Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Informatiksteuerungsorgan des Bundes ISB
IKT -Sicherheit

02. Oktober 2019

Stand der Informatiksicherheit in der Bundesverwaltung 2018

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 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 darauf legt das Informatiksteuerungsorgan des Bundes (ISB) die entsprechenden IKT-Vorgaben für die Bundesverwaltung fest.
Die Verwaltungseinheiten sind für den Schutz ihrer IKT-Systeme und -Anwendungen und ihrer Daten (Schutzobjekte) verantwortlich, dabei prüfen sie 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 zudem eng mit der Melde- und Analysestelle Informationssicherheit des Bundes (MELANI) zusammen.

2 Aktueller Stand der Informatiksicherheit in der Bundesverwaltung

Die Departemente und die Bundeskanzlei berichten dem ISB zum Jahresende über den Stand der Umsetzung von Sicherheitsmassnahmen (strukturierte Umfrage).
Basierend auf den Angaben 2018 stellt das ISB zusammenfassend fest, 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.
Um den Sicherheitsstand zu halten und nachhaltig flächendeckend sicherzustellen, müssen insbesondere die Informatiksicherheitsvorgaben überall vollständig umgesetzt und kontrolliert werden. Während sich die Umsetzung laufend verbessert (2018 war z.B. bei rund 90%

[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

aller Schutzobjekte die Umsetzung der Sicherheitsmassnahmen sichergestellt, im Vorjahr waren es noch rund 70%), erreichen die geforderten Kontrollen dieser Umsetzung noch nicht den gewünschten Stand (Kontrolle bei rund 66% der Schutzobjekte).

3 Faktor Mensch

Die Mitarbeitenden aller Stufen tragen eine enorm wichtige Rolle im Bereich der Informatiksicherheit. Dementsprechend werden die Mitarbeitenden der Bundesverwaltung regelmässig im Umgang mit der Informatiksicherheit geschult.
Unter der Leitung der Sicherheitsbeauftragten in den Verwaltungseinheiten werden nahezu alle neueintretenden Mitarbeitenden (rund 90%) in die Belange der Informatiksicherheit eingeführt. Zudem wurden 147 Fachkräfte wie bspw. Projektleiter, Systemverantwortliche oder Informatiksicherheitsbeauftragte spezifisch zum Informatiksicherheitsprozess der Bundesverwaltung geschult. Aus- und Weiterbildungen werden vom ISB mit dem Ausbildungszentrum des Bundes angeboten. Zusätzlich führt das ISB auch gezielte Ausbildungen in einzelnen Verwaltungseinheiten sowie bundesweite Sensibilisierungskampagnen durch.
Ergänzend zu den zentralen Sensibilisierungskampagnen führen viele Verwaltungseinheiten individuelle Massnahmen durch.

4 Sicherheitsvorfälle

Im Jahr 2018 hat der zentrale Leistungserbringer des Bundes, das Bundesamtes für Informatik und Telekommunikation (BIT), insgesamt über 800 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 dauernd angegriffen: Das können zielgerichtete Angriffe auf die IKT-Infrastruktur des Bundes oder sehr breit gestreute Angriffe - zum Beispiel mittels E-Mails - sein.
Dabei reicht das Spektrum der Angreifer von Massen-Spam-Verteiler über die organisierte Kriminalität oder Hacktivisten bis zu vermutlichen staatlichen Akteuren.

[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.

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

Die interne E-Mail-Analyse des BIT für den Monat September 2018 zeigt z.B. folgendes Bild (Zahlen gerundet):

Eingegangene E-Mails in die Bundesverwaltung:	14'500’000
Davon zentral gelöscht (nicht an die Empfänger weitergeleitet):	6'200’000
An die Empfänger weitergeleitete E-Mails:	8'300’000

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 (rund 6'500).

Das heisst, nur rund 57% der eingehenden Mails werden als «sicher» eingestuft und an die Empfängerinnen und Empfänger innerhalb der Bundesverwaltung weitergeleitet.

Phishing
Mittels Phishing wird versucht, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen oder es kann – mit angehängten Dokumenten - Schadsoftware auf das System geladen werden.

