Landtagswahl am 14. März 2021

Anforderungen an die Informationssicherheit

# Maßnahmen für die Ermittlung des vorläufigen Ergebnisses für die Städte, Gemeinden und Landkreise

17. Dezember 2020

**Inhaltsverzeichnis:**



## I Vorbemerkung:

In Baden-Württemberg erfolgt die Ergebnisermittlung für die Landtagswahl nach Auszählung der Stimmzettel weitgehend digitalisiert. Bereits auf der kommunalen Ebene wird für die Erfassung und Weiterverarbeitung von Teilergebnissen zunehmend spezielle Wahl-Software eingesetzt. Für die Übermittlung von Teilergebnissen werden elektronische Kommunikationswege genutzt. Integrität und Verfügbarkeit der Wahlergebnisse stehen damit in enger Abhängigkeit zur Informationstechnik. Mit Blick auf die aktuelle Gefährdungslage im Cyber-Raum sind daher bestimmte vorrangig zu ergreifende Maßnahmen notwendig, um eine korrekte und zeitgerechte Ergebnisermittlung sicherzustellen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat in enger Zusammenarbeit mit den Landeswahlleitungen sowie der Bundeswahlleitung die vorliegenden Maßnahmen für die Europawahl 2019 gemeinsam abgestimmt. In einem Vorgehensmodell angelehnt an den IT-Grundschutz des BSI hat eine Arbeitsgruppe den Wahlprozess analysiert, eine Schutzbedarfs- und Risikoanalyse vorgenommen und als Zwischenergebnis diese Maßnahmen **für Wahl- und IT-Verantwortliche der jeweiligen Ebenen** erarbeitet.

Betrachtet wurde die Ergebniszusammenstellung und –übermittlung ab dem Wahlraum nach Auszählung der Stimmzettel. Für die Auswahl der Maßnahmen wurden

bestimmte Kriterien zugrunde gelegt. Für Kommunen, Kreise und kreisfreie Städte wird ein Schutzbedarf von „Normal / Hoch / Hoch“ bzgl. Vertraulichkeit / Integrität / Verfügbarkeit zugrunde gelegt. Eine Maßnahme ist:

a) notwendig angesichts der Gefährdungslage im Cyber-Raum,
b) dem festgestellten Schutzbedarf und der Risikosituation angemessen,
c) in ihrer Komplexität überschaubar und bis zur Wahl realistisch umsetzbar,
d) und erbringt einen wesentlichen Sicherheitsgewinn.

Diese Maßnahmen sollen auch bei der Landtagswahl am 14. März 2021 Anwendung finden. Zu den „Maßnahmen für die Ermittlung des vorläufigen Ergebnisses“ werden hinsichtlich der Umsetzung der 18 Punkte des Maßnahmenkatalogs in Zusammenarbeit mit dem Informationssicherheitsbeauftragten für die Landesverwaltung Baden-Württemberg und dem Informationssicherheitsbeauftragten des Statistischen Landesamtes Baden-Württemberg zu noch erläuterungsbedürftigen Punkten ergänzende Hinweise und Erläuterungen gegeben. Diese sind beim jeweiligen Punkt des Maßnahmenkatalogs in kursiver Schrift eingefügt.

Als Hilfe für die Dokumentation der umgesetzten Maßnahmen dient die Checkliste mit Ausfüllhilfe in der Anlage.

## II 18 Maßnahmen für die Ermittlung des vorläufigen Ergebnisses

Die vorliegenden Maßnahmen betreffen folgende Schwerpunkte:

1. Benennung/Einbindung eines/einer Informationssicherheitsbeauftragten
2. Bereitstellung ausreichend personeller Ressourcen
3. Zutrittskontrolle für relevante Räume
4. Zugriffskontrolle für Wahl-Anwendungen innerhalb der jeweiligen Ebene
5. Nutzung authentischer Bezugs-Quellen für Software
6. Spezifische Nutzung der IT-Systeme für die Ergebniszusammenst. und -übermittlg.
7. Schutz vor Schadprogrammen und Viren
8. Einschränkung und Kontrolle der Cloud-Nutzung
9. Patch-Management und Sicherheits-Updates
10. Absicherung der Fernwartungszugänge für lokale IT-Systeme
11. Absicherung der Netzübergänge durch Firewalls/Sicherheitsgateways

