Europawahl im Mai 2019

Anforderungen an die Informationssicherheit

Maßnahmen für die Ermittlung des vorläufigen Ergebnisses

für: Kommunen / Kreise / kreisfreie Städte[1]

03. Dezember 2018

Vorbemerkung:

In der Bundesrepublik Deutschland erfolgt die Ergebnisermittlung für die Europawahl 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 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 wird die Ergebniszusammenstellung und –übermittlung ab dem Wahlraum nach Auszählung der Stimmzettel.

Für die Auswahl der Maßnahmen werden bestimmte Kriterien 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.

[1] Für Kommunen, Kreise und kreisfreie Städte wird ein Schutzbedarf von „Normal / Hoch / Hoch“ bzgl. Vertraulichkeit / Integrität / Verfügbarkeit zugrunde gelegt.

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.

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.

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.

5. Nutzung authentischer Bezugs-Quellen für Software

Software oder Software-Updates, die im Zusammenhang mit der Ergebniszusammen-stellung 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.

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.

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.

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).

9. Patch-Management und Sicherheits-Updates

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

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.

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.

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.

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.

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.

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).

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.

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).

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.

Anhang 1

Die hier aufgeführte tabellarische Zusammenstellung enthält weiterführende Hinweise, die bei Bedarf herangezogen werden können. Über die Querverweise auf den Modernisierten IT-Grundschutz des BSI[2] 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

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

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