Bürogeräten liefert auch der IT-Grundschutz des BSI[23].

2 B 3.406 Drucker, Kopierer und Multifunktionsgeräte: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b03/b03406.html

3 B 3.402 Faxgerät: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b03/b03402.html

Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: METHODIK

Schützen Sie sich vor professionellen gezielten Cyber-Angriffen

Stellen Sie sich vor, Sie besuchen eine internationale Produktmesse und erkennen zufällig bei einem der Anbieter ein Produkt, welches Ihrem bisherigen Verkaufsschlager auffallend ähnelt und zum halben Preis angeboten wird. Oder stellen Sie sich vor, Sie befinden sich mitten in den Verhandlungen zu einem Großauftrag oder versuchen ein strategisch wertvolles Unternehmen zu übernehmen und müssen erfahren, dass alle Ihre Angebote knapp unter- bzw. überboten werden. Und was wäre, wenn Ihr Produktionsleiter Ihnen gerade meldet, dass die Produktionslinie aufgrund eines unerklärlichen Computerfehlers ausgefallen ist und die Wiederherstellung mehrere Tage in Anspruch nehmen wird? Die genannten Beispiele sind keine hypothetischen Gedankenspiele, sondern reale Vorfälle, die bereits aufgetreten sind. Sie sind oftmals die Folge von Wirtschaftsspionage mittels professioneller gezielter Cyber-Angriffe.

Erfolgreiche Cyber-Angriffe verursachen mittelbare und unmittelbare Schäden, die sich letztlich finanziell auswirken. **Sie als Entscheidungsträger sind für den wirtschaftlichen Erfolg des Unternehmens verantwortlich** und müssen daher die ständige Überprüfung und Aktualisierung der IT-Sicherheitsmaßnahmen veranlassen und die Mittel dafür bereitstellen.

1 Gezielte Cyber-Angriffe

Im Zusammenhang mit professionellen gezielten Cyber-Angriffen hat sich der Begriff der „Advanced Persistent Threats (APT)“ eingebürgert, der eine spezielle Angriffsmethodik bzw. Ausprägungsform gezielter Cyber-Angriffe darstellt. Die konkrete Bedeutung variiert jedoch in verschiedenen Publikationen. In diesem Dokument wird folgende informelle Definition verwendet:

> *„Ein APT liegt dann vor, wenn ein **gut ausgebildeter Angreifer** mit Rückgriff auf große **Ressourcen** sehr **gezielt** ein Netz oder System angreift, sich dann in dem System ausbreitet, weitere Hintertüren einbaut und ggf. über **längere Zeit** Informationen sammelt oder Manipulationen vornimmt.“*

1.1 Opfer gezielter Cyber-Angriffe

Grundsätzlich stellen gezielte Cyber-Angriffe für jede Branche und jedes Unternehmen eine Bedrohung dar, das vertrauliche, geschäftskritische Informationen auf IT-Systemen verarbeitet oder dessen Erfolg von der Verfügbarkeit seiner IT-Systeme abhängt. Betriebsgeheimnisse, wie beispielsweise Forschungs- und Entwicklungsergebnisse, Herstellungsverfahren oder unternehmenspolitische Entscheidungen stehen dabei im Fokus der Angreifer. Das Bundesamt für Verfassungsschutz (BfV) stellt dies ebenfalls in Veröffentlichungen dar [1][2].

Aufgrund der Unterstützungsanfragen verschiedener Organisationen an das Bundesamt für Sicherheit in der Informationstechnik (BSI) und des aktiven Informationsaustausches, sowohl mit den Betroffenen als auch mit den in diesem Umfeld tätigen Experten (Computer Emergency Response Teams (CERT), Forensiker und Dienstleister), ist klar ersichtlich, dass ganze Branchen und deren Zulieferketten in Deutschland kompromittiert waren oder z. T. immer noch sind. Angegriffen werden nicht nur bekannte Großunternehmen sondern auch klein- und mittelständische Unternehmen (KMU), die beispielsweise in ihrem Marktsegment eine herausragende Position einnehmen oder die Rolle eines wichtigen Zulieferers für die zuvor genannten Großunternehmen innehaben.