12. Schaffung von Redundanz für IT-Systeme und Übertragungswege
13. Phishing-Schutz und Verhinderung von Datendiebstahl
14. Datenübertragung: Authentisierung + Verschlüsselung nach dem Stand der Technik
15. Monitoring der eingesetzten IT-Systeme und Anwendungen
16. Überprüfung der Notfallmaßnahmen
17. Maßnahmen für exponierte Web- und DNS-Server
18. Prüfung der Umsetzung dieser Maßnahmen

## 1. Benennung/Einbindung eines/einer Informationssicherheitsbeauftragten

Eine/Ein Informationssicherheitsbeauftragte(r) muss für die Ergebnisermittlung benannt/eingebunden und mit angemessenen Ressourcen ausgestattet werden. Der/Die Informationssicherheitsbeauftragte koordiniert und steuert die Umsetzung notwendiger Maßnahmen für die Informationssicherheit.

Die Aufgaben der/des Informationssicherheitsbeauftragten können auch von einer dritten Stelle wahrgenommen werden.

*Hinweise:*

*Es liegt im Verantwortungsbereich der Gemeinde bzw. des Landkreises für die Aufgabe „Vorbereitung und Durchführung der Landtagswahl“ einen Ansprechpartner zu benennen, der für die Initiierung der Umsetzung der Maßnahmen und für die Ermittlung des Umsetzungstandes zuständig ist. Der Aufgabenbereich ist auf den Prozess der Wahlergebniszusammenstellung und -übermittlung begrenzt.*

*Die Aufgabe kann z. B. übertragen werden auf*

- *einen in der Gemeinde bzw. im Landratsamt bereits bestellten Informations-sicherheitsbeauftragten,*
- *den Wahlleiter,*
- *einen sonstigen Mitarbeiter der jeweiligen Behörde,*
- *einen IT-Dienstleister,*
- *eine Nachbargemeinde, die die Aufgabe federführend für eine Gemeinde oder einen Verbund aus Gemeinden übernimmt (Interkommunale Zusammenarbeit).*

*Der Aufbau oder Betrieb eines Informationssicherheitsmanagements nach BSI IT-Grundschutz ist hierfür nicht erforderlich. Soll die Aufgabe des Informations-sicherheitsbeauftragten durch einen IT-Dienstleister oder den IT-Administrator*

*übernommen werden, könnte es ggf. zu Interessenkollisionen kommen. Dies sollte vermieden werden.*

## 2. Bereitstellung ausreichend personeller Ressourcen

Es muss sichergestellt werden, dass für Organisation und Durchführung der Ergebnisermittlung ausreichend Personal und praktikable Vertretungsregelungen vorhanden sind.

## 3. Zutrittskontrolle für relevante Räume

Für alle Räume mit Ausnahme des Wahlraums (Brief, Urne), die unmittelbar im Zusammenhang mit der Ergebniszusammenstellung und –übermittlung benutzt werden, müssen wirksame physische Zutrittskontrollen eingerichtet werden, um sicherzustellen, dass nur für autorisiertes Personal ein Zutritt möglich ist.

*Hinweise:*

*Es muss gewährleistet sein, dass unberechtigte Personen die unmittelbar zur Ergebniszusammenstellung und -übermittlung genutzten Räume nicht betreten können. Der Zutritt zu diesen Räumen sollte geregelt sein und kontrolliert werden. Weitere Personen dürfen erst nach Prüfung der Notwendigkeit Zutritt zu den betreffenden Räumen erhalten. Es empfiehlt sich daher, den Kreis der zutrittsberechtigten Personen vor der Landtagswahl konkret zu benennen und zu dokumentieren.*

## 4. Zugriffskontrolle für Wahl-Anwendungen innerhalb der jeweiligen Ebene

Für den Zugriff auf alle IT-Anwendungen, die für die Ergebniszusammenstellung innerhalb der jeweiligen Ebene eingesetzt werden, muss eine vorherige Authentisierung (Besitz oder Passwort) erfolgen. Hierfür wird vorausgesetzt, dass eine wirksame physische Zutrittskontrolle für die unter 3. genannten Räumlichkeiten etabliert ist, um sicherzustellen, dass nur für autorisiertes Personal ein Zugriff möglich ist. Falls eine wirksame physische Zutrittskontrolle nicht etabliert werden kann, sollte eine 2-Faktor-Authentisierung (Besitz + Passwort) für den Zugriff auf IT-Anwendungen erfolgen.

