Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Nationales Zentrum für Cybersicherheit NCSC
Informatiksicherheit Bund

9. Juni 2023

Bericht Informatiksicherheit Bund 2022

Inhalt

1 Organisation der Informatiksicherheit in der Bundesverwaltung

Die Informatiksicherheit in der Bundesverwaltung umfasst alle Massnahmen, um einen Cybervorfall zu verhindern und auftretende Cybervorfälle rasch zu entdecken und zu bewältigen. Ein Cybervorfall ist dabei definiert als unbeabsichtigtes oder von Unbefugten beabsichtigtes Ereignis, welches die Vertraulichkeit, Integrität, Verfügbarkeit oder Nachvollziehbarkeit von Daten beeinträchtigt oder zu Funktionsstörungen führt[1].
Damit die für die Informatiksicherheit nötigen Massnahmen in der gesamten Bundesverwaltung umgesetzt werden, erlässt der Bundesrat entsprechende Verordnungen und Weisungen. Er hat zudem dem Delegierten für Cybersicherheit die Kompetenz übertragen, Informatiksicherheitsvorgaben zu erlassen.[2] Die Erarbeitung der Vorgaben erfolgt durch das Nationale Zentrum für Cybersicherheit (NCSC). Dieses wird vom Ausschuss Informatiksicherheit (A-IS), dem Konsultativorgan für Informatiksicherheitsfragen in der Bundesverwaltung, unterstützt.
Die Verwaltungseinheiten sind für die Sicherheit ihrer Informatikschutzobjekte[3] verantwortlich. Dazu prüfen sie ihre Informatikschutzobjekte regelmässig und ergreifen die notwendigen Sicherheitsmassnahmen. Zudem sind sie für die Einhaltung und die Umsetzung der Informatiksicherheitsvorgaben, der Sicherheitsverfahren und der Beschlüsse des Bundesrates, des NCSC und der Departemente beziehungsweise der Bundeskanzlei in ihrem Zuständigkeitsbereich verantwortlich.

2 Aktueller Stand der Informatiksicherheit in der Bundesverwaltung

Gestützt auf Artikel 11 Absatz 2 der Cyberrisikenverordnung (CyRV; SR 120.73) informiert der Delegierte des Bundes für Cybersicherheit das Eidgenössische Finanzdepartement (EFD) zuhanden des Bundesrates regelmässig über den Stand der Informatiksicherheit in den Departementen und der Bundeskanzlei. Dazu erstellt das NCSC jährlich den «Bericht Informatiksicherheit Bund».
Als Grundlage für den Bericht dienen die Angaben der Departemente und der Bundeskanzlei zum Stand ihrer Informatiksicherheit an das NCSC. Das NCSC hat zu diesem Zweck eine strukturierte Umfrage bei allen Informatiksicherheitsbeauftragten der Departemente und der BK durchgeführt. Zusätzlich werden im Bericht die Erfahrungen und Feststellungen des NCSC selber sowie Sicherheitsmeldungen und -berichte der bundesinternen Leistungserbringer (LE) berücksichtigt.
Basierend auf diesen Informationen stellt das NCSC zusammenfassend fest, dass der aktuelle Sicherheitsstand der Informatik in der Bundesverwaltung insgesamt der aktuellen Bedrohungslage entspricht. Bei festgestellten Vorkommnissen konnten jeweils umgehend die notwendigen Schritte eingeleitet werden. Dabei ist jedoch zu beachten, dass trotz aufwendiger Sicherheitsvorkehrungen im Bereich der Informatik jedes Unternehmen davon ausgehen muss, Opfer einer Cyberattacke zu werden. Diese Feststellung gilt auch für die Bundesverwaltung.
Nachdem das NCSC die Informatiksicherheitsvorgabe «Si001 - IT-Grundschutz in der

[1] Verordnung vom 27. Mai 2020 über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, CyRV) SR 120.73

[2] CyRV Art. 11.

