Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Nationales Zentrum für Cybersicherheit NCSC
Informatiksicherheit Bund

21. April 2021

Stand der Informatiksicherheit in der Bundesverwaltung 2020

1 Informatiksicherheit in der Bundesverwaltung

Die Informatiksicherheit in der Bundesverwaltung umfasst alle Massnahmen, um einen Cybervorfall zu vermeiden. Dabei geht es darum, ein unbeabsichtigtes oder von Unbefugten beabsichtigtes Ereignis, welches die Vertraulichkeit, Integrität, Verfügbarkeit oder Nachvollziehbarkeit von Daten beeinträchtigt oder zu Funktionsstörungen führt, zu verhindern[1].
Der Bundesrat erlässt dazu Verordnungen und Weisungen über den Schutz der Bundesverwaltung vor Cyberrisiken. Der Delegierte für Cybersicherheit erlässt Informatiksicherheitsvorgaben.
Zudem fungiert der Ausschuss Informatiksicherheit (A-IS) als Konsultativorgan für das Nationale Zentrum für Cybersicherheit (NCSC) betreffend Informatiksicherheitsfragen in der Bundesverwaltung.

Die Verwaltungseinheiten (Ämter) sind für den Schutz ihrer Informatiksysteme, Anwendungen und Daten (Schutzobjekte) verantwortlich. Dazu prüfen sie ihre Schutzobjekte 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.

Zu einzelnen, spezifischen Angriffen oder Sicherheitslücken werden im vorliegenden Sicherheitsbericht keine Angaben gemacht. Letztere können einem potentiellen Angreifer direkt in die Hand spielen und damit die gesamte Informatik der Bundesverwaltung gefährden. Deshalb werden auch keine Angaben zu den einzelnen Departementen oder Ämtern bekannt gegeben.

2 Aktueller Stand der Informatiksicherheit in der Bundesverwaltung

Die Departemente, die Bundeskanzlei sowie die Parlamentsdienste berichten dem NCSC zum Jahresende über den Stand der Informatiksicherheit (Selbstdeklaration basierend auf einer strukturierten Umfrage). Die Angaben werden durch das NCSC plausibilisiert.

Basierend auf den Angaben 2020 stellt das NCSC zusammenfassend fest, dass der aktuelle Sicherheitsstand der Informatik in der Bundesverwaltung insgesamt der aktuellen Bedrohungslage angemessen ist.
Dabei ist jedoch zu beachten, dass trotz aufwendiger Sicherheitsvorkehrungen im Bereich der IT, jedes Unternehmen davon ausgehen muss, Opfer einer Cyber-Attacke zu werden (Assume-Breach-Paradigma[2]). Diese Feststellung gilt auch für die Bundesverwaltung.

Damit die im IKT-Grundschutz bzw. in den Sicherheitskonzepten geforderten Sicherheitsmassnahmen erfolgreich implementiert werden können, müssen die dazu notwendigen Sicherheitsdokumente aktuell (nicht älter als 5 Jahre) vorhanden sein. Im Bundesdurchschnitt sind bei 90% (Wert wie Vorjahr) aller Schutzobjekte die entsprechenden Sicherheitsdokumente vorliegend. Dies stellt grundsätzlich einen guten Wert dar.
Die Gültigkeit der vorhandenen Sicherheitsdokumente liegt im Bundesdurchschnitt bei 96%

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

[2] Der Begriff 'Assume-Breach-Paradigma' kennzeichnet die Tatsache, dass trotz aufwendiger Sicherheitsvorkehrungen im Bereich der IT jedes Unternehmen davon ausgehen muss, einmal Opfer einer Cyber-Attacke zu werden.

(Vorjahr 82%). Diese wesentliche Steigerung kann auf die Bereinigungs- und Aktualisierungsaktionen (auch basierend auf dem Bundesratsbeschluss zum letztjährigen Bericht) zurückgeführt werden.

Die Umsetzung der Sicherheitsmassnahmen (Grundschutzmassnahmen sowie Massnahmen aus den ISDS-Konzepten) war 2020 bei rund 78% aller Schutzobjekte sichergestellt. Davon wurden bei rund ¾ der entsprechenden Anwendungen die Umsetzung der Sicherheitsmassnahmen nachkontrolliert.
Die geforderten Kontrollen dieser Umsetzung erreichen jedoch noch nicht den gewünschten Stand.
Um den Stand bei der Umsetzung und Kontrolle der geforderten Sicherheitsmassnahmen weiter zu verbessern, wurden die nötigen Massnahmen angeordnet.

