EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
SWISS FEDERAL AUDIT OFFICE

20415 - Prüfung der Sicherheit und des Betriebs der Netzwerke

Bundesamt für Informatik und Telekommunikation

Bestelladresse Adresse de commande Indirizzo di ordinazione Ordering address	Eidgenössische Finanzkontrolle (EFK) Monbijoustrasse 45 3003 Bern Schweiz
Bestellnummer Numéro de commande Numero di ordinazione Ordering number	609.20415.004
Zusätzliche Informationen Complément d'informations Informazioni complementari Additional information	www.efk.admin.ch info@efk.admin.ch twitter: @EFK_CDF_SFAO + 41 58 463 11 11
Abdruck Reproduction Riproduzione Reprint	

Mit Nennung der männlichen Funktionsbezeichnung ist in diesem Bericht, sofern nicht anders gekennzeichnet, immer auch die weibliche Form gemeint.

Inhaltsverzeichnis

Das Wesentliche in Kürze 4

1 Auftrag und Vorgehen 8

1.1 Ausgangslage 8

1.2 Prüfungsziel und -fragen 9

1.3 Prüfungsumfang und –grundsätze 10

1.4 Unterlagen und Auskunftserteilung 10

1.5 Schlussbesprechung 10

2 Sicherheit der Netze Bundes 11

2.1 Interne Vorgaben sind nicht durchgängig aktuell und bekannt 11

2.2 Installation von schadhafter Software ist nicht ausgeschlossen 12

2.3 Unzureichende Überprüfung von Vorgaben und Konzepten 13

2.4 Unsachgemässe Löschung von Speichermedien kann zu Datenabfluss führen 14

2.5 Passwortrichtlinien müssen zwingend eingehalten werden 15

2.6 Der Einsatz selbstsignierter Zertifikate sollte vermieden werden 16

2.7 Aufgeschobene Wartung erhöht die Risiken 16

3 Überwachung der Netze und der Netzübergänge 18

3.1 Lücken in der Netzüberwachung 18

3.2 Firewall-Regeln werden nicht konsequent gelöscht 20

3.3 Manipulationen an Konfigurationen könnten vertuscht werden 20

3.4 Durch eine fehlende Validierung können mangelhafte Konfigurationen über längere Zeit bestehen 21

4 Erhaltung und Wiederherstellung der Infrastruktur nach Angriffen 23

4.1 Wiederherstellungsverfahren müssen regelmässig geprobt werden 23

4.2 Automatisierung kann kurzzeitige Ausfälle verhindern 24

Anhang 1: Rechtsgrundlagen 25

Anhang 2: Abkürzungen 26

Anhang 3: Glossar 28

Anhang 4: Follow-up der offenen Empfehlungen 31

20415 - Prüfung der Sicherheit und des Betriebs der Netzwerke

Bundesamt für Informatik und Telekommunikation

Das Wesentliche in Kürze

Als interner IKT-Leistungserbringer unterstützt das Bundesamt für Informatik und Telekommunikation (BIT) die Verwaltung mit Informatikmitteln und -diensten. Darunter fällt auch der Betrieb von Datennetzen und Telekommunikations-Infrastrukturen für die gesamte zivile Bundesverwaltung. Die rund 1100 Mitarbeitenden des BIT betreuen die IKT-Infrastrukturen für die 38 000 Arbeitsplatzsysteme und zirka 6300 Server. Mit dem Neubau des Rechenzentrums «Campus» in Frauenfeld wurde die Architektur des Netzwerk-Übergangs zu den Rechenzentren überarbeitet. Die Rechenzentrums-Netzwerkinfrastruktur und die Firewall Übergänge wurden neu aufgebaut. Dabei sind neue Technologien zu Einsatz gekommen.

Die Prüfung der Sicherheit und des Betriebs der Netzwerke fokussierte auf die Beurteilung der Angemessenheit der Massnahmen in den Bereichen Netzwerksicherheit und Firewall-Management, sowie auf die Service-Aufrechterhaltung der neuen Netze.

Die eingesetzten Technologien und Architekturen entsprechen den heutigen Standards und erlauben eine effektive und sichere Administration der Netze. Der Ausbauschritt der Netze ist weitgehend abgeschlossen und die betrieblichen Themen sind zweckmässig adressiert. Allerdings gibt es verschiedene Bereiche mit Handlungsbedarf und Optimierungspotenzial, namentlich in den Bereichen Grundschutz, Überwachung und Systemwiederherstellung.

Vorgaben müssen aktualisiert und deren Umsetzung überprüft werden

Interne Standards und Vorgaben sind wichtige Grundlagen für die Umsetzung der Sicherheitsanforderungen in jeglichen Systemen und Plattformen. Diese müssen laufend aktualisiert und allen Mitarbeitenden zugänglich gemacht werden. Die Mitarbeitenden müssen zudem stufengerecht bezüglich der Sicherheitsanforderungen geschult werden. Die technische Implementierung von Anforderungen und Massnahmen aus übergeordneten Dokumenten wie z. B. Informationssicherheits- und Datenschutzkonzepten oder Zonenpolicies muss von einer unabhängigen internen oder externen Stelle geprüft werden.

Grundschutzanforderungen müssen konsequenter umgesetzt werden

Der IKT-Grundschutz der Bundesverwaltung definiert die minimalen Sicherheitsanforderungen an Schutzobjekte. In verschiedenen Bereichen müssen die Grundschutzanforderungen durch das BIT noch konsequenter umgesetzt werden. So werden beispielsweise Speichermedien von Netzwerkkomponenten bei der Ausserbetriebnahme nicht endgültig gelöscht, was ein Risiko hinsichtlich eines Datenabflusses darstellt. Auch im Bereich der Umsetzung der Passwortanforderungen muss das BIT noch Nacharbeiten leisten. Für den Zugriff auf das Netzwerk-Management-System sollte eine 2-Faktor-Authentisierung geprüft werden.

Nur eine lückenlose Überwachung kann Verwundbarkeiten und Schwachstellen sicher erkennen

Zur Erkennung von Schwachstellen oder Angriffen auf die Kommunikations-Infrastruktur ist ein regelmässiges und flächendeckendes Scannen der Netze unerlässlich. Die bestehende Überwachung des Netzwerkverkehrs fokussiert auf Netzwerkübergänge nach aussen. Um eine Erkennung von Anomalien im Verkehr auch innerhalb des Perimeters sicherzustellen, sollten die entsprechenden Überwachungsmechanismen auch an den internen Zonenübergängen eingesetzt werden. Konfigurationen von Netzwerkkomponenten sind laufend zu prüfen und allfällige Änderungen, insbesondere Löschungen von unbenutzten Regeln, konsequent auszuführen.