[3] Anwendungen, Services, Systeme, Netzwerke, Datensammlungen, Infrastrukturen und Produkte der Informatik; mehrere gleiche oder zusammenhängende Objekte können zu einem Informatikschutzobjekt zusammengefasst werden, Art.3 Bst.h CyRV

Bundesverwaltung» vollständig überarbeitet und neu strukturiert hat, ist die Vorgabe seit dem 1. März 2022 in Kraft. Auf Basis der bisher gemachten Erfahrungen und den mit der Inkraftsetzung des Informationssicherheitsgesetzes (ISG)[4] erwarteten Änderungen werden zurzeit auch die Prozesse «P041 - Schutzbedarfsanalyse» und «P042 - ISDS-Konzept» angepasst.
Damit die Implementierung der im IT-Grundschutz bzw. in den Sicherheitskonzepten geforderten Sicherheitsmassnahmen erfolgreich nachgewiesen werden kann, müssen die dazu notwendigen Sicherheitsdokumente aktuell (nicht älter als 5 Jahre) vorhanden sein. Dies trifft für 80% der Schutzobjekte der Bundesverwaltung zu. Im Vergleich zum Vorjahr (90%) ist dieser Wert gesunken. Dies liegt daran, dass im Rahmen von Überprüfungen des Inventars in verschiedenen Verwaltungseinheiten zusätzliche Schutzobjekte identifiziert wurden, für welche nun die Sicherheitsdokumentation erstellt werden muss. Wegen der laufenden Bewirtschaftung der Inventare sind Schwankungen beim Erfüllungsgrad der Sicherheitsdokumentation nicht zu vermeiden. Der Wert von 80% zeigt aber, dass die Pflicht zur Führung von Sicherheitsdokumentationen von den Verwaltungseinheiten nach wie vor ernst genommen wird. Die Umsetzung der Sicherheitsmassnahmen sowie deren Kontrolle (Grundschutzmassnahmen sowie Massnahmen aus den ISDS-Konzepten) war zudem 2022 bei 73% aller Schutzobjekte sichergestellt (Vorjahr 70%). Diese leichte Verbesserung ist auf die vermehrten Kontrollen durch die Departemente und Verwaltungseinheiten zurückzuführen.

3 Sicherstellung der Informatiksicherheit - Faktor Mensch

Die Mitarbeitenden aller Stufen tragen eine wichtige Rolle im Bereich der Informatiksicherheit. Dementsprechend werden die Mitarbeitenden der Bundesverwaltung regelmässig im Umgang mit der Informatiksicherheit sensibilisiert und geschult.
Gut besucht wurden die vom NCSC durchgeführten Schulungen im Bereich der Informatiksicherheit. Diese Schulungen wurden im Ausbildungszentrum der Bundesverwaltung (AZB) angeboten. Sie wurden im Jahr 2022 wieder vermehrt vor Ort durchgeführt, statt wie im Vorjahr ausschliesslich online. Aufgrund der hohen Nachfrage ist vorgesehen, die Kurse im Jahr 2023 vier- statt dreimal durchzuführen.
Das NCSC veranstaltete zudem regelmässig Kurse und Sensibilisierungskampagnen, um bei den Informatiksicherheitsbeauftragten der Departemente (ISBD) und der Verwaltungseinheiten (ISBO) sowie anderen interessierten Personen der Bundesverwaltung ihr Fachwissen im Bereich der Cybersicherheit aufzubauen und dieses sicherzustellen. Dabei wurden 2022 mehrere Online-Expertenkurse zu den Themen Kryptografie mit durchschnittlich 100 Teilnehmenden, Bitcoin & Blockchain mit durchschnittlich 90 Teilnehmenden, IT-Forensik mit durchschnittlich 140 Teilnehmenden, Tor & Darknet mit durchschnittlich 140 Teilnehmenden und Kubernetes mit durchschnittlich 130 Teilnehmenden durchgeführt.

[4] Bundesgesetz vom 18. Dezember 2020 über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) BBl 2020 9975