*Hinweise:*

*Der Zugriff auf die für die Ergebniszusammenstellung genutzten Wahl-Anwendungen darf nur nach vorheriger Authentisierung des Nutzers, z. B. durch Anmeldung mittels eines Passwortes, möglich sein. Diese Art der Anmeldung ist ausreichend, wenn*

*gleichzeitig eine wirksame Zutrittskontrolle zu den für die Ergebniszusammenstellung und -übermittlung relevanten Räumen eingerichtet worden ist (s. Nr. 3). Ist dies nicht der Fall, sollte eine 2-Faktor-Authentisierung für die Wahlfachanwendung eingerichtet werden. Diese wird in der Regel durch die Faktoren Besitz (Token) und Wissen (Passwort) realisiert.*

## 5. Nutzung authentischer Bezugs-Quellen für Software

Software oder Software-Updates, die im Zusammenhang mit der Ergebniszusammenstellung und -übermittlung benötigt werden, sollten nur aus authentischen Quellen, vorzugsweise vom Hersteller selbst bezogen werden. Die Software oder Software-Updates müssen vor der Installation auf ihre Authentizität und Integrität überprüft werden. Hierzu sollten mindestens Prüfsummen, vorzugsweise digitale Signaturen, verifiziert werden.

*Hinweise:*

*Bei der Installation von Software oder Software-Updates, die im Zusammenhang mit der Ergebniszusammenstellung und -übermittlung stehen, sollte sichergestellt werden, dass ausschließlich unveränderte Kopien der freigegebenen Originalsoftware verwendet werden. Die Software ebenso wie die Softwareupdates sollten ausschließlich aus sicheren Quellen (z. B. Softwarehersteller, IT-Dienstleister) bezogen werden. Dies ist durch geeignete Prüfverfahren sicherzustellen. Sollten zu einem Softwarepaket Prüfsummen oder digitale Signaturen verfügbar sein, sollten diese vor der Installation überprüft werden. Die Administratoren sollten über die Bedeutung und Aussagekraft von Prüfsummen und digitalen Signaturen informiert werden.*

## 6. Spezifische Nutzung der IT-Systeme für die Ergebniszusammenstellung und -übermittlung

Es wird empfohlen, auf den eingesetzten IT-Systemen nur Software zu installieren, die für die Ergebniszusammenstellung und -übermittlung benötigt wird. Nicht benötigte Dienste und Funktionen des Betriebssystems sollten deaktiviert werden. Mit „IT-System“ sind in diesen Maßnahmen auch virtualisierte Betriebssystem-Instanzen gemeint.

*Hinweise:*

*Die Gemeinden und Landkreise sind für die von ihnen eingesetzten IT-Systeme verantwortlich. Es ist bekannt, dass vor allem Anwendungen wie E-Mail und die Internetnutzung Einfallstore für Schadsoftware sein können. Dem kann wirksam begegnet werden, indem auf den für die Ergebniszusammenstellung und -übermittlung*

*genutzten IT-Systemen nur zwingend benötigte Anwendungen und Funktionen installiert und ausgeführt werden.*
*Daher wird eine exklusive Nutzung der betreffenden IT-Systeme für die Ergebniszusammenstellung und -übermittlung empfohlen. Hierfür nicht benötigte Programme, Dienste und Funktionen sollten auf den jeweiligen Geräten nicht installiert, deinstalliert oder deaktiviert werden.*

## 7. Schutz vor Schadprogrammen und Viren

Auf allen PCs oder Server-Systemen, die für die Ergebniszusammenstellung und -übermittlung eingesetzt werden, muss eine Anti-Viren-Software (AV) mit aktuellen Signaturen eingesetzt werden. Reputationsdienste der AV-Hersteller sollten zur Verbesserung der Detektionsleistung der Viren-Schutzprogramme genutzt werden. Nach Möglichkeit sollte eine lokal replizierte Datenbank des Reputationsdienstes in eigener Verantwortung betrieben werden. In Office-Programmen sollte die Makro-Ausführung deaktiviert werden, es sei denn ein Makro ist für die Ergebniszusammenstellung erforderlich. Im Webbrowser sollte die Ausführung von Aktiven Inhalten (z.B. JavaScript) deaktiviert werden, es sei denn Aktive Inhalte werden für die Ergebniszusammenstellung oder –übermittlung benötigt.

