Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Informatiksteuerungsorgan des Bundes ISB
IKT - Sicherheit

Stand der Informatiksicherheit in der Bundesverwaltung 2019

1 Informatiksicherheit in der Bundesverwaltung

Die Informatiksicherheit in der Bundesverwaltung umfasst die Massnahmen zum Schutz der Integrität und Verfügbarkeit der Systeme der Informations-und Kommunikationstechnik (IKT) sowie die Massnahmen zum Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten, die in diesen Systemen gespeichert, verarbeitet und übertragen werden[1]. Der Bundesrat erlässt dazu die Weisungen über die IKT-Sicherheit in der Bundesverwaltung[2].
Basierend auf diesen Weisungen legt das Informatiksteuerungsorgan des Bundes (ISB) die entsprechenden IKT-Vorgaben für die Bundesverwaltung fest.
Dabei orientieren sich die IKT-Sicherheitsmassnahmen an den aktuellen internationalen Standards, insbesondere an den ISO-Standards betreffend die IKT-Sicherheitsverfahren, sowie der Beurteilung der Bedrohungslage.

Die Verwaltungseinheiten sind für den Schutz ihrer IKT-Systeme und -Anwendungen sowie ihrer Daten (Schutzobjekte) verantwortlich. Dabei prüfen die Verwaltungseinheiten ihre Schutzobjekte regelmässig und ergreifen die notwendigen Sicherheitsmassnahmen.

Für die Beurteilung der aktuellen Lage - und dem allenfalls nötigen Erlass von Sofortmassnahmen - arbeitet der Bereich IKT-Sicherheit Bund des ISB eng mit der Melde- und Analysestelle Informationssicherung des Bundes (MELANI) sowie weiteren IKT-Sicherheitsstellen[3] zusammen.

In der Informatiksicherheit unterscheidet sich die Bundesverwaltung nicht grundsätzlich von anderen Behörden, Unternehmen oder Privatpersonen: Alle werden laufend angegriffen und müssen sich entsprechend schützen. Dabei ist jedoch festzuhalten, dass staatliche Organisationen wie die Bundesverwaltung öfter Angriffen von anderen staatlichen Organisationen ausgesetzt sind als Privatpersonen oder KMU.

Zu einzelnen, spezifischen Angriffen oder Sicherheitslücken werden keine Angaben gemacht. Letztere können einem potentiellen Angreifer direkt in die Hand spielen und damit die

[1] Verordnung vom 9. Dezember 2011 über die Informatik und Telekommunikation in der Bundesverwaltung (Bundesinformatikverordnung, BinfV) SR 172.010.58

[2] https://www.isb.admin.ch/isb/de/home/ikt-vorgaben/grundlagen/w002-weisungen_bundesrat_ikt-sicherheit_bundesverwaltung_wisb.html

[3] z. B. dem Computer Emergency Response Team des ISB (GovCERT.ch), dem Computer Security Incident Response Team des BIT (CSIRT-BIT) oder dem Computer Emergency Response Team des VBS (FUB MilCERT)

gesamte Informatik der Bundesverwaltung gefährden. Deshalb werden im vorliegenden Sicherheitsbericht 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 ISB jeweils zum Jahresende über den Stand der Umsetzung von Sicherheitsmassnahmen (Selbstdeklaration basierend auf einer strukturierten Umfrage). Die Angaben werden durch das ISB insbesondere anhand von allfälligen Prüfresultaten der Informatikrevision gemäss Art. 28 Bundesinformatikverordnung plausibilisiert.
Basierend auf den Angaben 2019 konnte das ISB zusammenfassend feststellen, dass der aktuelle Sicherheitsstand der Informatik in der Bundesverwaltung insgesamt der aktuellen Bedrohungslage angemessen und auf vergleichbarem Niveau wie in ähnlichen Organisationen und der Privatwirtschaft ist.

Für die Umsetzung der geforderten Sicherheitsmassnahmen müssen die dazu notwendigen Sicherheitsdokumente vorhanden und aktuell sein.
Die Umsetzung der Sicherheitsmassnahmen war 2019 bei rund 90% aller Schutzobjekte sichergestellt, was grundsätzlich ein guter Wert ist. Denn es ist üblich, dass ein Teil der Dokumentationen in Überarbeitung ist.
Jedoch erreichen die geforderten Kontrollen der Umsetzung noch nicht den gewünschten Stand, auch wenn er sich gegenüber dem Vorjahr verbessert hat (Kontrolle bei rund 70% der Schutzobjekte, im Vorjahr lag dieser Wert bei 66%).
Mit der Umsetzung und Kontrolle der geforderten Sicherheitsmassnahmen kann der Sicherheitsstand gehalten und nachhaltig flächendeckend sichergestellt werden.