Im Jahr 2021 und 2022 realisierte das NCSC zusammen mit der Schweizerischen Kriminalprävention jeweils eine nationale Sensibilisierungskampagne für die Bevölkerung, welche auch bei den Bundesmitarbeitenden sichtbar war. 2022 lag der Fokus der Kampagne auf dem Thema der Achtsamkeit im Internet. Mit den Schwerpunkten Phishing und Betrug wurden Themen aufgenommen, welche auch innerhalb der Bundesverwaltung von Bedeutung sind. Im 2022 haben insgesamt 40 Bundesämter in den Departementen EDI, EDA, EFD, EJPD, UVEK, VBS, WBF die Sichtbarkeit der Kampagne unterstützt.
Um das Wissen hinsichtlich Gefahren, Bedrohungen und den bewussten Umgang mit digitalen und mobilen Hilfsmitteln weiter zu fördern, hat die Bundesverwaltung zudem im 2022 ein webbasiertes Schulungsangebot, zuerst als Pilot und ab 2023 vorgeschrieben für alle neu eintretenden Mitarbeitenden, zum Thema «Informatiksicherheit in der Bundesverwaltung» erarbeitet. Dieses Modul wird allen Bundesmitarbeitenden unabhängig von ihrer Funktion und Position ermöglichen, sich eingehend mit dem Thema Informatiksicherheit zu befassen.
Um Fragen der Mitarbeitenden in den Verwaltungseinheiten betreffend der Informatiksicherheit direkt zu behandeln, verfügt die Bundesverwaltung zudem auf Stufe Departement und Bundeskanzlei über 8 Informatiksicherheitsbeauftragte (ISBD) und über 80 amtsspezifische Informatiksicherheitsbeauftragte (ISBO).
Unter der Leitung der ISBD und ISBO wurden im 2022 rund 94% der neu eintretenden Mitarbeitenden in die Belange der Informatiksicherheit eingeführt (Vorjahr 95%).
In der aktuellen Arbeitswelt arbeiten die Bundesmitarbeitenden deutlich mobiler als noch vor COVID19. Deshalb finden immer mehr digitale Hilfsmittel Einzug in die Bundesinformatik, wobei viele Gefahrenquellen im Vorgang mittels sicheren VPN-Verbindungen auf die Systeme der Bundesverwaltung ausgeschlossen werden.

4 Sicherheitsvorfälle und Schwachstellen

4.1 Sicherheitsvorfälle

Die IT-Infrastruktur der Bundesverwaltung ist permanent äusserst vielfältigen Cyberangriffen ausgesetzt. Im Berichtsjahr 2022 gab es jedoch keine Vorfälle, die das ordnungsgemässe Funktionieren der Bundesverwaltung gefährdet haben. Die Sicherheitsteams der Leistungserbringer der Bundesverwaltung konnten die Cyberangriffe erfolgreich verhindern und setzen dazu eine Vielzahl an Massnahmen um. Das Computer Security Incident Response Team (CSIRT) des Bundesamtes für Informatik und Telekommunikation (BIT) sowie das Cyber Fusion Center (CFC) der Führungsunterstützungsbasis (FUB) weisen für das Jahr 2022 zur Veranschaulichung dieser Massnahmen folgende Aktivitäten zur Verhinderung von Cyberangriffen auf ihre Systeme aus:

- Das CSIRT BIT hat 2022 insgesamt 116 Aufträge zu Domainsperrungen ausgelöst. Auslöser dieser Sperrungen war praktisch immer der Missbrauch von Internetseiten zur Malware-Verbreitung bzw. zu Phishing-Kampagnen. Diese Sperrungen erfolgten durch das BIT CSIRT in Zusammenarbeit mit dem GovCERT des NCSC. Zusätzlich wurde seitens BIT gemeldet, dass einige Firewalls für gewisse Netze eine direkte Verbindung ins Internet zuliessen. Die Firewall-Regeln, die das erlaubten, wurden nach Bekanntwerden rasch angepasst und die Sicherheitslücken konnten so umgehend geschlossen werden. Ausserdem wurde auf einigen Servern (v. a. Linux) mangelhafter Malware-Schutz festgestellt. Die Betreiber wurden informiert so dass der Mangel zeitnah behoben werden konnte.

- Das Cyber Fusion Center (CFC) der FUB hat 2022 insgesamt 559 Ereignisse bearbeitet. Diese Ereignisse reichten von einem Malware-Verdacht bis hin zu Phishing-Versuchen. Allgemein gesehen gab es jedoch keine kritischen Sicherheitsvorfälle, weshalb die Gesamtsituation als eher ruhig beschrieben werden kann. Diese ruhige Situation widerspiegelt sich auch in den Vorfallzahlen und hält weiter an.

Während der Berichtsperiode haben sich einige Distributed Denial of Services[5] (DDoS) Angriffe ereignet, welche den Informatiksicherheitsbeauftragten des Bundes aufzeigten, dass dieses Thema immer noch wichtig ist. DDoS-Angriffe zielen darauf ab, durch zahlreiche, zeitgleiche Zugriffe, eine Überlastung und damit Nicht-Verfügbarkeit von Webservern, Online-Services oder ganzer Netzwerke zu erreichen. Als Gegenmassnahme für diese Angriffe, wurde neu eine Web Application Firewall (WAF) eingesetzt, auf der eine Zugriffslimite («Rate Limiting») konfiguriert worden ist. Diese schränkt die Anzahl Anfragen pro IP-Adresse ein und schützt die Bundesverwaltung somit gegen diese Art von Angriffen.