Digitale Daten, die von einem externen Datenträger (z.B. USB-Stick oder CD) gelesen werden, müssen vor dem Öffnen auf Schadsoftware überprüft werden. Eine Schnittstellenkontrolle für USB-Ports sollte aktiv sein, um zu verhindern, dass unautorisierte USB-Sticks in das System eingebunden werden können.

*Hinweise:*

*Es wird davon ausgegangen, dass zum Schutz der gesamten IT-Systeme eine regelmäßig aktualisierte Anti-Viren-Software bei den Gemeinden und Landkreisen bereits jetzt schon im Einsatz ist und auch für alle für die Ergebniszusammenstellung und -übermittlung am Wahltag eingesetzten IT-Systeme verwendet werden kann. Reputationsdienste ergänzen die signaturbasierte Erkennung von Schadsoftware und sollten datenschutzkonform verwendet werden. Die Beschaffung/Aktivierung eines bis dato nicht vorhandenen Reputationsdienstes eigens für die Wahl ist jedoch nicht erforderlich.*

*Folgende Fragestellungen sind in diesem Zusammenhang relevant:*

- *Wird ein geeignetes System zur Erkennung und Blockierung von Schadsoftware (Virenscanner) verwendet?*
- *Werden zur Erkennung von Schadsoftware regelmäßig Updates der Virenscanner eingesetzt?*

– *Werden Reputationsdienste verwendet?*
– *Ist die Ausführung von aktiven Inhalten geregelt (z. B. Makros in Office Dokumenten)?*
– *Gibt es eine Regelung für den kontrollierten Einsatz von USB-Sticks?*
– *Gibt es einen allen Betroffenen bekannten Meldeweg für den Fall eines Virusfundes?*

*Die Nutzung der USB-Schnittstelle kann hierbei durch folgende Maßnahmen eingeschränkt werden:*

- *Organisatorische Maßnahmen*
- *Bios-Einstellungen*
- *Windows Boardmittel (Gruppenrichtlinien)*
- *Software von Drittanbietern*
- *Hardwareschutz (USB-Schlösser, Verkleben von Ports).*

## 8. Einschränkung und Kontrolle der Cloud-Nutzung

In allen IT-Anwendungen, die für die Ergebniszusammenstellung und -übermittlung eingesetzt werden, sollten ggf. integrierte Cloud-Speicher-Funktionen deaktiviert werden. Hierzu zählen in erster Linie Office-Programme. Mit dieser Maßnahme soll verhindert werden, dass Wahl-Daten in Cloud-Speicher gelangen und dort ggf. manipuliert werden können. Eine Ausnahme bilden Anti-Viren-Programme (vgl. unter Schadprogramme).

*Hinweise:*

*Die Nutzung öffentlicher Cloudspeicher (z. B. Google, Amazon, Office365-Cloud) usw. sollte deaktiviert bzw. durch geeignete Maßnahmen unterbunden werden.*

## 9. Patch-Management und Sicherheits-Updates

Herstellerseitig bereitgestellte Sicherheits-Updates müssen nach notwendigen Testläufen unverzüglich eingespielt werden.

*Hinweise:*

*Das Installieren entsprechender Patches und Sicherheitsupdates sowohl für die jeweiligen Betriebssysteme als auch für alle auf einem IT-System erforderlichen und genutzten Softwarekomponenten (Wahlsoftware; ggf. Office-Anwendungen, aber auch Java, Flash und Co.) muss gewährleistet sein.*

## 10. Absicherung der Fernwartungszugänge für lokale IT-Systeme

Für den engeren Zeitraum der Ergebniszusammenstellung und -übermittlung müssen Fernwartungszugänge grundsätzlich deaktiviert sein. Im Falle einer unabweisbar notwendigen Fernwartung in diesem Zeitraum sollte die/der Wahl-Verantwortliche der jeweiligen Ebene informiert werden. Für die Aktivierung des Fernwartungs-Zugriffs muss eine Initiierung und Freischaltung aus den lokalen IT-Systemen heraus erfolgen. Für die Authentisierung durch den Fernwartungs-Partner sollte ein Zwei-Faktor-Verfahren eingesetzt werden. Nach dem Ende der Fernwartung müssen alle aktivierten Fernwartungszugänge wieder deaktiviert werden. Die Fernwartung sollte nur über ein besonders gesichertes Fernwartungs-Gateway erfolgen, das in einer Sicherheitszone (DMZ) betrieben wird. Für die Fernwartung sollte nur Personal zum Einsatz kommen, welches sowohl vom Auftraggeber als auch vom Fernwartungsdienstleister für diese Aufgabe autorisiert worden ist.