Neue Systeme und Infrastrukturen werden mindestens bei der Inbetriebnahme auf mögliche Schwachstellen überprüft. Mit einer periodischen Prüfung kann die Sicherheit längerfristig aufrechterhalten werden. Die Verantwortlichkeiten für diese Prozesse müssen besser geregelt werden.

Periodische Wiederanlauftest sind für einen sicheren Betrieb unerlässlich

Die Anwendung mit den gesamten Informationen und Konfigurationen zu den Netzwerken stellt das Kernelement für den Betrieb und die Wartung der Netzwerke des BIT dar. Eine Sicherung der Daten wird gemacht. Wichtig ist jedoch, dass auch die Wiederherstellung in einem Notfall reibungslos funktioniert. Nur durch regelmässiges Testen und Üben kann sichergestellt werden, dass die Notfallpläne im Ernstfall auch funktionieren. Dies muss das BIT mittelfristig in die Planung aufnehmen.

Acht Empfehlungen aus früheren Prüfungen wurden sinngemäss umgesetzt, eine befindet sich noch in Umsetzung. Die Details dazu sind im Anhang 4 beschrieben.

Generelle Stellungnahme des Bundesamtes für Informatik und Telekommunikation (BIT)

Das BIT empfand die Zusammenarbeit mit den Prüfexperten in den Interviews als sehr angenehm. Einzelne Empfehlungen der Findings aus der Ergebnisbesprechung wurden in den Teams der Business Unit Network Services (PS-NET) bereits umgesetzt. Zur Umsetzung der noch offenen Empfehlungen der einzelnen Findings werden ab Program Increment 5 (ab Mai 2022) bei PS-NET, sowie beim CSO entsprechende Stories im JIRA erfasst. Die Umsetzung in den betroffenen Fachbereichen wird durch die neuen Security-Champions eingefordert und überprüft.

Das BIT dankt der EFK für die gegebenen Hinweise, die uns helfen, die Sicherheit unserer Leistungen zu verbessern.

Generelle Stellungnahme der Bundeskanzlei, Bereich Digitale Transformation und IKT-Lenkung (DTI)

Keine generelle Stellungnahme abgegeben.

1 Auftrag und Vorgehen

1.1 Ausgangslage

Das Bundesamt für Informatik und Telekommunikation (BIT) ist einer der internen IKT-Leistungserbringer (LE) der Bundesverwaltung (BV). Es unterstützt die Verwaltung mittels Informatik, um wirtschaftliche, sichere, benutzer- und bürgerfreundliche Lösungen zu entwickeln und einzusetzen. Das BIT unterstützt die Geschäftsprozesse in der BV und sorgt für eine funktionierende Telekommunikation zwischen allen Bundesstellen im In- und Ausland. Es bietet in der Verwaltung nicht nur standardisierte Arbeitsplatzsysteme an, sondern integriert und entwickelt auch massgeschneiderte informatikgestützte Fachanwendungen. Als Erbringer von Standarddiensten ist das BIT in den Bereichen Telekommunikation, Internet, betriebswirtschaftliche Lösungen und operative Sicherheit für die ganze Bundesverwaltung tätig.

Die Prüfung der Sicherheit und des Betriebs der Netzwerke beim BIT fand in zwei Bereichen statt. Einerseits im Bereich Plattform Services (PS) in der Abteilung Network Services (PS-NET) und bei Strategy & Innovation (SI) in der Abteilung Chief Security Officer (SI-SUR). Zusätzlich wurde auch der Bereich Digitale Transformation und IKT-Lenkung (DTI) der Bundeskanzlei und das Nationale Zentrum für Cybersicherheit (NCSC) in die Prüfung miteinbezogen.

Das BIT befindet sich in einer Transformationsphase, in der die ganze Organisation nach SAFe for Lean Enterprises 5.0, einem Agilen Framework, reorganisiert wird. Die Abteilung PS-Net besteht aktuell aus sieben DevOps Teams mit je 10-14 Mitarbeitenden, die für das nachfolgend im Kapitel 2 beschriebene Netzwerk verantwortlich sind.

Strategie «Netzwerke des Bundes»

Im Rahmen der Strategieerarbeitung wurde basierend auf dem Bedarf und mit Blick auf die Vision das Portfolio Datenkommunikationsinfrastrukturen des Bundes entwickelt.

Die untenstehende Grafik stellt die Netzinfrastrukturen dar, welche für die Abdeckung des Bedarfs an der Vernetzung von Standorten in der Bundesverwaltung unter Berücksichtigung der Anforderungen erforderlich sind. Zu jeder Infrastruktur ist der jeweilige LE festgehalten.

OSI-Schicht[1]	Infrastrukturebene	Datenkommunikationsinfrastruktur	IKT-LE	Führung der IKT-Netzwerk-Services
Schicht 3	IP-Netzwerke	Führungsnetz Schweiz	FUB	VBS
		Digital IP-Backbone CF	offen	SD DAKO
		IP-Backbone für die Vernetzung der IP-Teilnetze BSA	BIT	SD DAKO
		IP-Teilnetze für die Vernetzung der BSA entlang der Nationalstrassen	ASTRA	UVEK
		Restliche IP-Netzwerke der zivilen Bundesverwaltung	BIT	SD DAKO
	Virtualisierungsebene für IP-Netzwerke	Führungsnetz Schweiz (VMPLS/BMPLS)	FUB	VBS
		Core-Carrier-Netz Bund (ziviles MPLS Netzwerk)	BIT	SD DAKO
Schicht 2	Optische Transportnetzwerke (OTN)	Führungsnetz Schweiz	FUB	VBS
		Optisches Behördennetz Bund (OBNB)	FUB	SD DAKO
Schicht 1	Glasfaserkabel	Führungsnetz Schweiz	FUB	VBS
		Nationalstrassen	ASTRA	UVEK
		Agglomeration Bern	BIT	SD DAKO
Schicht 0	Kabelkanalisation	Führungsnetz Schweiz	FUB	Die Aufteilung der Führung zwischen IKT-LE und Bau- und Liegenschaftsorganen wird departemental unterschiedlich gehandhabt.
		Nationalstrassen	ASTRA	
	Datenkommunikationsräume	Militärische Anlagen	FUB	
		Nationalstrassen	ASTRA	
		Gebäude des Bundes	BIT	

Abbildung 1: Portfolio Datenkommunikationsinfrastrukturen des Bundes (Bild: Strategie «Netzwerke des Bundes»)

Der Standarddienst Datenkommunikation (SD DAKO)

Als IKT-Standarddienst (IKT-SD) wird eine durch den Bereich DTI zentral geführte IKT-Leistung bezeichnet, die in der Bundesverwaltung vielfach und unter gleichen oder ähnlichen Anforderungen der Leistungsbezüger (LB) verwendet wird. Die Leistungserstellung erfolgt durch einen oder mehrere, interne oder externe Leistungserbringer.