3 Faktor Mensch

Die Mitarbeitenden aller Stufen nehmen eine enorm wichtige Rolle im Bereich der Informatiksicherheit wahr. Dementsprechend wurden die Mitarbeitenden der Bundesverwaltung auch 2019 im Umgang mit der Informatiksicherheit geschult.
Unter der Leitung der Informatiksicherheitsbeauftragten in den Verwaltungseinheiten werden nahezu alle neueintretenden Mitarbeitenden (rund 95%) in die Belange der Informatiksicherheit eingeführt. Schulungslücken bestehen in erster Linie noch bei externen Mitarbeitenden.
Zudem wurden im Berichtsjahr 130 Fachkräfte wie z. B. Projektleiter, Systemverantwortliche oder Informatiksicherheitsbeauftragte spezifisch zur IKT-Sicherheit und zum Informatiksicherheitsprozess der Bundesverwaltung geschult.
Aus- und Weiterbildungen werden vom ISB im Ausbildungszentrum des Bundes angeboten. Zusätzlich führt das ISB auch gezielte und massgeschneiderte Ausbildungen in einzelnen Verwaltungseinheiten sowie umfassende, bundesweite Sensibilisierungskampagnen durch.
Ergänzend zu den zentralen Sensibilisierungskampagnen des ISB führen viele Verwaltungseinheiten individuelle Massnahmen zur Sensibilisierung durch (vor allem im Bereich von Phishing E-Mails).

4 Sicherheitsvorfälle

Im Jahr 2019 hat der grösste interne Leistungserbringer des Bundes, das Bundesamt für Informatik und Telekommunikation (BIT), insgesamt rund 900 Sicherheitsvorfälle[4] bearbeitet. Dabei ist festzuhalten, dass nicht jeder Sicherheitsvorfall direkten Schaden für die Bundesverwaltung bedeutet. Im Rahmen der Bearbeitung von Sicherheitsvorfällen werden beispielsweise kritische Schwachstellen präventiv untersucht.

Sicherheitsvorfälle lassen sich grundsätzlich in drei Kategorien einteilen:

- Angriffe auf die 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 gezielte Angriffe auf die IKT-Infrastruktur des Bundes oder sehr breit gestreute Angriffe über E-Mails sein.
Dabei reicht das Spektrum der Angreifer von Massen-Spam-Verteiler über die organisierte Kriminalität oder «Hacktivisten» bis zu vermutlich staatlichen Akteuren.

E-Mails mit Malware
Gezielte Angriffe erfolgen zum Beispiel durch den Versand von E-Mails mit schädlicher Software (Malware) - oder mit Links auf solche - an Empfängerinnen und Empfänger der Bundesverwaltung.
Das BIT analysiert ständig die eingehenden E-Mails und sorgt dafür, dass unsicher erscheinende E-Mails gar nicht erst den Empfängern zugestellt werden.

Gemäss der Analyse des BIT für das Jahr 2019 wurden 78% der eingehenden Mails gelöscht, bevor sie dem Empfänger zugestellt wurden:

Eingegangene E-Mails in die Bundesverwaltung:	306'687'261	(100%)
Davon zentral gelöscht (nicht an die Empfänger weitergeleitet):	238'548'362	(78%)
An die Empfänger weitergeleitete E-Mails:	68'138’899	(22%)

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.

Phishing
Mittels Phishing wird versucht, über gefälschte Web-Seiten, E-Mails oder Kurznachrichten an persönliche Daten einer Benutzerin oder eines Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen oder mit angehängten Dokumenten Schadsoftware auf das System zu laden.

Bei 58 Phishing-Attacken haben Mitarbeitende der Bundesverwaltung ihre Zugangsdaten zu

[4] 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. Da das BIT viele Querschnitts- und Basisleistungen für die ganze Bundesverwaltung erbringt, ergibt sich aus dieser Statistik ein repräsentatives Bild.

privaten E-Mail-Diensten bekanntgegeben. Datenverluste oder Bedrohungen für die IKT-Infrastruktur des Bundes wurden in diesen Fällen nicht festgestellt. Die betroffenen Mitarbeitenden werden durch den Informatiksicherheitsbeauftragten ihrer Organisationseinheit jeweils über die festgestellte Attacke und die nötigen Massnahmen informiert. Damit können die Betroffenen die entsprechenden Zugangsdaten (Passwörter) ändern und ihr Verhalten verbessern.