*Hinweise:*

*Mit Fernwartung wird ein räumlich getrennter Zugriff auf IT-Systeme und die darauf laufenden Anwendungen zu Konfigurations-, Wartungs-, Reparatur- oder Kontroll-zwecken bezeichnet. Die Fernwartung kann passiv durch einen ausschließlich betrachtenden Zugang auf das IT-System bzw. die Anwendungen erfolgen oder aktiv durch direkte administrative Eingriffe in das Betriebssystem oder laufende Anwendungen. Wichtig ist, dass die Fernwartungszugänge überprüft und, falls erforderlich, Maßnahmen zu deren Absicherung umgesetzt werden. Bei Fragen zur Ausgestaltung der bei den Gemeinden und Landkreisen eingesetzten Fernwartungs-zugänge wird empfohlen, sich an den ggf. beauftragten IT-Dienstleister zu wenden. Es sind neben den klassischen IT-Systemen auch daran angebundene, unterstützende Systeme, wie Telefonanlagen zu beachten und deren Fernwartungszugänge zu überprüfen.*

## 11. Absicherung der Netzübergänge durch Firewalls/Sicherheitsgateways

Die für die Ergebniszusammenstellung eingesetzten IT-Systeme müssen durch eine wirksame Firewallstruktur von externen Netzen (z.B. Internet, Kommunalnetz, Landesnetz) getrennt werden. Jeder ein- und ausgehende Datenverkehr muss durch die Firewallstruktur geleitet werden. Eine wirksame Firewallstruktur sollte mindestens aus einer zustandsbehafteten Stateful-Inspection-Firewall bestehen. Eine Struktur aus Paketfilter – ApplicationGateway – Paketfilter (P-A-P) wird empfohlen.

*Hinweise:*

*Der Einsatz von Firewalls/Sicherheitsgateways ist Stand der Technik. Daher wird davon ausgegangen, dass bei allen Gemeinden und Landkreisen bereits Mechanismen zum Schutz des internen Netzwerks (z. B. Firewalls, Stateful-Inspection-Funktionalitäten, Intrusion-Prevention-Systeme) nach außen bestehen. Auskünfte dazu, wie die Absicherung der Netzübergänge im Einzelnen erfolgt, erteilt der IT-Dienstleister.*

## 12. Schaffung von Redundanz für IT-Systeme und Übertragungswege

Für den Fall einer Fehlfunktion oder eines Ausfalls der für die Ergebniszusammenstellung und -übermittlung eingesetzten IT-Systeme oder Übertragungswege sollten redundante Systeme und Wege im Vorfeld organisiert werden. Hierzu können zählen: ein Laptop mit UMTS-Modem oder die Vorbereitung einer telefonischen Übertragung (Handy/Smartphone) zum Beispiel mit Passwort-Authentisierung. Mit diesen mobilen und batteriebetriebenen Geräten kann die Verfügbarkeit auch bei einem lokalen Ausfall der Stromversorgung gewährleistet werden.

*Hinweise:*

*Es sollten rechtzeitig Überlegungen angestellt werden, wie bei einem Ausfall der IT-Systeme eine sichere und korrekte Ergebniszusammenstellung und -übermittlung des vorläufigen Ergebnisses am Wahlabend dennoch gewährleistet werden kann. Diese Alternativen müssen am Wahlabend zur Verfügung stehen. Hierbei handelt es sich um keine neue Anforderung. Alternative Verfahren und Übermittlungswege wurden von den Gemeinden und Landkreisen bereits in der Vergangenheit vorgehalten, zuletzt bei der Bundestagswahl 2017 und der Europawahl 2019.*

## 13. Phishing-Schutz und Verhinderung von Datendiebstahl

Für den Zugang zu einem zentralen Wahlfachverfahren über den Browser sollte die verwendete URL nur manuell eingegeben oder über ein Lesezeichen im Browser aufgerufen werden. Damit kann der irrtümlichen Eingabe von Wahlergebnissen auf gefälschten Webseiten vorgebeugt werden.

## 14.a Authentisierung bei Übermittlung per Telefon, Fax oder Bote

Bei der Übermittlung von Wahlergebnissen per Telefon, Fax oder Bote muss eine Authentisierung zum Beispiel über ein Passwort erfolgen, das im Vorfeld vereinbart

wurde. Hiermit kann verhindert werden, dass unbefugte Personen eine Übermittlung von Wahldaten vornehmen können. Im Nachgang sollten die übermittelten Wahlergebnisse ab der Gemeindeebene aufwärts über einen authentisierten zweiten Kanal verifiziert werden (z.B. Telefon mit Passwort).