Der SD DAKO umfasst sämtliche drahtgebundene und drahtlose Datenkommunikation zwischen den Standorten und Vollzugsstellen der BV, einschliesslich der Vernetzung innerhalb der Gebäude sowie der Netzübergänge zu bundesexternen Netzen.

1.2 Prüfungsziel und -fragen

Prüfung der Sicherheit und des Betriebs der Netzwerke mit Beurteilung der Angemessenheit der Massnahmen in den Bereichen Netzwerksicherheit und Firewall, sowie bezüglich Service-Continuity.

Die Prüffragen lauteten:

1. Sind das Bundesnetz und die dazu gehörenden Netzwerkkomponenten so konzipiert, dass eine angemessene Sicherheit (Verfügbarkeit, Vertraulichkeit, Integrität) und Resilienz sichergestellt ist?
2. Ist eine lückenlose und permanente Überwachung der Infrastruktur am Perimeter und im Inneren des Netzes sichergestellt und werden Auffälligkeiten zeitnah detektiert und bearbeitet?
3. Bestehen angemessene Massnahmen zur Erhaltung resp. Wiederherstellung der Netzverfügbarkeit bei Angriffen?
4. Follow-up: Umsetzung von diversen Empfehlungen verifizieren

1.3 Prüfungsumfang und –grundsätze

Die Prüfung wurde von Roland Gafner (Revisionsleiter) vom 18. Oktober bis 10. Dezember 2021 durchgeführt. Die Federführung lag bei Bernhard Hamberger. Der Revisionsleiter wurde durch eine externe Firma unterstützt.

Die Beurteilungen orientieren sich an der «Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (CyRV)», der «Si001 - IKT-Grundschutz der Bundesverwaltung» (Version 4.6) und der «Si003 - Netzwerksicherheit in der Bundesverwaltung» (Version 3.1). Weiter kamen die Empfehlungen der International Organization for Standardization (ISO/IEC) Standards 2700x zur Anwendung.

Im Rahmen der Prüfung wurden Bereiche des Netzwerks auf Schwachstellen gescannt. Auch wurden diverse technische Prüfungen auf den Systemen durchgeführt. Die Resultate dieser Prüfungen wurden mit dem BIT besprochen.

Die Ergebnisbesprechung hat am 22. November 2021 stattgefunden. Der vorliegende Bericht berücksichtigt nicht die weitere Entwicklung nach der Ergebnisbesprechung.

1.4 Unterlagen und Auskunftserteilung

Die notwendigen Auskünfte wurden der EFK von den geprüften Verwaltungseinheiten umfassend und zuvorkommend erteilt. Die gewünschten Unterlagen sowie die benötigte Infrastruktur standen dem Prüfteam vollumfänglich zur Verfügung.

1.5 Schlussbesprechung

Die Schlussbesprechung fand am 31. März 2022 statt. Teilgenommen haben seitens BIT der stellvertretende Direktor, der Product Manager Zugangssysteme und Netzwerke, der Business Owner Network Services und der Projektleiter Management Vorhaben. Von Seiten des Bereichs DTI hat der Leiter Digitale Standardleistungen teilgenommen. Die EFK war vertreten durch den Mandatsleiter, den Federführenden und den Revisionsleiter.

Die EFK dankt für die gewährte Unterstützung und erinnert daran, dass die Überwachung der Empfehlungsumsetzung den Amtsleitungen bzw. den Generalsekretariaten obliegt.

EIDGENÖSSISCHE FINANZKONTROLLE

[redacted]

[redacted]

Fachbereichsleiter

Revisionsleiter

2 Sicherheit der Netze Bundes

Der Kern des Netzwerkes bildet ein Core Netzwerk, bestehend aus dem Core Carrier Network (CCN), dem Software-Defined Network (SDN) und dem BIT Internet Core (BIC) in den beiden Rechenzentren «PRIMUS» und «CAMPUS». Die Aussenstandorte in der Schweiz und im Ausland werden auf unterschiedliche Art und Weise an dieses Core Netzwerk angebunden. Das Netzwerk wird durch einen Sicherheitsperimeter geschützt, in dem verschiedene Sicherheitselemente wie beispielsweise Proxies, Firewalls und Web Application Firewalls zum Einsatz kommen. Das gesamte Access-Management, d. h. der Zugriff auf das Netzwerk wird in der Abteilung PS-NET verantwortet. Grossen Wert wird auf die Automatisierung und die Vereinfachung von Routineabläufen, wie z. B. Konfiguration von Netzwerk Ports, gelegt. Für die gesamte Automatisierung ist ebenfalls ein Team aus PS-NET verantwortlich.

Die eingesetzten Technologien und Architekturen entsprechen den heutigen Standards und erlauben eine effektive und sichere Administration der Netze. Der Aufbau der Netze ist weitgehend abgeschlossen und die betrieblichen Themen sind zweckmässig adressiert, allerdings gibt es verschiedene Bereiche mit Handlungsbedarf und Optimierungspotenzial, welche nachfolgend aufgezeigt werden.

2.1 Interne Vorgaben sind nicht durchgängig aktuell und bekannt

Der BIT-interne Standard zur Kryptographie liegt in der Version 1.41 vor und ist auf den 1. November 2017 datiert. Darin werden veraltete Sicherheitsprotokolle nicht explizit von der Verwendung ausgeschlossen. Diese dürfen gemäss den Bundesvorgaben und dem heutigen Stand der Technik aus Sicherheitsgründen jedoch nicht mehr verwendet werden. Weiter stellte sich im Laufe der Prüfung heraus, dass nicht durchgängig bekannt ist, welche BIT-internen Sicherheitsvorgaben überhaupt existieren und wo diese zu finden sind.

Bei der Mitarbeitereinführung wird der Prozess für die Meldung von Sicherheitsvorfällen und Schwachstellen geschult und die Ansprechstellen bekannt gegeben. In der Prüfung hat sich aber gezeigt, dass nicht überall bekannt ist, inwiefern und wo Schwachstellen oder Sicherheitsvorfälle gemeldet werden müssen.