4.2 Schwachstellen

Das NCSC wurde am 29. September 2021 von der unabhängigen US-Organisation MITRE[6] neu als Autorisierungsstelle und damit zur Vergabe von Common Vulnerabilities and Exposures (CVE)[7]-Nummern anerkannt. In dieser Rolle ist das NCSC zuständig für die Erstellung und Veröffentlichung von Informationen über die ihm gemeldeten Schwachstellen und der zugehörigen CVE-Einträge. Das NCSC ist damit nicht nur offizielle Anlaufstelle zum Melden von Sicherheitslücken in der Schweiz, sondern führt auch deren CVE-Nummern für den internationalen Austausch. Seit der Anerkennung wurden von NCSC 30 CVE publiziert, 15 davon im Berichtsjahr 2022.
Ausserhalb der CVE-Veröffentlichung bearbeitet das NCSC auch Meldungen über verwundbare Systeme für die Bundesverwaltung sowie für externe Stellen (Kantone, Gemeinden, Betreiber kritischer Infrastrukturen und Schweizer Unternehmen). Schwachstellen in Applikationen und Systemen sind eine der Hauptursachen für Sicherheitsvorfälle, weshalb eine schnelle Identifikation und Behebung auch für die Bundesverwaltung enorm wichtig ist. Insgesamt hat das NCSC im Jahr 2022, 27 Hinweise auf hochgradige und kritische Schwachstellen veröffentlicht. In der Berichtsperiode wurden u. a. folgende Schwachstellen mit einer hohen Kritikalität behandelt:

Untersuchungen von Smartphone Apps
Im Zusammenhang mit der Fussball-Weltmeisterschaft in Katar hat der für die Geschäftshandys zuständige Bereich DTI der Bundeskanzlei - in Absprache mit dem Nationalen Zentrum für Cybersicherheit (NCSC) und dem Bundesamt für Informatik und Telekommunikation (BIT) - zum Schutz der Angestellten und der Daten des Bundes im November 2022 in den Geschäftshandys zwei Apps gesperrt.
Die zur Einreise nach Katar benötigten Apps «Ehteraz» und «Hayya to Qatar 2022» verlangten weitreichenden Zugriff auf Daten. Aufgrund dessen hat das NCSC in Zusammenarbeit mit Fachstellen des Bundes technische Prüfungen der Apps durchgeführt. Als Vorsichtsmassnahme wurde entschieden, die beiden Apps auf den Geschäftshandys zu sperren.

[5] Denial of Service bezeichnet in der Informationstechnik die Nichtverfügbarkeit eines Internetdienstes, der eigentlich verfügbar sein sollte. Häufigster Grund ist die Überlastung des Datennetzes. Der Hauptunterschied zwischen DDoS- und DoS-Angriffen besteht darin, dass erstere mehrere Systeme nutzen und deshalb die Netze und Systeme mit höherem Datenvolumen überlasten kann.

[6] Die MITRE Corporation ist eine Organisation zum Betrieb von Forschungsinstituten im Auftrag der Vereinigten Staaten, die durch Abspaltung vom Massachusetts Institute of Technology (MIT) entstanden ist. Sie wird als Non-Profit-Organization geführt.

[7] Common Vulnerabilities and Exposures ist ein Referenzier-System zur Benennung und Kritikalitätsbezeichnung von Schwachstellen in Computersystemen.

Atlassian Confluence Server

Kurz nach Bekanntwerden der kritischen Schwachstelle im Produkt Atlassian Confluence Server[8] Anfang Juni 2022, wurde diese in der Bundesverwaltung umgehend durch Aktualisierungen behoben. Ein Angreifer hätte diese Schwachstelle ausnutzen und damit als nicht-authentifizierter Benutzer beliebigen Code auf den Confluence-Servern ausführen können. Die Systeme wurden im Anschluss auf allfällige Hinweise einer Kompromittierung überprüft. Da keine Anzeichen einer Kompromittierung festgestellt wurden, konnten die Server unmittelbar danach wieder in Betrieb genommen werden.