Die vom BSI durchgeführte Cyber-Sicherheitsumfrage 2014 [3] stellt fest, dass etwa 56% aller befragten Unternehmen in den vergangenen 30 Monaten[1] Opfer eines Cyber-Angriffes wurden. Die Zuordnung der erfolgreichen Angriffe ist ohne intensive forensische Untersuchung schwierig, dennoch gehen 22% der befragten Unternehmen davon aus, eine Malware-Infektion aufgrund eines gezielten Cyber-Angriffes erlitten zu haben. 7% der befragten Unternehmen gaben an, Opfer eines expliziten APT-Hackings geworden zu sein.

Nach den Erkenntnissen des BSI, die aus der Bearbeitung von Vorfällen stammen, sind folgende Bereiche besonders gefährdet:

- Rüstungsindustrie
- Hochtechnologiebranche: Auto-, Schiffbau und Raumfahrt
- Forschungseinrichtungen
- Öffentliche Verwaltung

Wie auch das BfV in seinen Publikationen ausführt, ist dabei allerdings zu berücksichtigen, dass von einer sehr hohen Dunkelziffer ausgegangen werden muss.

1.2 Motivation der Angreifer

Professionelle gezielte Cyber-Angriffe verfolgen die Absicht, das **spezifisch ausgewählte Ziel** auszuspähen oder im Extremfall zu schädigen. Diese gezielten Cyber-Angriffe könnten sowohl aufgrund einer Konkurrenzsituation oder aus staatlichem Interesse erfolgen und werden mit allen zur Verfügung stehenden Ressourcen durchgeführt. Diese Ressourcen werden durchaus effizient eingesetzt, sodass ein stufenweiser Anstieg der Angriffsbemühungen bzw. der Angriffsqualität nachzuvollziehen ist.

Beispiele für die Absicht solcher gezielten Cyber-Angriffe sind:

- Wirtschaftsspionage
- Militärspionage
  Der Vorfall bei Lockheed Martin [4] verbindet sowohl Wirtschafts- als auch Militärspionage und verdeutlicht den finanziellen und zeitlichen Vorteil sowie den Wissenstransfer, der durch den Nachbau eines Kampfflugzeuges erzielt werden konnte.
- Politische Ausspähung
  Die NSA-Affäre [5] offenbart, dass gezielte Cyber-Angriffe aus allen Richtungen erfolgen können und eine Vielzahl verschiedener Zielsetzungen verfolgen.
- Sabotage
  Das Schadprogramm Stuxnet [6], dem die erfolgreiche Störung des iranischen Atomprogramms zugeschrieben wird, bleibt bis auf Weiteres das Paradebeispiel für einen Sabotageangriff.

1 Bezogen auf den Zeitraum der Umfrage vom 24.06.2014 bis 19.09.2014

1.3 Besonderheiten professioneller gezielter Cyber-Angriffe

Ein wesentlicher Aspekt der hier zugrundeliegenden Definition für APT ist die langfristige Ausrichtung des Angriffs. Der Angreifer beabsichtigt, so lange wie möglich im kompromittierten Netzwerk zu agieren. Um also keine Aufmerksamkeit zu erregen und eine Entdeckung zu vermeiden oder möglichst lange hinaus zu zögern, bereitet er sich sich umfassend vor und geht anschließend vorsichtig vor.

- Angriffsmethoden werden vor dem Einsatz modifiziert und geprüft, um sicher zu stellen, dass sie von aktuellen Standard-IT-Sicherheitsmaßnahmen nicht erkannt werden.
- Spuren werden verwischt.
- Offensichtliche Schäden oder Manipulationen werden zunächst vermieden.
- Für den Fall der Entdeckung werden Hintertüren vorbereitet.