Beurteilung

Gemäss heutiger Erkenntnisse wird die Verwendung von veralteten Protokollen nicht mehr empfohlen. Vorgaben, insbesondere für Kryptographie, müssen laufend aktualisiert werden. Nur so kann sichergestellt werden, dass keine veralteten bzw. unsichere Mechanismen verwendet werden. Grundsätzlich sollten alle internen Standards und Richtlinien periodisch auf deren Aktualität überprüft werden.

Es hat sich gezeigt, dass insbesondere bei langjährigen Mitarbeitenden, der Prozess und die Meldestelle für Sicherheitsvorfälle nicht mehr ganz präsent ist. Für eine LE Organisation ist von zentraler Bedeutung, dass neben Sicherheitsvorfällen auch Schwachstellen, respektive Sicherheitslücken gemeldet werden. Nur so kann sichergestellt werden, dass allfällige Auswirkungen den LB zeitnah kommuniziert werden können.

Voraussetzung dafür ist, dass allen Personengruppen die Prozesse und Vorgaben bekannt sind. Mindestens muss sichergestellt werden, dass Mitarbeitende diese Informationen abrufen können.

Empfehlung 1 (Priorität 2)

Die EFK empfiehlt dem BIT, interne Standards zur Sicherheit zu aktualisieren und einer periodischen Überprüfung zu unterziehen. In diesem Zusammenhang müssen die Mitarbeitenden des BIT über die Struktur und Ablage der Sicherheitsvorgaben informiert werden.

Stellungnahme des BIT

Die Empfehlung ist akzeptiert.

Die Empfehlung ist akzeptiert.

Die BIT Standards zur Sicherheit werden alle 3 Jahre auf ihre Aktualität geprüft und nötigenfalls überarbeitet. Der Standard zur Kryptographie wurde gerade überarbeitet und in der Version 1.5 verabschiedet. Die Publikation ist noch ausstehend.

Empfehlung 2 (Priorität 1)

Die EFK empfiehlt dem BIT, eine flächendeckende und regelmässige Sensibilisierung der Mitarbeitenden bezüglich des Prozesses zur Meldung von Sicherheitsvorfällen und Sicherheitslücken durchzuführen.

Stellungnahme des BIT

Die Empfehlung ist akzeptiert.

Die Empfehlung ist akzeptiert.

Die regelmässige Kommunikation und Sensibilisierung wird etabliert.

2.2 Installation von schadhafter Software ist nicht ausgeschlossen

Die Admin-VDI Umgebung existiert in drei unterschiedlichen Versionen, Admin-VDI 1.0 und Admin-VDI 2.0 (Non Persistent) und Admin-VDI 2.0 (Persistent). Die Desktop Virtualisierung verfolgt den Ansatz, die Funktionen einer Netzwerkkomponente über einen zentralen Service bereitzustellen. In den Version 1.0 und 2.0 (Persistent) können Administratoren eigene Software installieren, die über ein persönliches Transfer-Laufwerk vom Bundesclient auf den Admin-VDI-Client transferiert werden kann. Beim Transfer der Software wird diese durch den Bundesclient und auf dem Transfer-Laufwerk auf Malware geprüft. Die von den Administratoren verwendete Software wird jedoch weder einer Sicherheitsprüfung unterzogen, noch wird sichergestellt, dass sie von einer vertrauenswürdigen Quelle stammt. Auf dem Admin-VDI 2.0 (Non Persistent) kann keine Software durch den einzelnen Administrator installiert werden. Für die Nutzung der Admin-VDI Umgebung besteht eine Benutzeranleitung, in der gefordert wird, dass für die Installation von Software aus dem SW-Repository und für eine Notfallinstallation die Freigabe des Bereichsleiters einzuholen sei.

Ziel des BIT ist es, die Admin-VDI Umgebung V1.0 bis Mitte 2022 abzulösen und dann soweit möglich nur noch den Admin-VDI-Client 2.0 (Non Persistent) einzusetzen. Dies wird das Risiko der Installation korrumpierter Software längerfristig vermindern.

Beurteilung

Die auf dem Admin-VDI zu installierende Software wird doppelt auf Malware geprüft. Somit ist diesbezüglich der IKT-Grundschutz erfüllt. Zudem kann von einem Admin-VDI-Client kein Zugriff auf das Internet oder auf das E-Mail-System erfolgen, was die Angriffsvektoren weiter reduziert. Trotzdem besteht aufgrund der fehlenden Sicherheitsüberprüfung und der

fehlenden Überprüfung auf vertrauenswürdige Quellen das Risiko, dass Schadsoftware eingeschleust wird. Da die Umgebung im Ablöseprozess steht und durch die sicherere Version ersetzt wird, verzichtet die EFK hier auf eine Empfehlung.

2.3 Unzureichende Überprüfung von Vorgaben und Konzepten

Die gemäss Si003 umzusetzenden Zonenpolicies sind im Intranet des Bereiches DTI abrufbar. In jeder Zonenpolicy ist der Inhaber und Betreiber der Zone definiert. Durch die Inhaber erstellte Zonenpolicies werden durch den Bereich DTI geprüft und freigegeben. Hierbei wird lediglich die Architekturkonformität geprüft[1]. Die Inhaber der Zonen überprüfen die Umsetzung der Zonenpolicies durch den Betreiber nicht. Es findet somit keine Überprüfung der Umsetzung durch den Bereich DTI (Inhaber der Zone) beim BIT (Betreiber der Zone) statt. Gemäss den Vorgaben liegt es im Ermessen des Zoneninhabers, diesen Sachverhalt zu prüfen. Für sicherheitskritische Zonen ist eine Überprüfung jedoch angebracht. Bei den Zonenpolicies, bei welchen das BIT als Inhaber geführt ist, ist dieses auch vielfach gleichzeitig der Betreiber. Auch BIT-intern findet keine Prüfung der Umsetzung statt. Seitens des Bereichs DTI wird an die Eigenverantwortung der Betreiber appelliert, dass die Zonen korrekt aufgebaut werden. Auch aus der Sicht der Sicherheit liegt es in der Verantwortung der Betreiber, die Zonen korrekt zu implementieren, bzw. der Inhaber, die korrekte Implementierung zu überprüfen.

Innerhalb des BIT wird jeder Antrag zur Änderung einer Firewall-Regel auf die Konformität gegenüber der Zonenpolicy geprüft.

Im Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) Standarddienst Datenkommunikation (SD-DAKO) wurden Massnahmen zur Verminderung von Risiken definiert. Die Umsetzung der Massnahmen wurden terminiert und mit einer Verantwortlichkeit hinterlegt. Die Umsetzung der Massnahmen werden seitens DTI als verantwortliche Stelle des Standarddienstes SD-DAKO nicht explizit überprüft.