Identitätsdiebstahl mit Phishing-Methoden werden zunehmen. Da die Methoden dazu immer ausgefeilter und gezielter auf das Opfer zugeschnitten sind, geht davon eine grosse Gefahr aus. Auch werden aktuelle Ereignisse für Angriffe unmittelbar genutzt (z. B. die Corona-Krise, Weltmeisterschaften, usw.).
Nebst technischen Sicherheitsmassnahmen zum Erkennen von Phishing-E-Mails und Web-Seiten mit Malware, wird das Thema auch in den Sicherheitskampagnen intensiv behandelt. Erste Erfolge zeigen sich bereits indem von den Mitarbeitenden markant mehr Phishing-Mails erkannt und an das BIT gemeldet wurden.

Infizierte Geräte
Im Jahr 2019 wurden vom BIT insgesamt 107 infizierte Geräte entdeckt. Dabei wurden 19 Arbeitsplatzgeräte nachweislich infiziert (Vorjahr: 84) und mussten neu aufgesetzt werden (insgesamt betreut das BIT rund 30'000 Arbeitsplatzstationen).
Auch wenn die Zahl von 19 infizierten Geräten klein erscheint, muss beachtet werden, dass von jedem infizierten Gerät eine Bedrohung für die ganze Bundesverwaltung ausgehen kann.

Angriffe auf die Internetpräsenz der Bundesverwaltung
Im Jahr 2019 konnten 30 Angreifer blockiert werden, welche Angriffe auf die Internetpräsenz der Bundesverwaltung[5] durchführten. Weitere Sperrungen wurden als Schutzmassnahme gegen intensives Scanning der Infrastruktur der Bundesverwaltung durchgeführt.

4.2 Externe Sicherheitsvorfälle mit direkter Auswirkung auf die Bundesverwaltung

Infizierte Web-Seiten
Unsichere Webseiten sind eine Bedrohung auch für die Bundesverwaltung. Sie weisen oftmals grobe Sicherheitslücken auf und können deshalb für Phishing-Attacken oder zum Verteilen von Malware missbraucht werden. Der Bund hat 2019 den Zugriff auf rund 715 solcher Web-Seiten präventiv oder reaktiv gesperrt.

Sicherheitslücken in Hardware-Komponenten und Betriebssystemen
Bekannt gewordene Sicherheitslücken in Hardware-Komponenten und/oder Betriebssystemen werden umgehend behoben. Ist dies nicht möglich, werden die betroffenen Bereiche eng überwacht und mit entsprechenden Massnahmen geschützt. Bisher wurden keine Missbräuche solcher Sicherheitslücken erkannt.

4.3 Interne Störungen und Vorkommnisse

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

[5] Diese Web-Seiten werden bundesintern gehostet.

Durch Fehlverhalten von Mitarbeitenden kam es in einigen wenigen Fällen dazu, dass das entsprechende Arbeitsplatzsystem neu aufgesetzt werden musste. Betroffene Mitarbeitende werden jeweils nach einem Vorfall durch die entsprechenden Informatiksicherheitsbeauftragen speziell geschult (siehe oben: Phishing).

5 Weitere Massnahmen

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

Um die Umsetzung der Informatiksicherheit in der Bundesverwaltung, aber auch zugunsten des Landes zu stärken, hat der Bundesrat die Schaffung eines Nationalen Zentrums für Cybersicherheit (NCSC) beschlossen. Die Arbeiten für die Etablierung des Zentrums sind 2019 gestartet worden und werden eine weitere, wesentliche Verbesserung im Bereich der Informatiksicherheit sicherstellen[6].

Zur Unterstützung der Mitarbeitenden der Bundesverwaltung hat das ISB im Mai 2019 eine Sensibilisierungskampagne zur Informatiksicherheit gestartet. Die Inhalte dieser Kampagne sind auch für KMU und die Öffentlichkeit zugänglich[7].

Informatiksteuerungsorgan des Bundes

[6] www.ncsc.ch

[7] www.informatiksicherheit.admin.ch