Dies ist so erfolgreich, dass eine Kompromittierung meist erst nach mehreren Monaten und oft nicht durch den Betroffenen selbst, sondern in etwa 2/3 der Fälle [7] durch Externe aufgrund von Anomalien bemerkt wird. Studien zu diesem Thema sprechen von durchschnittlich 87 Tagen [8] – 229 Tagen [7] bis zur Feststellung des Angriffs. Dem BSI sind Einzelfälle bekannt, in denen die Angriffe 2-3 Jahre lang unentdeckt blieben. Während dieses Zeitraums ist ein kompromittiertes Netzwerk unter der vollen Kontrolle der Angreifer!

1.4 Vorgehensweise der Angreifer

Die Vorgehensweise der Angreifer lässt sich anhand der folgenden sieben Einzelschritte darstellen, die in der Fachliteratur [9] auch „Kill Chain“ genannt wird:

1. Aufklärung (Reconnaissance)
2. Erstellen eines Transportmediums für Exploit-Code (Weaponization)
3. Ausbringen des Exploits (Delivery)
4. Ausführen des Exploits (Exploitation)
5. Fußfassen im System (Installation)
6. Kontaktaufnahme zum Kontrollserver (Command and Control)
7. Daten sammeln oder Manipulationen vornehmen (Actions on Objective)

Dies macht deutlich, dass ein gezielter Cyber-Angriff gut vorbereitet und generalstabsmäßig durchgeführt wird. Es macht auch deutlich, dass der Angriff verschiedene Phasen umfasst, die jeweils unterschiedliche IT-Sicherheitsmaßnahmen erfordern. Einzelne Hersteller von IT-Sicherheitslösungen gehen daher dazu über, ihre Produkte zu erweitern und immer mehr verschiedene Schutzfunktionen zu integrieren.

1.5 Handlungsbedarf

Erfolgreiche Cyber-Angriffe verursachen mittelbare und unmittelbare Schäden, die sich letztlich finanziell auswirken. Bereits alleine die Bereinigung des Unternehmensnetzwerkes kann Monate in Anspruch nehmen und ist mit hohen Kosten verbunden. Diese Kosten sind individuell für jedes Unternehmen, können aber in der Regel kalkuliert werden. Der Schaden durch einen Informationsabfluss ist dagegen meist nicht bezifferbar. Er kann beispielsweise einen erheblichen langfristigen Verlust von Marktanteilen nach sich ziehen. Um diese Schäden zu verhindern oder wenigstens zu minimieren, müssen die IT-Sicherheitsmaßnahmen dieser Bedrohungslage angepasst werden.

Gezielte Cyber-Angriffe zeichnen sich dadurch aus, dass sie üblicherweise in der Lage sind, Standard-IT-Sicherheitsmaßnahmen zu umgehen. Daher müssen die bisherigen Lösungsansätze erweitert werden, um allen Phasen der „Kill Chain“ geeignete Gegenmaßnahmen gegenüber stellen zu können.

Dies bedeutet auch, die Möglichkeit zu akzeptieren, dass das Unternehmensnetzwerk bereits infiltriert sein könnte. Daraus folgt, dass neben der Abwehr der Angriffsversuche die schnellstmögliche Detektion und Eindämmung bereits erfolgreicher gezielter Cyber-Angriffe massiv an Bedeutung zunimmt und entsprechende Maßnahmen eingeführt bzw. verstärkt werden müssen.