Microsoft Exchange Server

Ende September 2022 wurde von einem vietnamesischen Cybersicherheitsunternehmen[9] erstmals über zwei kritische Zero-Day-Schwachstellen[10] in Microsoft Exchange Servern berichtet. Diese können in Kombination ausgenutzt werden und werden als «ProxyNotShell» bezeichnet. Diese Schwachstellen wurden weltweit bereits aktiv ausgenutzt, noch bevor ein offizieller Patch verfügbar war. In diesen Fällen ist es besonders wichtig, schnell zu reagieren und den Empfehlungen – die bis zur Abschaltung des anfälligen Systems gehen können – zu folgen, bis beispielsweise ein offizieller Patch verfügbar ist.
Mit der Ausnutzung der beiden Sicherheitslücken[11] hätten Angreifer beispielsweise Zugang zu verwundbaren Systemen erhalten und Schadcode aus der Ferne über das Internet ausführen können. Es bestand daher dringender Handlungsbedarf sowohl in der Bundesverwaltung als auch in anderen Unternehmen.
Die Sicherheitslücken liessen sich aber gemäss Informationen des Herstellers nur mit einem bereits am Server authentifizierten Konto ausnutzen, was die Wahrscheinlichkeit eines Angriffs reduzierte.
Am 8. November 2022 hat Microsoft entsprechende Updates veröffentlicht, um die Schwachstelle zu beheben. Diese wurden in der Bundesverwaltung umgehend eingespielt. Zudem wurden alle verwundbaren Systeme einer eingehenden Prüfung unterzogen. Es wurden jedoch keine Hinweise einer Kompromittierung gefunden.

Schwachstelle in FortiOS VPN

Der Hersteller von Sicherheitsprodukten Fortinet informierte am 13. Dezember 2022 über eine kritische Sicherheitslücke[12] im Produkt FortiOS VPN. Durch das Ausnutzen der Schwachstelle konnten nicht authentifizierte Benutzer verwundbare Geräte aus der Ferne zum Absturz bringen oder möglicherweise auch Schadcode ausführen. Direkt nach Bekanntgabe dieser Schwachstelle hat die Bundesverwaltung reagiert und die betroffenen Systeme innerhalb von zwei Tagen aktualisiert und auf allfällige Hinweise einer Kompromittierung überprüft. Es wurden jedoch auch hier keine kompromittierten Systeme gefunden.

Mögliche Sicherheitslücken bei Hilfsmitteln zu Video-Konferenzen

Homeoffice hat sich als fester Bestandteil in der Arbeitswelt etabliert und dadurch finden Sitzungen und Workshops oftmals online statt. In der Bundesverwaltung ist geregelt, welche «Video- Conferencing-Lösungen» genutzt werden dürfen. Als zusätzliche Hilfsmittel bei Video-Konferenzen kommen jedoch auch kommerzielle und kostenlose Online-Tools aus dem Internet zum Einsatz wie z. B. Whiteboards, Umfrage-Tools, Planungs-Tools, virtuelle Pinboards.

---

[8] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26134

[9] https://ncsgroup.vn/blog/warning-new-attack-campaign-utilized-a-new-0day-rce-vulnerability-on-microsoft-exchange-server-12715.html

[10] Als Zero-Day-Lücken werden Schwachstellen benannt für die es noch kein Patch gibt, durch den die Ausnutzung einer Schwachstelle verhindert wird.

[11] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41040
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41082

[12] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42475

Solche Hilfsmittel stellen potenziell ein Risiko für Geräte der Bundesverwaltung dar, da diese von Cyberkriminellen als Angriffsvektor ausgenutzt werden können.
Um diesem Sicherheitsrisiko entgegenzutreten, wird zurzeit im Rahmen der Strategischen Initiative 2 (SI-2) Kundenzentrierung vom Bereich Digitale Transformation und IKT-Lenkung der Bundeskanzlei (BK-DTI) eine Leitlinie mit Weisungscharakter für kollaborative Tools für die agile Zusammenarbeit erstellt. Zusätzlich sind die ISBO/ISBD beauftragt, die Mitarbeitenden entsprechend zu sensibilisieren.

Kritische Schwachstelle bei Citrix

Der Hersteller Citrix hat am 13. Dezember 2022 über eine kritische Schwachstelle[13] in seinen Produkten Citrix ADC und Citrix Gateway informiert. Es handelt sich um eine Authentifizierungsschwachstelle, die ebenfalls das Ausführen von Schadcode über das Internet ermöglicht hätte. Aufgrund der Kritikalität wurden die Systeme der Bundesverwaltung innerhalb von wenigen Tagen gepatched, u. a. war auch das Mobile Device Management (MDM) System der Bundesverwaltung davon betroffen.