### 14.b Authentisierung vor Datenübermittlung (Client-Server)

Vor der Übermittlung von Wahlergebnissen über öffentliche elektronische Kommunikationsleitungen (z.B. Internet) sollte eine 2-Faktor-Authentisierung (Besitz + Passwort), soweit vorhanden, eingesetzt werden. Hiermit kann wirksam verhindert werden, dass unbefugte Personen eine Übermittlung von Wahldaten vornehmen können.

*Hinweise:*

*Sofern die Gemeinde oder der Landkreis an das kommunale Verwaltungsnetz (KVN) angeschlossen ist, erfolgt die Ergebnisübermittlung nicht über öffentliche Netze. Gleiches gilt für die Übermittlung der Schnellmeldungen an die Dezentrale Wahldatenerfassung. Diese erfolgt über das kommunale Verwaltungsnetz und das Landesverwaltungsnetz (KVN-LVN).*

### 14.c Verschlüsselung für die Datenübermittlung (Client-Server)

Bei der Übermittlung von Wahlergebnissen über öffentliche elektronische Kommunikationsleitungen (z.B. Internet) müssen Verschlüsselungsverfahren nach dem Stand der Technik eingesetzt werden. Hierzu zählen aktuell z.B. TLS 1.2 für die Kommunikation zwischen Webbrowser und Webserver.

*Hinweise:*

*Bei der Übermittlung von Wahlergebnissen über öffentliche elektronische Kommunikationsleitungen sollte geprüft werden, ob mit vertretbarem Aufwand eine Verschlüsselung der Kommunikationsverbindungen möglich und praktikabel ist. Ist dies der Fall, sollte die Kommunikationsverbindung geeignet verschlüsselt werden.*

### 14.d Authentisierung für die Datenübermittlung per E-Mail

Bei der Übermittlung von Wahlergebnissen per E-Mail über öffentliche elektronische Kommunikationsleitungen (z.B. Internet) sollten Verfahren für Authentisierung und Integritätssicherung nach dem Stand der Technik eingesetzt werden. Hierzu zählen aktuell z.B. OpenPGP bzw. S/MIME.

Bei der Nutzung von OpenPGP oder S/MIME signiert man E-Mail-Nachrichten vor dem Versenden mit dem nicht-öffentlichen Schlüssel des Absenders (sog. Private-Key). Der Empfänger verifiziert die Signatur der empfangenen E-Mail-Nachricht anhand des öffentlichen Schlüssels des Absenders (sog. Public-Key).

*Hinweise:*

*Sofern Sender und Empfänger sich innerhalb des kommunalen Verwaltungsnetzes befinden, findet keine Übermittlung von Wahlergebnissen über öffentliche Netze (z. B. Internet) statt. Bei der Übermittlung mittels E-Mail sollte von jeder Gemeinde geprüft werden, ob diese ausschließlich über das kommunale Verwaltungsnetz erfolgt. Die Prüfung kann durch Eingabe der E-Mail-Domains von Sender und Empfänger bei www.emra.bwl.de durchgeführt werden (nur über Verwaltungsnetze erreichbar). Bei der Übermittlung von Wahlergebnissen über öffentliche Netze kann z. B. DE-Mail oder BePo eine Authentisierung und Verschlüsselung nach dem Stand der Technik gewährleisten.*

## 15. Monitoring der eingesetzten IT-Systeme und Anwendungen

Die für die Ergebniszusammenstellung und -übermittlung eingesetzten IT-Systeme, insbesondere Server-Komponenten, sollten über eine geeignete Systemüberwachungs- bzw. Monitoringlösung eingebunden werden, welche den Systemzustand und die Funktionsfähigkeit des IT-Systems und der darauf betriebenen Dienste und Anwendungen überwachen. Fehlerzustände sowie die Überschreitung definierter Grenzwerte sollten an das Betriebspersonal gemeldet werden.