2 Maßnahmen

Die nachfolgenden Ausführungen gehen davon aus, dass grundlegende Standard-IT-Sicherheitsmaßnahmen, wie beispielsweise die am Schutzbedarf orientierte Umsetzung der IT-Grundschutz-Kataloge [10] oder die Anwendung der Standards der ISO/IEC 2700x-Reihe [11] bereits vorhanden sind. Zusätzlich bietet die Cyber-Sicherheits-Veröffentlichung des BSI „Basismaßnahmen der Cyber-Sicherheit“ [12] einen pragmatischen Einstieg und liefert Anregungen für Standard-IT-Sicherheitsmaßnahmen. Sie werden daher in Kapitel 2.1 nur angerissen.

2.1 Standard-IT-Sicherheitsmaßnahmen

Die Schutzwirkung gegenüber gezielten Cyber-Angriffen kann zwar eingeschränkt sein, die Standard-IT-Sicherheitsmaßnahmen stellen aber auch dafür eine zusätzliche Hürde dar. Sie bilden somit einen verhältnismäßig einfach und kosteneffizient umzusetzenden Basisschutz, auf dem einige der erweiterten IT-Sicherheitsmaßnahmen aufsetzen können. Die Planung darüber hinausgehender Maßnahmen ist unzweckmäßig, solange den Angreifern aufgrund des fehlenden oder unvollständigen Basisschutzes eine offene Flanke präsentiert wird.

2.2 Strategische Entscheidungen durch das Management

Um erweiterte IT-Sicherheitsmaßnahmen etablieren oder anpassen zu können, die auch gegen gezielte Cyber-Angriffe wirken, müssen entsprechende Rahmenbedingungen geschaffen werden. Diese erfordern verschiedene strategische Entscheidungen durch das Management. Die folgenden „8 Leitfragen“ sind dafür exemplarische Beispiele:

- ✔ **Was muss geschützt werden? Was sind Ihre Kronjuwelen?**
  Die Einführung zusätzlicher oder die Anpassung bestehender IT-Sicherheitsmaßnahmen ist in der Regel mit hohen Kosten verbunden. Um einerseits eine angemessene Balance zwischen den Aufwänden und dem stets verbleibenden Restrisiko zu erreichen und um andererseits fundierte Entscheidungen treffen zu können, müssen die kritischen Geschäftsprozesse des Unternehmens, dessen kritische IT-Systeme und die schützenswerten Informationen identifiziert werden.
  Diese Analyse muss – abhängig von der Unternehmensstruktur und den IT-gestützten Geschäftsprozessen – auch Dienstleister, Zulieferer und Partner berücksichtigen.
- ✔ **Vor wem soll das Wissen und die Technik, die den Erfolg des Unternehmens ausmachen, geschützt werden?**
  Unternehmenspolitische Entscheidungen, wie der Abschluss von Großaufträgen, Joint Ventures oder die Ausgliederung von Unternehmenssparten bzw. die Übernahme fremder Unternehmen (-steile) können das Interesse von Konkurrenten oder Nachrichtendiensten wecken. Diese Entscheidungen sind nicht immer bei Ihrem IT-Sicherheitspersonal bekannt. Die Kenntnis derartiger Anlässe kann die Bewertung von Angriffsversuchen, wie beispielsweise von Spearphishing, entscheidend beeinflussen. Es ist also sinnvoll, eigene Planungen und Entscheidungen zu reflektieren und potenzielle Auswirkungen einer Risikoabschätzung zuzuführen und ggf. das IT-Sicherheitspersonal zu beteiligen.
- ✔ **Wer soll die Maßnahmen im täglichen Betrieb betreuen?**
  Auch bei überwiegend technisch realisierten IT-Sicherheitsmaßnahmen muss deren qualifizierte Betreuung sichergestellt werden. Die Effektivität einzelner Maßnahmen ist abhängig von der kontinuierlichen Aktualisierung der Detektionsparameter (Signaturen, Regelsätze). Darüber hinaus erfordern einzelne Produkte eine regelmäßige manuelle Auswertung und profitieren in besonderem Maße von eingesetzten Analyse-Spezialisten. Alternativ oder ergänzend kann die strategische

Entscheidung auch lauten, externe Dienstleister zu beauftragen. Es muss also die Frage der personellen Ressourcen geklärt sowie deren Befugnisse festlegt werden.