4.3 Veraltete Systeme / Netzwerkprotokolle

Das NCSC stellt fest, dass in der Bundesverwaltung nach wie vor veraltete Systeme und Netzwerkprotokolle eingesetzt werden. Dies erhöht das Risiko von Sicherheitslücken substantiell.

Die Verantwortung für den Ersatz veralteter Systeme und Netzwerkprotokolle liegt bei den Anwendungsverantwortlichen der Leistungsbezüger in den Ämtern und Departementen. Diese haben aufgrund von Priorisierungen jedoch nicht in jedem Fall die nötigen Ressourcen um die Protokolle abzulösen und sind sich nach Einschätzung des NCSC nicht immer bewusst, welche Sicherheitsrisiken sie damit eingehen. Zwar werden die Risiken in den Sicherheitsberichten der Verwaltungseinheiten ausgewiesen und von den Geschäftsleitungen getragen, faktisch dürfte es aber aufgrund der technischen Komplexität den wenigsten Verantwortungsträgerinnen und -trägern bewusst sein, welche Informationssicherheitsrisiken sie tatsächlich akzeptieren. Diese Situation kann zu einer Kumulierung von Sicherheitsrisiken führen. Im Sinne seiner koordinierenden Führungsverantwortung im Bereich Cybersicherheit wird das NCSC diese Problematik verfolgen.

Zu beachten ist jedoch, dass einige veraltete Systeme – vor allem in Labor Umgebungen – bereits in isolierten Netzwerken untergebracht sind und keinen Netzwerkverkehr mit Bundesnetzen haben.

Bereinigung veralteter Protokollversionen TLS1.0/1.1

Aus einer Erhebung des BIT wurden unterschiedliche Schnittstellen identifiziert, die das Authentisierungs- und Verschlüsselungsprotokoll der veralteten Protokollversionen «TLS 1.0 und TLS 1.1» verwenden. TLS[14] ist ein Protokoll, welches die Vertraulichkeit und Integrität bei Datenübertragungen in Netzwerken sicherstellen soll. Aufgrund der Tatsache, dass TLS 1.0 und TLS 1.1 veraltete Protokollversionen sind und Schwachstellen aufweisen, ist der Betrieb von Systemen, welche diese Protokollversionen verwenden, in der Bundesverwaltung nicht mehr gestattet. Ein Grossteil dieser Protokolle verbirgt sich jedoch nicht in den klassischen https- Verbindungen[15], sondern in proprietären Protokollen, welche ebenfalls TLS nutzen. Die grosse Verbreitung von TLS in den unterschiedlichsten Produkten stellt deshalb eine Herausforderung dar und eine Bereinigung dieser Situation ist entsprechend aufwendig und zeitintensiv (z.T. bis Ende 2026).

[13] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27518

[14] Englisch: Transport Layer Security

[15] https: Hypertext Transfer Protocol Secure ist ein Kommunikationsprotokoll im World Wide Web, mit dem Daten abhörsicher übertragen werden können.

Zusammengefasst muss gesagt werden, dass zurzeit noch 1786 Systeme aktiv mit den veralteten Protokollversion in der Bundesverwaltung im Einsatz sind. Positiv zu erwähnen ist hingegen, dass innerhalb des Berichtsjahres 2022 etwa so viele veraltete TLS 1.0 und 1.1 Protokollversionen aktualisiert werden konnten wie derzeit noch offen sind. Solange mit den veralteten TLS-Versionen nur bundesintern kommuniziert wird und die betroffenen Systeme nicht öffentlich aus dem Internet erreichbar sind, ist das Risiko als gering anzusehen.

Empfehlungen im Umgang mit veralteten Protokollversionen
Das NCSC empfiehlt den Leistungserbringern folgendes Vorgehen:
Für eine flächendeckende und konsequente Bereinigung der veralteten Protokollversionen ist eine komplette Blockierung dieser zu veranlassen und ggf. kontrolliert und gesondert - für jene welche zwingend benötigt werden – mit einer entsprechenden Migrationsplanung wieder zuzulassen. Eine Lösung für solche Systeme könnte darin bestehen, diese z. B. in eine isolierte Netzwerkumgebung zu verlagern, so dass kein Netzwerkverkehr mit anderen IT-Systemen der Bundesverwaltung generiert wird.