Beurteilung

Die Vorgaben zu den Zonen sind ein wichtiger Bestandteil zur Umsetzung der Netzwerksicherheit. Jede Zonenpolicy sollte durch den Zoneninhaber oder in dessen Auftrag durch eine unabhängige Stelle auf Sicherheit überprüft werden, dabei sind mindestens die Konformität zu Bundesvorgaben bezüglich Sicherheit zu prüfen. Dabei erfordern allfällige Abweichungen eine Ausnahmebewilligung. Weiter sind die Zonenpolicies im Gesamtumfeld zu betrachten, denn jede Zonenpolicy hat einen Gegenpart der übereinstimmen muss.

Das Formulieren der Vorgaben ist der erste Schritt, die Umsetzung der zweite Schritt im Sicherheitszyklus (PDCA-Zyklus, Plan-Do-Check-Act). Wenn bei der Umsetzung der Zonenpolicies auf Eigenverantwortung des Betreibers gesetzt wird, spricht das für ein gutes Verhältnis zwischen Inhaber und Betreiber, blendet aber die letzten beiden Schritte aus. Um Fehler oder Missverständnisse in der Umsetzung zu verhindern, empfiehlt sich eine unabhängige Überprüfung.

Gleich wie bei den Zonenpolicies wird auch die Umsetzung der Massnahmen zur Verminderung der Risiken nicht überprüft. Auch diese sind der Eigenverantwortung des Zoneninhabers überlassen. Somit fehlt auch hier die Überprüfung im PDCA-Zyklus der für die Gewährleistung einer durchgängigen Sicherheit elementar ist.

[1] Si003 - Netzwerksicherheit in der Bundesverwaltung, Kapitel 4 Prüfkriterien

Empfehlung 3 (Priorität 1)

Die EFK empfiehlt dem BIT, die Umsetzung der Vorgaben aus den Zonenpolicies durch eine unabhängige interne oder externe Stelle prüfen zu lassen.

Stellungnahme des BIT

Die Empfehlung ist akzeptiert.

Die Empfehlung ist akzeptiert.

Der Bereich SI-SUR wird die Prüfung in die Audit-Planung aufnehmen.

Empfehlung 4 (Priorität 1)

Die EFK empfiehlt dem Bereich DTI, die Umsetzung der Massnahmen zur Risikominderung aus dem ISDS-Konzept SD-DAKO bei den verschiedenen Leistungserbringern zu Überwachen und deren Stand nachweisbar zu dokumentieren.

Stellungnahme des DTI

Die Empfehlung ist akzeptiert.

DTI wird die Umsetzung der Massnahmen zur Risikominderung aus dem ISDS-Konzept SD-DAKO in seinem halbjährlichen Reporting «Stand der Informatiksicherheit in den Standarddiensten SD» integrieren und sukzessive weiterentwickeln.

2.4 Unsachgemässe Löschung von Speichermedien kann zu Datenabfluss führen

Für die Dekommissionierung von Geräten sind Prozesse definiert. Im Prozess selbst wird ein Formatieren des Flash-Speichers empfohlen. Festverbaute Speicher werden jedoch nicht entfernt und verbleiben im System. Ein Formatieren des Speichers reicht jedoch nicht aus, um Rückschlüsse auf deren Inhalte zu verhindern. Formatieren bedeutet lediglich, dass die Zuordnungstabelle der Informationen gelöscht wird, aber die Daten weiterhin auf dem Speichermedium verbleiben. Ein Wiederherstellen der Informationen ist daher möglich.

Beurteilung

Der IKT-Grundschutz verlangt, dass bei der Entsorgung von Datenträgern und Speichermedien keine Rückschlüsse auf Inhalte oder gespeicherte Daten möglich sind. Die praktizierte Löschmethode festverbauter Speichermedien (z. B. Flash-Speicher, EEPROM, etc.) widerspricht der Vorgabe aus dem Grundschutz und kann zu Datenabflüssen führen. Eine sichere Methode, in dem alle Speichermedien mehrmals mit Zufallsinhalten überschrieben werden (wipe) sollte hier zum Einsatz kommen.

Empfehlung 5 (Priorität 1)

Die EFK empfiehlt dem BIT, sämtliche Speichermeiden bei der Entsorgung einem sicheren Löschverfahren zu unterziehen. Sollte es mit zumutbarem Aufwand möglich sein, so wird zusätzlich empfohlen die festverbauten Speichermedien zu entfernen und einer gesonderten Vernichtung zuzuführen.

Stellungnahme des BIT

Die Empfehlung ist akzeptiert.

Die Empfehlung ist akzeptiert.

Die Empfehlung ist bereits wie nachfolgend beschrieben umgesetzt:

Der Bereich PS-NET unternimmt sämtliche vom Hersteller vorgesehenen Massnahmen um Daten auf Speichermedien vor der Entsorgung zu löschen.

Falls eine Löschung (insbesondere bei Flash Speichermedien) rückgängig gemacht werden kann und die auf dem Speichermedium enthaltenen Daten besonders schützenswert sind (insbesondere bei Netzwerksicherheits-Infrastruktur wie Firewalls) hat das BIT einen sog. Secure-RMA Vertrag mit dem Lieferanten abgeschlossen.

Bei Infrastruktur ohne schützenswerte Daten (insb. im Access-Netzwerk Bereich) wird aus wirtschaftlichen Gründen darauf verzichtet.

Die Umsetzung der Empfehlung die festverbauten Speichermedien in diesen Geräten zu entfernen wird als nicht zumutbar eingeschätzt, insbesondere da heute Speichermedien in den unterschiedlichsten Chips enthalten sein können und daher nicht einfach zu identifizieren sind.

2.5 Passwortrichtlinien müssen zwingend eingehalten werden

Für den Zugriff auf das zentrale Managementsystem für das Netzwerkumfeld, OSS (Operating Support System), wird ein Benutzer gegenüber dem Verzeichnisdienst OpenLDAP authentifiziert. Dabei sind ein Benutzername und ein Passwort erforderlich. Anlässlich der technischen Prüfung wurde ein Passwortwechsel vollzogen. Dabei wurde festgestellt, dass die eingeblendeten Kennwortanforderungen nicht dem IKT-Grundschutz entsprechen. Auch der Versuch ein triviales Kennwort (test1234) einzugeben, war erfolgreich. Dies bedeutet, dass neu eingegebene Kennwörter nicht gegen die eingeblendeten Kennwortanforderungen geprüft werden.