- ✔ **Wie viel ist dem Unternehmen der Schutz seines Erfolges wert?**
  Die wesentlichste Gestaltungs- und Einflussmöglichkeit, die Ihnen als verantwortlichem Entscheider innerhalb Ihres Unternehmens zur Verfügung steht, ist die Budgetierung der finanziellen Ressourcen für IT-Sicherheit. Negativ formuliert kann diese Entscheidung die Wirksamkeit der IT-Sicherheitsmaßnahmen massiv einschränken.

- ✔ **Welche Beschränkungen können den Mitarbeitern zugemutet werden, um den Erfolg des Unternehmens zu sichern?**
  Komfort und IT-Sicherheit korrespondieren nur schlecht miteinander. Um die identifizierten schützenswerten Informationen – bildlich gesprochen die Kronjuwelen des Unternehmens – zu verteidigen, sollte zumindest in besonders gefährdeten Teilbereichen die ausnutzbare Angriffsfläche minimiert werden. Dazu gehören auch die bei den Mitarbeitern eher unpopulären Entscheidungen, die Nutzerrechte zu beschränken, die Nutzung privater IT-Geräte (Bring your own Device (BYOD)) zu regeln oder ganze Netzbereiche voneinander oder vom Internet zu entkoppeln.

- ✔ **Welche organisatorischen und juristischen Vorbereitungen benötigt der Einsatz der (erweiterten) IT-Sicherheitsmaßnahmen?**
  In Kapitel 1.4 wurde geschildert, dass gezielte Cyber-Angriffe mehrere Phasen umfassen. Den einzelnen Schritten gelingt es häufig, die IT-Sicherheitsmaßnahmen zu umgehen oder aber sie werden nicht als Teil eines gezielten Cyber-Angriffes erkannt. Eines der wichtigsten Maßnahmenpakete ist daher das Monitoren, das Loggen und die Analyse / Korrelation der Einzelereignisse von möglichst vielen Sensoren.
  Dies erfordert jedoch verschiedene Vorbereitungen, wie die Berücksichtigung der Datenschutzbestimmungen, der Einbeziehung der Personalvertretung und klare Regelungen über die private Nutzung der unternehmenseigenen IT (Betriebsvereinbarung).
  Aufgrund der Komplexität des Themas kann es trotzdem dazu kommen, dass Indikatoren weder von den technischen Systemen noch von den eigenen Analysten erkannt werden. Dann ist es außerordentlich hilfreich, einer Information Sharing Initiative anzugehören, um relevante Benachrichtigungen zu erhalten oder anlassbezogen Fragen vertraulich stellen zu können.
  Dafür benötigt das eingesetzte IT-Sicherheitsteam wiederum die Befugnis, entsprechende Kontakte nutzen und ggf. (anonymisierte) Informationen zum eigenen Vorfall austauschen zu dürfen.

- ✔ **Was ist zu tun, wenn der Angriff dennoch erfolgreich war?**
  Auch wenn im Fall der Fälle Aufklärung, Eindämmung und Bereinigung eines Vorfalls Wochen oder sogar Monate in Anspruch nehmen können, so würde es zu unnötigen Verwirrungen und Komplikationen führen, wenn grundlegende Entscheidungen erst im Laufe des Vorfalls getroffen werden. Die Details eines Vorfalls sind nur begrenzt zu antizipieren. Trotzdem sollten Notfallpläne vorbereitet werden. Es sollten im Vorfeld sowohl Prozesse, Zuständigkeiten und Befugnisse festlegt als auch Unterstützungsmöglichkeiten eruiert werden.
  Dazu zählt einerseits die Einbindung interner Stellen, wie die des Datenschutzbeauftragten oder der Personalvertretung – soweit Mitarbeiter betroffen sind – andererseits aber auch externer Stellen, wie beispielsweise Provider, Sicherheits- und/oder Strafverfolgungsbehörden sowie spezialisierte Dienstleister (Forensik, Computer Emergency Response Team (CERT) u.a.).