5 Zusammenfassung der internen Leistungserbringer

Generell gesehen war das Berichtsjahr 2022 für die bundesinternen IT-Leistungserbringer aus Sicht Cyberbedrohungen ein relativ ereignisarmes Jahr. Hingegen ist global gesehen die Cybersicherheit noch mehr in den Fokus gerückt. Es sind immer noch ähnliche Themen wie im Jahr 2021 wichtig und aktuell. Zudem hat es sich wiederum gezeigt, dass funktionierende Lifecycles und Patch-Management sehr wichtige Komponente zum Schutz der IT-Systeme sind. Sehr viele Angriffe zielen auf Komponenten ab, für die es seit einiger Zeit entsprechende Patches oder Workarounds gegeben hat.
Als wichtige Herausforderung identifizieren die Leistungserbringer die Überprüfung von Zugriffsrechten in den Systemen und die Sicherstellung der Informatiksicherheit bei Entwicklungsumgebungen, damit Sicherheitsfehler nicht in die Produktivumgebung übertragen werden.
Mit der Zunahme der Nutzung von Cloud-Diensten drängt sich ausserdem zusehends die Frage nach einer sicheren und effektiven Zusammenarbeit auf, z. B. bei Abklärungen nach einem Vorfall mit unterschiedlichen Cloud-Anbietern. Auch aufgrund der aktuellen angespannten internationalen Lage machen sich die Leistungserbringer Gedanken über die Auswirkungen bei einer Strom-Mangellage und der Verfügbarkeit ihrer IT-Systeme.
Als Teil der Etablierung von DevSecOps[16] für die Umsetzung von agilen Projekten und die entsprechende Einbettung der Informatiksicherheit, ist der Einsatz von sogenannten Security Champions bei mehreren Leistungserbringern gestartet worden. Mit der Rolle als Security Champions unterstützen die Projektmitarbeitenden die Produkt-Owner und Projektleiter, damit die Sicherheit als Teil der Entwicklung mit in die Projekte einfliesst und dabei automatisch Bestandteil der Produkte (Security by Design Ansatz) wird. Dies wird in agilen Projekten immer wichtiger, da die Weiterentwicklung an Produkten laufend durchgeführt wird. Dabei ist die Informatiksicherheit nicht mehr an klassische Meilensteine geknüpft, sondern ein Entwicklungsprozess, der laufend überwacht werden muss.
Das Programm «Mitigation Credential Theft – MCT» ist im Berichtsjahr in der Phase «Umsetzung» bei den Leistungserbringern angelangt. Dabei gilt es unter anderem zu verhindern, dass Software ungewollt oder unerwünscht installiert wird.
Aus diesem Grund wurde die Einführung einer Privilege Access Manager (PAM) Software gemäss neuem IT-Grundschutz (Version 5) und auch gemäss der Einsatzrichtlinie E033 (Identitätsschutz) für alle Systeme der Büroautomation vorausgesetzt. Im Jahr 2022 wurde

[16] DevSecOps ist ein sogenanntes Kofferwort, welches sich aus den englischen Begriffen „Development“, „Security“ und „Operations“ zusammensetzt.

dafür ein entsprechendes Werkzeug für das Management dieser Infrastruktur eingeführt und der produktive Betrieb für die Administration der Windows-Server gestartet. Ebenso wurde ein Proof-of-Concept (PoC) für die Linux-Systeme erstellt, so dass auch für das Management der Linux-Systeme im Jahr 2023 der produktive Betrieb in Angriff genommen werden kann.

6 Stärkung der Informatiksicherheit

Aus der laufenden Lagebeurteilung und den Sicherheitsvorfällen leitet die Bundesverwaltung die entsprechenden Sicherheitsmassnahmen ab. Nebst allfälligen Sofortmassnahmen, werden Massnahmen auf rechtlicher, organisatorischer und technischer Seite nachhaltig und verhältnismässig erarbeitet und umgesetzt.

6.1 Massnahmen 2022

Zur Stärkung der Informatiksicherheit haben alle Departemente und die Bundeskanzlei im 2022 Massnahmen umgesetzt bzw. entsprechende Aktionen durchgeführt.