Beurteilung

Die Kennwortanforderungen im OSS genügen nicht den Vorgaben aus dem IKT-Grundschutz. Das Einblenden der Kennwortanforderung beim Passwortwechsel ist eine gute Unterstützung für den Benutzer, jedoch ist die fehlende Prüfung des Kennwortes auf Konformität unvorsichtig. Insbesondere weil es sich beim OSS um das zentrale Managementsystem im Netzwerkumfeld handelt. Angesichts der sensiblen Informationen im OSS ist die Authentisierung mittels eines zweiten Faktors dringend ratsam.

Empfehlung 6 (Priorität 1)

Die EFK empfiehlt dem BIT, die Kennwortanforderungen im OSS so anzupassen, dass die Vorgaben aus dem IKT-Grundschutz zwingend eingehalten werden. Weiter ist die Implementierung einer 2-Faktor-Authentifizierung für das OSS zu prüfen und sofern möglich umzusetzen.

Stellungnahme des BIT

Die Empfehlung ist akzeptiert.

Die Empfehlung ist akzeptiert.

Die Empfehlung ist bereits wie folgt in Umsetzung:

Aufgrund des 1. Berichtsentwurf konnte die Situation bereits korrigiert werden. Die Kennwortanforderungen im OSS entsprechen nun den Vorgaben der Si001 v4. Die notwendigen Anpassungen für die Si001 v5 erfolgen im Rahmen der Umsetzung der Vorgabenänderung.

Die Implementierung einer 2-Faktor-Authentifizierung wird aktuell geprüft.

2.6 Der Einsatz selbstsignierter Zertifikate sollte vermieden werden

Aus den Schwachstellenscans ist ersichtlich, dass im Out of Band Management[2], dem abgetrennten Netzwerk zur Verwaltung der Netzwerkkomponenten, selbstsignierte Zertifikate verwendet werden. Solche Zertifikate werden nicht durch die Swiss Government PKI verwaltet und genügen nicht den Sicherheitsanforderungen, wie sie im IKT-Grundschutz in der Bundesverwaltung (Si001) gefordert werden. Im ISDS-Konzept SD DAKO Kapitel 6.1, wird die Verwendung von Zertifikaten aus der zentralen PKI (CA Swiss Government PKI) für verschlüsselte Verbindungen als Massnahme vorgegeben. Eine Ausnahmegenehmigung für Abweichung von den Vorgaben liegt zum Prüfzeitpunkt nicht vor.

Beurteilung

Die Verwendung von selbstsignierten Zertifikaten entspricht nicht den Vorgaben. Das Risiko einer Verletzbarkeit bei der Verwendung von selbstsignierten Zertifikaten im abgetrennten Out of Band Management kann hingegen als gering eingestuft werden.

Aus diesem Grund verzichtet die EFK auf eine Empfehlung.

Die Abweichung zum IKT-Grundschutz sollte transparent ausgewiesen werden und wenn erforderlich dem ordentlichen Bewilligungsprozess unterzogen werden[3].

2.7 Aufgeschobene Wartung erhöht die Risiken

Ende Oktober bis Ende November 2021 wurde ein Stopp für alle Changes verhängt, welche die Infrastruktur für die Covid-Zertifikate negativ beeinflussen könnten. Dieser Stopp hatte zur Konsequenz, dass Schwachstellen der Kritikalität «Hoch», welche in der Prüfung durch einen Scan festgestellt wurden, nicht zeitnah geschlossen werden konnten. Auch konnten für die Ausfallsicherheit wichtige betriebliche Arbeiten, nicht mehr durchgeführt werden.

Eine weitere Herausforderung für zeitnahe Changes auf den Netzwerkebenen liegt in der Praxis, Endsysteme in den Rechenzentren «PRIMUS» und «CAMPUS» nicht zwingend redundant ans Netzwerk anzuschliessen. In der IKT-Richtlinie für die Netzwerkanbindung von Servern ist vorgesehen, dass eine physische Infrastruktur-Komponente im Normalfall über zwei Hochgeschwindigkeits-IP-Interfaces und über ein separates Out-Of-Band Management Interface verfügen soll.

Beurteilung

Der Change Stopp kam aus Sicht Netzwerk einem generellen Change Stopp für jegliche Änderungen des Netzwerkes gleich. Durch diesen Unterbruch konnten neu entdeckte

[2] Out-of-Band ist ein Netzwerkbegriff, der sich auf einen separaten Kommunikationskanal bezieht, der nicht über den üblichen Datenstrom läuft.

[3] Mit dem Inkrafttreten des überarbeiteten IKT-Grundschutz (Version 5.0) per 1. März 2022 ist keine Bewilligung mehr erforderlich.

Schwachstellen nicht zeitnah geschlossen und notwendige betriebliche Arbeiten nicht durchgeführt werden. Wenn dieser über eine längere Zeit (mehrere Wochen) anhält, erhöht sich die Wahrscheinlichkeit eines grösseren Ausfalls des Netzwerkes aufgrund nicht durchgeführter Wartungsarbeiten laufend. Der angeordnete Change Stopp wurde zum Zeitpunkt der Ergebnisbesprechung aufgehoben. Aus diesem Grund verzichtet die EFK hier auf eine Empfehlung.

Wenn Endsysteme redundant ans Netzwerk angeschlossen sind, können Wartungsarbeiten an den Netzwerkanschlüssen ohne Betriebsunterbruch durchgeführt werden. Die fehlende klare Anweisung, Endsysteme in den Datacentern immer redundant an das Netzwerk angeschlossen werden müssen, verhindert die Durchführung von netzwerkbezogenen Wartungsarbeiten im laufenden Betrieb. Ein einzelnes IP-Interface ist aufgrund der Ausfallwahrscheinlichkeit oder Einschränkungen bei der Wartung nicht empfehlenswert.

Empfehlung 7 (Priorität 2)

Die EFK empfiehlt dem BIT, den redundanten Anschluss von Endsystemen in Datacentern zu prüfen und in den technischen Anweisungen, wenn möglich, entsprechend zu fordern.

Stellungnahme des BIT

Die Empfehlung ist akzeptiert.

Die Empfehlung ist akzeptiert.

Die Empfehlung ist bereits umgesetzt und entspricht der seit längerem vorhandenen Praxis.

Das BIT verfügt heute bereits über eine technische Richtlinie, die einen redundanten Anschluss von Systemen an die Netzwerke im Datacenter fordert. Diese technische Richtlinie wird seit längerem (2018) systematisch umgesetzt.