- ✔ **Ist das inzwischen erreichte Schutzniveau immer noch ausreichend?**
  Um diese Leitfrage beantworten zu können, muss sowohl die allgemeine Bedrohungslage als auch die konkrete Gefährdung der IT-Sicherheit des Unternehmens bekannt sein. Die Nachbereitung erfolgreicher Cyber-Angriffe und die Auswertung abgewehrter Cyber-Angriffe bilden hierzu eine nicht zu vernachlässigende Voraussetzung. Dem gegenüber steht die regelmäßige Re-Evaluierung der IT-Sicherheitsmaßnahmen, beispielsweise in Form von Penetrationstest, Audits oder anlassunabhängigen, forensisch orientierten IT-Sicherheitsüberprüfungen. Anhand dieses Inputs kann dann die Risikoabschätzung aktualisiert und der Anpassungsbedarf bewertet werden.

2.3 Erweiterte IT-Sicherheitsmaßnahmen

Die konkrete Zusammenstellung der erweiterten IT-Sicherheitsmaßnahmen ist abhängig von den lokalen Gegebenheiten und der individuellen Gefährdungsanalyse. Dennoch gelten einige grundlegenden Empfehlungen.

- ✔ **Angriffsfläche reduzieren**
  Der Übergang von Standard-IT-Sicherheitsmaßnahmen zu erweiterten Maßnahmen ist bei dieser Empfehlung fließend. Sie beinhaltet verschiedene Ansätze. Beispielsweise sollte die Bekanntgabe interner technischer oder organisatorischer Informationen vermieden werden (Metainformationen in Dokumenten; Antwortverhalten von Diensten; etc.), um potenziellen Angreifern wenige Ansatzpunkte zu liefern. Dieses Ziel verfolgen auch solche Maßnahmen, die Schwachstellen und Sicherheitslücken schließen bzw. deren Ausnutzung verhindern sollen. Einen umfassende Systemhärtung rundet dieses Maßnahmenpaket ab.
- ✔ **Defense in Depth – Layered Defense**
  Wie in den Kapiteln 1.4 und 1.5 beschrieben versucht ein Angreifer bei gezielten Cyber-Angriffen immer tiefer in das Unternehmensnetzwerk einzudringen, um seinen Auftrag auszuführen. Da die Erfolgswahrscheinlichkeit hinsichtlich der Überwindung der Standard-IT-Sicherheitsmaßnahmen hoch ist, sollte eine vielschichtige IT-Sicherheitslösung, die auch eine laterale Ausbreitung im Netz detektiert, implementiert werden. Die verschiedenen Sensortypen und Einzelmaßnahmen sollten dabei den unterschiedlichen Phasen der „Kill Chain“ entgegen wirken.
- ✔ **Korrelation von Sensordaten**
  Durch die langfristige Ausrichtung der gezielten Cyber-Angriffe fällt es schwer, Einzelereignisse einem solchen Angriff zuzuordnen. Die Vielfalt der im vorhergehenden Aufzählungspunkt empfohlenen unterschiedlichen Ansätze sollte genutzt werden, um eine gemeinsame Korrelation zu ermöglichen und somit auch zeitlich voneinander abhängige Ereignisse zu erkennen.
- ✔ **Manuelle Auswertung**
  Gezielte Cyber-Angriffe sind oft individuell auf das Einsatzziel abgestimmt und können über neuartige Merkmale verfügen. Spezifische, eindeutige Signaturen stehen daher nur selten sofort zur Verfügung. Strebt man eine möglichst geringe Quote von False Negatives an, so führen die notwendigerweise offener definierten Detektionsparameter zu einer erhöhten Quote von False Positives. Die technische Erfassung und Bewertung von Ereignissen sollte daher unbedingt um eine manuelle Auswertung durch Spezialisten ergänzt werden.