Im Zusammenhang mit dem Arbeiten aus dem Homeoffice, als Folge der Corona-Massnahmen, zeigten sich – vor allem zu Beginn – Probleme bei den Kapazitäten für den Fernzugriff auf das Bundesnetz (der Bedarf nach Zugriffen stieg um den Faktor 10). Die Kapazitäten konnten durch die verschiedenen Leistungserbringer jedoch rasch erhöht werden, so dass das Arbeiten aus dem Homeoffice grundsätzlich gut funktionierte und weiterhin funktioniert. Bisher wurden keine Sicherheitsvorfälle bekannt, welche auf den Homeoffice-Betrieb zurückzuführen sind. Der Versuch einzelner Mitarbeitenden, auf den Bundesgeräten eigene Software zu installieren, konnte durch die Sicherheitsmassnahmen des Bundesamtes für Informatik und Telekommunikation (BIT) unterbunden werden. Auch mussten einige vom BIT angebotene Produkte aus Sicherheitsgründen wieder aus dem Angebot genommen werden.

Eine Pendenz besteht nach wie vor bei der fehlenden Möglichkeit, (Konferenz-) Gespräche mit schützenswerten Inhalten über ein Konferenzsystem abzuhalten. Ein Projekt wurde gestartet, um diese Problematik anzugehen.

Aus Sicht des NCSC liegen Risiken auch in der fehlerhaften Konfiguration der IT-Infrastruktur sowie dem Einsatz von Software mit Schwachstellen, welche nicht unmittelbar behoben werden.

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 geschult.
Unter der Leitung der Informatiksicherheitsbeauftragten in den Verwaltungseinheiten (ISBO) werden nahezu alle neueintretenden Mitarbeitenden in die Belange der Informatiksicherheit eingeführt. Während 2019 rund 95% der neueintretenden Mitarbeitenden geschult wurden, fiel dieser Wert 2020 auf 87%. Als Begründung wurde aufgeführt, dass keine Präsenzschulungen durchgeführt werden konnten. Zudem bestehen Lücken bei externen Mitarbeitenden. Zurzeit prüft das EPA ein bundesweites Eintrittspaket, das grundlegende Ausbildungsinhalte für neue Mitarbeitende und Führungskräfte beinhaltet. So sollen auch die Belange der Informatiksicherheit abgedeckt werden.
Ergänzend zu den zentralen Sensibilisierungskampagnen des ehemaligen Informatiksteuerungsorgans des Bundes (ISB) bzw. des NCSC führen viele Verwaltungseinheiten individuelle Massnahmen durch. So führten z. B. einzelne Departemente verschiedene Sensibilisierungsmassnahmen mit Tests zu Phishing E-Mails durch.

4 Sicherheitsvorfälle

Im Jahr 2020 hat der grösste Leistungserbringer des Bundes, das Bundesamt für Informatik und Telekommunikation (BIT), mit dem Computer Security Incident Response Team (CSIRT) insgesamt 834 Sicherheitsvorfälle[3] bearbeitet. Dabei ist festzuhalten, dass nicht jeder Sicherheitsvorfall direkten Schaden für die Bundesverwaltung bedeutet: im Rahmen der Bearbeitung von Sicherheitsvorfällen werden zum Beispiel auch kritische Schwachstellen präventiv untersucht.

Sicherheitsvorfälle lassen sich grundsätzlich in drei Kategorien einteilen:

- Angriffe auf Teile der Bundesverwaltung;
- Externe Sicherheitsvorfälle mit direkter Auswirkung auf die Bundesverwaltung;
- Interne Störungen und Vorkommnisse.

4.1 Angriffe auf die Bundesverwaltung

Die Bundesverwaltung wird laufend angegriffen: Das können sehr breit gestreute Angriffe über E-Mails oder gezielte Angriffe auf die IKT-Infrastruktur des Bundes sein.
Dabei reicht das Spektrum der Angreifer von Massen-Spam-Verteiler über die organisierte Kriminalität oder Hacktivisten bis hin zu vermuteten staatlichen Akteuren.

Eingehende E-Mails
Das BIT analysiert alle eingehenden E-Mails und sorgt dafür, dass unsicher erscheinende E-Mails gar nicht erst den Empfängern zugestellt werden.

Im Jahr 2020 wurden 48% der eingehenden Mails gelöscht noch bevor sie dem Empfänger zugestellt wurden:

Eingegangene E-Mails in die Bundesverwaltung	159'827'600 (Vorjahr: 306'687'261)
Davon zentral gelöscht[4]	76'576'865 (Vorjahr: 238'548'362)
An die Empfänger weitergeleitete E-Mails	83'250'735 (Vorjahr: 68'138'899)

Der massive Rückgang der eingegangenen, bzw. der nicht zentral gelöschten E-Mails, dürfte darauf zurückzuführen sein, dass einerseits bekannte Spam-Versender unschädlich gemacht wurden sowie andererseits die Spam- und Virenfilter der E-Mail Provider massiv mehr schädliche E-Mails löschen und dementsprechend nicht weiterleiten.