(https://community.bit.admin.ch/team/eabit/Private/iktvorgaben/IKTVorgaben%20genehmigt/R0109_V1.2.pdf)

3 Überwachung der Netze und der Netzübergänge

3.1 Lücken in der Netzüberwachung

Die Netzwerke des BIT werden nicht flächendeckend und regelmässig auf Schwachstellen geprüft. Zudem sind aufgrund der Reorganisation im BIT die Verantwortlichkeiten für die BIT eigene Scan-Infrastruktur noch unklar. Diese Problematik zeigt auch der «Quartalsbericht 2021 Q1 Vulnerability Assessment» auf. Die ehemals Verantwortlichen arbeiten nicht mehr bei SI-SUR-SEC. Der Weiterbetrieb ist derzeit als «Rucksack» definiert. Dadurch besteht das Risiko, dass die Arbeiten und die Betreuung der Stakeholder des Scanning vorübergehend nicht in der gewohnten Qualität durchgeführt werden. Ein neuer Security Officer wurde mit der Erarbeitung der Vorgaben für Betrieb und Weiterentwicklung des Schwachstellen-Scannings beauftragt. Künftig sollen die Arbeiten durch die dezentralen Cyber-Champions durchgeführt werden.

Die interne Netzwerkkommunikation der bestehenden Netzwerk-Infrastruktur (Legacy) wird mehrheitlich [redacted]. Dies bedeutet, dass die Web Application Firewall (WAF) [redacted].

Im Bereich der drahtlosen Kommunikation (WLAN) ist in der Bundesverwaltung Network Access Control (NAC) zu 100% aktiviert. Diese Technologie dient der Abwehr von Schadsoftware und unautorisierten Zugriffen aus dem Netzwerk. Auf kabelgebundenen Access Ports ist NAC [redacted] implementiert. Durch das Projekt «Migration Client Zone», welches zum Prüfzeitpunkt gestartet wurde und bis zirka Ende 2023 abgeschlossen werden soll, wird der NAC Mechanismus in der ganzen Client Zone, inkl. deren Unterzonen aktiviert werden. Dies in Umsetzung der Anforderungen aus der Zonenpolicy «Client Zone». Nach Abschluss des Projektes soll NAC auf 80 - 90% der kabelgebundenen Access Ports aktiv sein. Nicht vorgesehen ist NAC für Spezial-Ports insbesondere bei der [redacted] und der [redacted] der Bundesverwaltung. Dazu wären Folgeprojekte erforderlich.

Im internen Netzwerk (LAN) findet [redacted] statt. Auf Client Ports der Netzwerkkomponenten wird die Anzahl der Hardware-Adressen überwacht. Diese Praxis verhindert, dass mehr als zwei Adressen pro Port existieren können. In einem solchen Fall wir dieser blockiert und eine Meldung generiert.

Der im Rahmen der technischen Prüfung durchgeführte Schwachstellenscan im CCN zeigte einige Schwachstellen mit der Kritikalität «Hoch» auf. Die Details zu den technischen Scans wurden dem BIT zur Verfügung gestellt.

Beurteilung

Um Schwachstellen auf Netzwerkkomponenten oder in Software zeitnah zu finden und zu schliessen, sollten Schwachstellenscans regelmässig und flächendeckend durchgeführt werden. Prioritär sollen die exponierten Bereiche, wie der Netzwerk-Perimeter oder das Core Netzwerk gescannt werden. In der Klärung der Verantwortlichkeiten ist zu regeln durch wen und wie schnell Schwachstellen geschlossen werden müssen. Weiter ist sicherzustellen, dass eine Nachprüfung oder ein erneuter Schwachstellenscan als Kontrolle durchführt wird.

Der Schutz der Netzwerke muss immer dem aktuellen Stand der Technik respektive der aktuellen Bedrohungslage entsprechen. Gute Praxis in der Netzwerkarchitektur ist heute,

nicht nur den Netzwerk-Perimeter, sondern auch Zonenübergänge aktiv zu überwachen und Massnahmen zur Erkennung sowie Behandlung von Anomalien zu implementieren. Beim Befall von Systemen kann damit die Verbreitung von Infektionen eingedämmt werden.

NAC ist eine wirkungsvolle Sicherheitsmassnahme, um den Zugang von nicht berechtigten Endgeräten zum Netzwerk zu verhindern. Insbesondere die Domotik Endgeräte oder Endgeräte der Gebäudeautomation, welche sich oft an schlecht zutrittsgesicherten Orten befinden, sollten daher auch einen NAC-Schutz aufweisen. Um den Schutz des internen Netzwerkes zu erhöhen, ist die Implementation von NAC innerhalb der Bundesverwaltung eine dringend umzusetzende Massnahme. Die EFK erachtet die Ziele im Rahmen des Projekts «Migration Client Zone», als angemessen.

Ein flächendeckender Einsatz von IDS/IPS innerhalb aller LAN-Zonen ist aus Sicht EFK nicht zwingend. Es sollte jedoch darauf geachtet werden, dass ein IDS/IPS je nach Schutzbedarf der Informationen an ausgewählten Zonengrenzen implementiert wird.

Empfehlung 8 (Priorität 1)

Die EFK empfiehlt dem BIT, die Verantwortlichkeit für die Scan-Infrastruktur umgehend zu klären und periodische und flächendeckende Schwachstellenscans durchzuführen.

Stellungnahme des BIT

Die Empfehlung ist akzeptiert.

Die Empfehlung ist akzeptiert.

Das Vorgehen wird durch den CSO geklärt. Heute werden Referenzgeräte gescannt. Sollen alle 22’000 vom BIT betriebene Netzwerkelemente gescannt mit dem heute eingesetzten Werkzeug Tenable Security Center gescannt werden, sind die Lizenzkosten hoch. Aktuell sind Klärungen im Gang ob mit anderen Lösungen flächendeckende Scans durchgeführt werden können.

Empfehlung 9 (Priorität 1)

Die EFK empfiehlt dem BIT, die aktive Nutzung der Web Application Firewall auch innerhalb des Netzwerkes an den jeweiligen Zonenübergängen sicherzustellen. Dadurch können Anomalien in den Netzwerken erkannt und die Ausbreitung von möglichen Infektionen zeitnah unterbunden werden.

Stellungnahme des BIT

Die Empfehlung ist akzeptiert.

Die Empfehlung ist akzeptiert.

Die Empfehlung ist bereits umgesetzt und entspricht der seit längerem vorhandenen Praxis.

Der Einsatz einer Web-Application-Firewall an jedem Zonenübergang (d.h. sowohl innerhalb des Rechenzentrums als auch zwischen Clients (internen wie externen)) für Zugriffe auf Webanwendungen ist in der Zonenpolicy jeder Zone nach Si003 (und Si001 v5) vorgeschrieben und ist so umgesetzt.