*Hinweise:*

*Es sollten geeignete Maßnahmen zur Überwachung der für die Ergebniszusammenstellung und -übermittlung eingesetzten IT-Systeme, insbesondere der Server-Komponenten, installiert werden, um sicherzustellen, dass Ausfälle und Fehler schnellstmöglich den jeweils Verantwortlichen gemeldet und umgehend beseitigt werden können. Hierzu gehört z. B. die Bereitstellung einer Vor-Ort-Präsenz bzw. einer Rufbereitschaft am Wahltag bzw. Wahlabend. Falls Systeme in die Verantwortung von IT-Dienstleistern fallen, sollten ggf. Vereinbarungen zu deren Überwachung in der Wahlnacht getroffen werden.*

## 16. Überprüfung der Notfallmaßnahmen

Für Sicherheitsvorfälle im engeren Zeitraum der Wahl sollten rechtzeitig Notfallmaßnahmen vorbereitet werden. Bereits vorhandene Maßnahmen sollten überprüft und

getestet werden (z.B. Akkulaufzeit von Laptop oder Smartphone). Insbesondere müssen geeignete Melde- und Alarmierungswege festgelegt und dokumentiert sein.

Sicherheitsrelevante Ereignisse sind an die/den Wahl-Verantwortliche/n der jeweiligen übergeordneten Ebene zu melden.

Für die richtige Reaktion auf sicherheitsrelevante Ereignisse sollten kompetente Stellen eingebunden werden (z.B. Sicherheits-Team im kommunalen RZ-Dienstleister).

*Hinweise:*

*Es wird davon ausgegangen, dass die Gemeinden und Landkreise aufgrund der Erfahrungen bei vergangenen Wahlen Vorkehrungen für verschiedene Notfallszenarien getroffen haben. Sofern nicht bereits erfolgt, sollten die Vorkehrungen einschließlich der Melde- und Alarmierungswege dokumentiert und getestet werden.*

### 17.a Anti-DDoS-Maßnahmen für exponierte Web- und DNS-Server

Die folgenden 3 Schwerpunkte betreffen primär externe Server und Dienste, die für die Ergebniszusammenstellung und -übermittlung eine direkte oder mittelbare Rolle spielen und aus dem Internet oder aus Landesnetzen sichtbar/kontaktierbar sind („exponierte Server“).

Um Denial-of-Service-Angriffe (DDoS) im engeren Zeitraum der Wahl erkennen zu können, müssen exponierte Web- und DNS-Server verstärkt überwacht werden. Des Weiteren müssen notwendige Basis-Maßnahmen umgesetzt werden. Um DDoS-Angriffe mit sehr hohen Datenraten abwehren zu können, sollten externe Dienstleister eingebunden werden. Sofern exponierte Server nur in gesicherten Landesnetzen sichtbar/kontaktierbar sind, sollten Basis-Maßnahmen ausreichen.

### 17.b Prüfung der Software-Aktualität auf exponierten Web- und DNS-Servern

Exponierte Web- und DNS-Server müssen rechtzeitig vor dem Wahlzeitraum auf das Vorhandensein eines aktuellen Patch-/Software-Standes überprüft oder getestet werden. Sofern diese Server-Dienstleistungen über einen externen Hoster/Provider bezogen werden, sollten die entsprechenden Kontrollfragen an diesen externen Hoster/Provider gestellt werden.

## 17.c Prüfung der Eingabe-/Ausgabe-Validierung auf exponierten Webservern

Rechtzeitig vor dem engeren Wahlzeitraum sollte ein Test oder eine Überprüfung durchgeführt werden, ob eine wirksame Eingabe-/Ausgabe-Validierung implementiert ist, welche durch folgende Mechanismen gekennzeichnet ist:

Für alle ankommenden Daten/Zeichenketten muss die Wahl-/Webanwendung eine wirksame Eingabe-Kontrolle (sog. Validierung) ausführen, um missbräuchlich eingeschleuste Zeichenketten zu erkennen – und zu verwerfen. Die Validierung kann auch durch ein vorgeschaltetes Sicherheitsgateway erfolgen. Vorzugsweise sollte eine Validierung nach einem Whitelisting-Verfahren erfolgen, d.h. nur diejenigen Zeichenketten, die gemäß einer Positiv-Liste aus Zeichenketten-Mustern erwartet werden, dürfen die Validierung erfolgreich passieren.