So wurde unter anderem Folgendes umgesetzt:

- die Mitarbeitenden wurden über verschiedene Massnahmen, wie z. B. die nationale Sensibilisierungskampagne S-U-P-E-R[17], Phishing-Kampagnen, oder im Intranet verfügbar gemachte Informationen zu Themen wie Home-Office, Auslandreisen und Datenschutz (z. T. überdepartemental) sowie die Cybersicherheit generell sensibilisiert;
- das Projekt Endpoint Detection and Response (EDR)[18] beim EDA wurde gestartet. Ziel ist die Einführung einer EDR-Lösung auf möglichst vielen Systemen innerhalb der Bundesverwaltung;
- das Programm Security Champions für agile Projektumsetzung wurde eingeführt;
- das Projekt DigiSec, mit dem Ziel eine Anwendung zur Umsetzung eines ISMS in der Bundesverwaltung vorzulegen, wurde gestartet;
- die Informationssicherheits-Management-Systeme (ISMS) in verschiedenen Verwaltungseinheiten wurden weiter ausgebaut;
- die externe Zertifizierung nach ISO 27001, um die Informatiksicherheit zu gewährleisten, wurde bei gewissen Verwaltungseinheiten fortgesetzt;
- das Bug-Bounty-Programm der Bundesverwaltung wurde durch das NCSC gestartet[19];
- die Etablierung des «securitxt.txt»-Standards auf den Internetseiten der Bundesverwaltung zur Verbesserung des Meldeflusses von Schwachstellen[20] wurde lanciert;
- personelle Ressourcen für die Informatiksicherheit wurden weiter ausgebaut;
- das Programm zur Verhinderung von Identitätsdiebstahl und -Missbrauch «Mitigation Credential Theft – MCT» wurde fortgeführt;
- der Makrosignatur-Service, welcher Risiken von MS-Office-Makros ausgehend reduziert, wurde eingeführt.

[17] Sensibilisierungskampagne S-U-P-E-R: https://www.s-u-p-e-r.ch/de/

[18] Mit dem englischen Begriff Endpoint Detection and Response (EDR) wird eine Kategorie von Werkzeugen und Techniken beschrieben, die helfen aktive Bedrohungen auf Endgeräten rasch zu erkennen und darauf zu reagieren.

[19] Bug-Bounty-Programme zur Erhöhung der Cyberresilienz in der Bundesverwaltung (admin.ch) https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/medienmitteilungen/newslist.msg-id-89868.html

[20] https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-behoerden/aktuelle-themen/security-txt.html

6.2 Massnahmen 2023

Zur kurz- und mittelfristigen Stärkung der Informatiksicherheit haben die Departemente und die Bundeskanzlei u. a. folgende Massnahmen geplant:

- Erweiterung der monatlich wiederkehrende Web Scans von sämtlichen im Internet exponierten Webseiten, um bekannte Schwachstellen zu beseitigen.
- Weitere geschäftskritische Anwendungen werden in das Bug-Bounty-Programm aufgenommen, wodurch Anwendungen proaktiv auf mögliche Schwachstellen geprüft werden.
- Durchführen von Awareness Schulungen / Sensibilisierungskampagnen.
- Systeme, welche vom Internet zugänglich sind, werden durch weitere Penetration-Tests untersucht und die entsprechenden Massnahmen umgesetzt.
- Etablieren eines ISMS gemäss ISG, angelehnt an ISO 27001.
- Ablösung der bundeseigenen Verschlüsselungssoftware «SecureCenter» durch die Nachfolgelösung «CHCrypt».

NCSC wird in ein Bundesamt überführt

Die Bedeutung der Cybersicherheit hat in den vergangenen Jahren auf allen Ebenen stark zugenommen. Dabei ist die Gewährleistung der Cybersicherheit zu einer unverzichtbaren Aufgabe des Bundes geworden. Aufgrund der zunehmenden Bedeutung des NCSC hat der Bundesrat am 2. Dezember 2022 beschlossen, das NCSC in ein Bundesamt zu überführen. Dazu wird das NCSC neu im VBS angesiedelt werden. Das NCSC übernimmt weiterhin die Kernaufgaben der Cybersicherheit, wozu die Unterstützung der Kritischen Infrastrukturen bei der Bewältigung von Cybervorfällen, die Bereitstellung einer nationalen Anlaufstelle für Bevölkerung und Unternehmen, die Verbreitung von Informationen und Warnungen zu Cyberbedrohungen und entsprechenden Schutzmassnahmen, die Sensibilisierung der Bevölkerung, das Management von Schwachstellen sowie der Schutz der Systeme der Bundesverwaltung gehören[21].

[21] NCSC als Bundesamt: https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-92048.html