Im Jahr 2018 wurden vom BIT insgesamt 119 Phishing-Attacken erkannt. Dabei wurden 84 Arbeitsplatzgeräte verseucht und mussten neu aufgesetzt werden (insgesamt betreut das BIT rund 30'000 Arbeitsplatzstationen). Bei 35 Phishing-Attacken haben Mitarbeitende der Bundesverwaltung ihre Zugangsdaten zu privaten E-Mail-Diensten bekanntgegeben. Datenverluste oder Bedrohungen für die IKT-Infrastruktur des Bundes wurden in diesen Fällen nicht festgestellt. Die betroffenen Mitarbeitenden werden jeweils durch ihren Informatiksicherheitsbeauftragten über die festgestellte Attacke informiert, damit diese die entsprechenden Zugangsdaten aktualisieren können.
Auch wenn die Zahl von 84 verseuchten Geräten klein erscheint, muss beachtet werden, dass von jedem verseuchten Gerät eine Bedrohung für die ganze Bundesverwaltung ausgeht.
Identitätsdiebstahl mit Phishing-Methoden werden zunehmen. Da die Methoden dazu immer ausgefeilter und auf das Opfer zugeschnitten sind, geht davon eine grosse Gefahr aus.
Nebst technischen Sicherheitsmassnahmen zum Erkennen von Phishing-E-Mails, wird das Thema auch in den Sicherheitskampagnen intensiv behandelt.

Damit die Mitarbeitenden verdächtige E-Mails rasch und unkompliziert zur Analyse melden können, hat das BIT einen entsprechenden Melde-Button in das E-Mail-Programm Outlook integriert.

4.2 Externe Sicherheitsvorfälle mit direkter Auswirkung auf die Bundesverwaltung

Infizierte Websites
In die Kategorie «Externe Sicherheitsvorfälle» gehört zum Beispiel der Umgang mit potentiell unsicheren Web-Seiten: Diese weisen oftmals grobe Sicherheitslücken auf und können deshalb für Phishing-Attacken oder zum Verteilen von Malware missbraucht werden. Der Bund hat 2018 den Zugriff auf rund 610 solcher Web-Seiten präventiv und reaktiv gesperrt.
Dabei wurden zum Beispiel auch der Zugriff auf Web-Seiten mit den Top Level Domains .site, .trade oder .download gesperrt, da von diesen eine grosse Bedrohung ausgeht.
Diese Sperrungen ergänzen die eingesetzten kommerziellen Sicherheitslösungen (Proxy und Firewall).

Sicherheitslücken in Computerprozessoren
Am 3. Januar 2018 wurden Sicherheitslücken in Computerprozessoren unter den Namen SPECTRE und MELTDOWN öffentlich bekannt. Da die Problematik weltweit besteht und Korrekturen auf der tiefsten Ebene der Prozessoren erfolgen müssten, ist keine rasche grundsätzliche Lösung dieser bereits langandauernden Schwachstellen zu erwarten. In der Bundesverwaltung verfolgen die zuständigen Stellen die Entwicklungen intensiv. Auch überwachen die Leistungserbringer alle Systeme, um einen allfälligen Missbrauch der Schwachstellen unmittelbar zu erkennen und die nötigen Sofortmassnahmen einzuleiten. Updates werden jeweils so schnell wie möglich eingespielt. Bisher wurden keine Missbräuche dieser Sicherheitslücke 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.
Durch nicht korrektes Verhalten 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 Sicherheitsbeauftragen speziell geschult.

5 Fazit und weitere Massnahmen

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

Um die Umsetzung der Informatiksicherheit in der Bundesverwaltung, aber auch zugunsten des Landes zu stärken, hat der Bundesrat die Schaffung eines Kompetenzzentrums für Cyber-Sicherheit beschlossen. Die Arbeiten für die Etablierung des Kompetenzzentrums sind 2019 gestartet worden und werden eine weitere, wesentliche Verbesserung im Bereich der Informatiksicherheit sicherstellen.

Auf der technischen Seite wurden bereits Ende 2015 mit der Einführung einer Lösung, welche das Ausführen von Schadsoftware oder anderer nicht legitimer Software auf den Arbeitsplätzen verhindert, gute Resultate erzielt (Application Whitelisting). Die Anzahl mit Malware

infizierter Systeme ging um den Faktor 10 zurück. Weiter muss in einem nächsten Schritt die Sichtbarkeit der Malware verbessert werden, so dass umgehend nach Bekanntwerden einer Malware alle Systeme darauf abgesucht werden können.

Zur Unterstützung der Mitarbeitenden hat das ISB im Mai 2019 eine Sensibilisierungskampagne Informatiksicherheit für die Bundesverwaltung gestartet. Die Inhalte dieser Kampagne sind auch für KMU und die Öffentlichkeit zugänglich (www.informatiksicherheit.admin.ch).