Die beispielhaften Empfehlungen können durch eine Vielzahl von Produktlösungen, organisatorische und administrative Maßnahmen sowie durch extern erbrachte Dienstleistungen realisiert werden. Entscheidend ist jedoch, dass der eigene Bedarf möglichst präzise eruiert wird und kommerzielle Advanced Threat Protection (ATP)-Lösungen und ATP-Konzepte, die wiederum eine große Anzahl verschiedener Funktionalitäten beinhalten, genau dahingehend geprüft werden, wie gut der eigene Bedarf abgedeckt wird.

3 Fazit

Wie auch bei anderen Auseinandersetzungen entwickeln sich die Methoden der Cyber-Angreifer laufend weiter. Vorgehensweisen oder Tools, die ursprünglich bei gezielten Cyber-Angriffen eingesetzt werden, können später Anwendung bei ungezielten Angriffen finden. Die Konzeption und Umsetzung von Schutzmöglichkeiten kann dieser Entwicklung nur mit einer entsprechendem Verzögerung folgen. Um ein jederzeit ausreichendes Schutzniveau aufrecht zu erhalten, muss also die Risikoabschätzung zyklisch wiederholt und die IT-Sicherheitslösung ggf. angepasst werden.

IT-Sicherheit stellt also keinen statischen Zustand dar, sondern muss als ein ständiger Regelkreislauf, als ein andauernder Prozess verstanden werden!

4 Quellen und weiterführende Informationen

[1] BfV Arbeitsfeld Elektronische Angriffe , „Elektronische Angriffe mit nachrichtendienstlichem Hintergrund“,
http://www.verfassungsschutz.de/download/broschuere-2014-07-elektronische-angriffe-mit-nachrichtendienstlichem-hintergrund.pdf

[2] BfV Arbeitsfeld Wirtschaftsschutz, „Elektronische Attacken auf Informations- und Kommunikationstechnik“,
http://www.verfassungsschutz.de/download/faltblatt-2014-04-elektronische-attacken.pdf

[3] BSI-Veröffentlichung, „Ergebnisse der Cyber-Sicherheitsumfrage 2014“,
http://www.allianz-fuer-cybersicherheit.de/umfrage

[4] US Justizministerium, „Los Angeles Grand Jury Indicts Chinese National in Computer Hacking Scheme Allegedly Involving Theft of Trade Secrets“,
http://www.justice.gov/usao/cac/Pressroom/2014/105.html

[5] Zeit Online, „Snowden-Enthüllungen: Alles Wichtige zum NSA-Skandal“,
http://www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal/komplettansicht

[6] Symantec, „W32.Stuxnet Dossier“,
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[7] Mandiant, „M-Trends® 2014: Beyond the Breach“,
http://www.mandiant.com

[8] Trustwave , „Trustwave Global Security Report 2014“,
http://www2.trustwave.com/rs/trustwave/images/2014_Trustwave_Global_Security_Report.pdf

[9] M. Cloppert, "Security Intelligence: Attacking the Kill Chain,"
http://computer-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain/

[10] BSI-Veröffentlichung IT-Grundschutz, „IT-Grundschutz-Kataloge“,
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

[11] International Organization for Standardization, „ISO/IEC 27001 - Information security management“,
http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

[12] BSI-Veröffentlichung zur Cyber-Sicherheit, „Basismaßnahmen der Cyber-Sicherheit“,
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/risikomanagement/BSI-CS_006.pdf?__blob=publicationFile

[13] Mandiant, Veröffentlichung zu APT1,
https://www.mandiant.com/blog/mandiant-exposes-apt1-chinas-cyber-espionage-units-releases-3000-indicators/

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **info@cyber-allianz.de** gesendet werden.