Mit der Analyse der eingehenden E-Mails trägt das BIT einen wesentlichen Teil zur Sicherheit der ganzen Bundesverwaltung bei.

Phishing
Mittels Phishing wird versucht, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten einer Benutzerin oder eines Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen oder es kann – mit angehängten Dokumenten - Schadsoftware auf das System geladen werden. Mitarbeitende der Bundesverwaltung bleiben davor nicht verschont: 2020 wurden 34 erfolgreiche Phishing-Angriffe erkannt (Vorjahr 58).

[3] Als Sicherheitsvorfall werden alle eingehenden Sicherheitsmeldungen erfasst. Dazu gehören auch Verdachtsfälle, die sich nach der Analyse als harmlos bzw. als falscher Alarm herausstellen oder Phishing-Fälle, welche nicht direkt die Bundesverwaltung betreffen.

[4] Zentral gelöscht - und damit unschädlich gemacht - werden E-Mails von bekannten Spam- und Malware-Versendern sowie E-Mails, in welchen direkt Viren und Malware erkannt werden.

Für Phishing-Angriffe werden aber auch Adressen von Verwaltungseinheiten der Bundesverwaltung missbraucht. Besonders beliebt sind die Abteilung Mehrwertsteuer und die Zollverwaltung als Absender. Um an die Daten der Opfer zu gelangen, werden z. B. Steuerrückvergütungen versprochen.
In der ganzen Bundesverwaltung werden die Mitarbeitenden weiterhin auf Phishing-Angriffe sensibilisiert. Dabei wird auch aufgezeigt, wie subtil die inzwischen verwendeten Methoden sind.

4.2 Externe Sicherheitsvorfälle mit direkter Auswirkung auf die Bundesverwaltung

Infizierte Web-Seiten
In die Kategorie «Externe Sicherheitsvorfälle» gehört zum Beispiel der Umgang mit potentiell unsicheren Web-Seiten: Diese weisen oftmals gravierende Sicherheitslücken auf und können deshalb für Phishing-Attacken oder zum Verteilen von Malware missbraucht werden. Der Bund hat 2020 den Zugriff auf rund 217 solcher Web-Seiten (teilweise schon präventiv) gesperrt.
Durch die laufende Verbesserung der Auswertung der Internetzugriffe mussten 2020 nur noch wenige externe URL-Sperrungen vorgenommen werden. Von diesen URL gingen Angriffe auf die Internetpräsenz der Bundesverwaltung aus.

4.3 Interne Störungen und Vorkommnisse

Interne Störungen betreffen hauptsächlich die Verfügbarkeit der Systeme und der Daten. Im vergangenen Jahr zeigten sich keine gravierenden Unterbrüche, welche die geforderte Verfügbarkeit namhaft beinträchtig hätte.

Infizierte Geräte
Nachweislich infiziert wurden 20 (Vorjahr: 55) Geräte, davon befanden sich 5 Geräte (25%) im Public-WLAN-Netz der Bundesverwaltung (nicht Geräte der Bundesverwaltung).
Auch wenn «nur» 15 Bundesgeräte (Vorjahr: 19) infiziert wurden, so könnte jedes verseuchte Gerät eine Bedrohung für die ganze Bundesverwaltung darstellen. Die betroffenen Geräte wurden bereinigt und die betroffenen Mitarbeitenden speziell darauf aufmerksam gemacht.
Als positiv darf der stetige Rückgang von infizierten Geräten bezeichnet werden. Dieser Umstand ist nebst technischen Massnahmen auch dem Verhalten der Mitarbeitenden geschuldet.

5 Weitere Massnahmen

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.

Die Grundlagen für das Nationale Zentrum für Cybersicherheit (NCSC) sind in der am 1. Juli 2020 in Kraft getretenen «Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung[5]» (Cyberrisikenverordnung, CyRV) geregelt. Damit wurden Weisungsbefugnisse für die Informatiksicherheit in der Bundesverwaltung an den Delegierten des Bundes für Cybersicherheit delegiert. Ebenfalls zu jenem Zeitpunkt sind die ISB-Bereiche Informatiksicherheit, MELANI und GovCERT in das NCSC übergetreten.

Zur Unterstützung der Mitarbeitenden hat das ISB im Mai 2019 eine Sensibilisierungskampagne «Informatiksicherheit für die Bundesverwaltung» gestartet, welche bis Ende 2020 weitergeführt wurde. Die Inhalte dieser Kampagne sind auch für KMU und die Öffentlichkeit zugänglich[6].

Nationales Zentrum für Cybersicherheit NCSC

[5] SR **120.73**

[6] www.informatiksicherheit.admin.ch