## 18. Prüfung der Umsetzung dieser Maßnahmen

Der/Die Informationssicherheitsbeauftragte muss nach Abschluss der Wahlvorbereitungen die Umsetzung dieser Maßnahmen überprüfen. Das Ergebnis muss dokumentiert und dem/der Wahl-Verantwortlichen der jeweiligen Ebene berichtet werden.
*Hinweise:*

*Aufgabe des Informationssicherheitsbeauftragten ist es, nach Abschluss der Wahlvorbereitungen die unter 1 – 17 dargestellten Maßnahmen im Hinblick auf ihre Umsetzung zu überprüfen. Eine darüber hinaus gehende Kontrolle ist nicht erforderlich. Das Ergebnis der Prüfung sollte schon im eigenen Interesse in geeigneter Weise festgehalten werden. Dabei ist es zulässig, bei der Bewertung von Maßnahmen zu dem Schluss zu kommen, dass diese für die speziellen Gegebenheiten nicht erforderlich oder unzutreffend sind. Diese Schlussfolgerung wäre zu dokumentieren.*
*In welcher Form die Dokumentation der Ergebnisse der Prüfung erfolgen soll, ist nicht vorgegeben. Um die mit der Aufgabe des Informationssicherheitsbeauftragten betrauten Bediensteten der Gemeinden und Landkreise zu entlasten, wurde in Zusammenarbeit mit dem Informationssicherheitsbeauftragten für die Landesverwaltung Baden-Württemberg und dem Informationssicherheitsbeauftragten des Statistischen Landesamtes Baden-Württemberg die beigefügte Dokumentationshilfe (Checkliste mit Ausfüllhilfe) erarbeitet. In der Checkliste werden die umzusetzenden Maßnahmen im Einzelnen aufgeführt, die nach deren Erledigung abgehakt werden können. Der Ausfüllhilfe kann gleichzeitig entnommen werden, auf welche Art und Weise und durch welche Unterlagen dokumentiert werden kann, wie einzelne Maßnahmen umgesetzt worden sind.*

*Eine Übersendung der Dokumentation an die übergeordnete Ebene und die Landeswahlleiterin ist nicht erforderlich. Diesen bleibt es gleichwohl vorbehalten, im Bedarfsfall die getroffenen Vorkehrungen für die Sicherheit der Landtagswahl abzufragen.*

## Anhang

Die hier aufgeführte tabellarische Zusammenstellung enthält weiterführende Hinweise, die bei Bedarf herangezogen werden können. Über die Querverweise auf den Modernisierten IT-Grundschutz des BSI[1] wird auch ein Abgleich mit einer bestehenden Sicherheitskonzeption ermöglicht.

| Nr. wie oben | Querverweise auf Bausteine mit Sicherheitsanforderungen im Kompendium des Modernisierten IT-Grundschutz des BSI |
|---|---|
| 1 | ISMS.1.A4 |
| 2 | ORP.2.A3 |
| 3 | INF.1.A7, INF.7.A4 |
| 4 | SYS.1.1.A2, SYS.2.1.A1, SYS.1.1.A26, ORP.4.A9 |
| 5 | OPS.1.1.3.A10, APP.1.1.A1 |
| 6 | SYS.1.1.A16, SYS.2.1.A16 |
| 7 | OPS.1.1.4.A3, OPS.1.1.4.A4, OPS.1.1.4.A6, SYS.1.1.A31, OPS.1.1.4.A8, SYS.2.1.A32, SYS.2.1.A33, OPS.1.2.3.A4 |
| 8 | APP.1.1.A12 |
| 9 | OPS.1.1.3.A10 |
| 10 | OPS.2.4.A2, OPS.2.4.A3, OPS.2.4.A17, OPS.2.4.A23 |
| 11 | NET.3.2, NET.1.1.A4 |
| 12 | APP.3.2.A15, SYS.1.1.A28, SYS.1.2.2.A12 |
| 13 | SYS.3.2.1.A14 |
| 14.a | - ohne Verweis - |
| 14.b | APP.3.2.A17, SYS.1.1.A26, SYS.2.1.A37 |
| 14.c | CON.1.A3, SYS.1.1.A18 |
| 14.d | - ohne Verweis - |
| 15 | SYS.1.1.A23 |

| Nr. wie oben | Querverweise auf Bausteine mit Sicherheitsanforderungen im Kompendium des Modernisierten IT-Grundschutz des BSI |
|---|---|
| 16 | DER.4, DER.1.A3, DER.2.1 |
| 17.a | APP.3.2.A18, NET.1.1.A30 |
| 17.b | APP.3.2.A6, APP.3.6.A5 |
| 17.c | APP.3.1.A16 |

[1] www.bsi.de → Themen → IT-Grundschutz → IT-Grundschutz-Kompendium