3.2 Firewall-Regeln werden nicht konsequent gelöscht

Für die Erstellung von Regeln auf den Firewall besteht ein zweckmässiger Prozess. Jedoch ist kein Prozess zur Auswertung und anschliessenden Deaktivierung von nicht mehr benutzten Firewall-Regeln implementiert. Im Gegensatz zur Erstellung werden die Deaktivierung und Löschung nicht immer gemeldet. Dies führt zu unnötigen Übergängen was ein gewisses Sicherheitsrisiko darstellt.

Beurteilung

Die Meldung der Deaktivierung und Löschung von Firewall-Regeln ist auch aus Sicht der EFK ein schwieriges Unterfangen. Die Beantragung von Firewall-Regeln erfolgt oft im Rahmen von Projekten zur Einführung von neuen Systemen und Anwendungen. Nach Projektabschluss werden die Systeme und Anwendungen bis zum End of Life dem Betrieb übergeben. Auch während dem Betrieb sind oft Anpassungen an Firewall-Regeln erforderlich.

Die effektivste Variante alle Firewall-Regeln im Überblick zu behalten besteht darin, deren Anwendung zu überwachen. Wenn Firewall-Regeln über einen bestimmen Zeitraum nicht mehr angewendet werden, kann mit den Betreibern der Systeme und Anwendungen Kontakt aufgenommen und die Deaktivierung besprochen werden.

Empfehlung 10 (Priorität 1)

Die EFK empfiehlt dem BIT, die Verwendung von Firewall-Regeln zu überwachen und einen Prozess zur Deaktivierung und Löschung von nicht mehr benutzten Firewall-Regeln zu schaffen.

Stellungnahme des BIT

Die Empfehlung ist akzeptiert.

Die Empfehlung ist akzeptiert.

Es existiert bereits ein MAC Prozess für das Löschen von Firewall-Regeln.

Das BIT wird einen Prozess definieren, um Firewall Regeln regelmässig – aber mit einer langen Periode, d.h. einmal jährlich - auf ihre Nutzung zu überwachen und in Absprache mit dem Antragsteller/Anwendungsbetreiber zu löschen. Die lange Periode ist damit begründet, dass in verschiedenen Fällen Kommunikationsbeziehungen nur sehr sporadisch genutzt werden und somit einen langen Beobachtungszeitraum erfordern.

3.3 Manipulationen an Konfigurationen könnten vertuscht werden

Systemlogs werden von den Netzwerkkomponenten automatisch an Syslog-Server, das OSS und an das Computer Emergency Response Team (CSIRT) weiterversandt. Wenn die Systemlogs aufgrund unterbrochener Kommunikation nicht an die zentralen Systeme weitergeleitet werden können, findet keine nachträgliche Weiterleitung mehr statt. Bei ausbleibender oder deaktivierter Weiterleitung von Systemlogs kann nicht nachvollzogen werden, ob lokale Systemlog Konfiguration von Administratoren geändert wurden und ob Einträge in Systemlogs nachträglich verändert wurden.

Durch das OSS werden alle vier Stunden die Konfigurationen von den Netzwerkkomponenten gelesen und in OSS gespeichert. Mit dem Werkzeug «Config Viewer» ist ein Versionsvergleich möglich. Die Versionen der Konfigurationen werden jedoch nicht proaktiv auf Änderungen verglichen.

Auf das OSS und damit auf die Netzwerkkomponenten haben eine Vielzahl interner und externer Mitarbeiter Vollzugriff. Die Begründung liegt darin, dass die Pikett-Organisation auf Basis der Aufbauorganisation des BIT vor der Transformation aufgebaut ist. Aktuell werden neue Zugriffsgruppen geschaffen, um die Zugriffsberechtigungen granularer zu verteilen.

Beurteilung

Die Konfiguration erlaubt, dass lokale Logs und Systemereignisse bei Unterbrüchen aktiv von Administratoren ausgesetzt oder manipuliert werden können. Dadurch könnten Konfigurationsänderungen vertuscht werden. Es besteht die Möglichkeit innerhalb OSS die Konfigurationen zu vergleichen, was jedoch weder systematisch noch mittels Stichproben gemacht wird.

Das Risiko der Manipulation von Logs und Systemereignissen wird durch die hohe Anzahl von Administratoren mit umfassenden Zugriffsrechten zusätzlich erhöht. Der Umstand, dass die Pikett-Organisation noch nach der alten Aufbauorganisation funktioniert, ist den involvierten Personen bewusst. Auch wurden bereits Aktivitäten in die Wege geleitet, um die Zugriffe auf Mitglieder der sieben DevOps-Teams von PS-NET zu verteilen.

Empfehlung 11 (Priorität 2)

Die EFK empfiehlt dem BIT, regelmässige Abgleiche oder Stichproben der Konfigurationen vorzunehmen, um unberechtigte Konfigurationsänderungen festzustellen.

Stellungnahme des BIT

Die Empfehlung ist akzeptiert.

Die Empfehlung ist akzeptiert.

Das BIT wird im Rahmen der Umsetzung der WTO 20011 (Lifecycle Netzwerk-Elemente) einen Prozess etablieren, bei dem die Konfigurationen periodisch mit der Soll-Konfiguration verglichen und validiert werden. Dies stellt eine Verbesserung gegenüber den heute praktizierten regelmässigen Konfigurations-Vergleichen dar.

3.4 Durch eine fehlende Validierung können mangelhafte Konfigurationen über längere Zeit bestehen

Während der technischen Überprüfung konnte festgestellt werden, dass keine zyklische Validierung der bestehenden Konfigurationen vorgenommen wird. Unsachgemässe Anpassungen von Konfigurationen können so über einen längeren Zeitraum unbemerkt weiterbestehen. Durch die fehlende regelmässige Validierung der Konfigurationen haben sich tatsächliche Schwachstellen ergeben. Beispielsweise blieben dadurch [redacted] oder nicht mehr zeitgemässe [redacted] unbemerkt bestehen.

Beurteilung

Durch die fehlende, zyklische Überprüfung von Konfigurationen können mangelhafte Konfigurationen unbemerkt und über einen längeren Zeitraum bestehen. Wenn Konfigurationen nicht via geordnetes Change-Management durchgeführt werden, wird gegen die Vorgabe des IKT-Grundschutzes verstossen.

Auf Grund der Wichtigkeit des SD DAKO sind zyklische Konfigurationsprüfungen vorzunehmen.

Empfehlung 12 (Priorität 2)

Die EFK empfiehlt dem BIT, zyklische Validierungen der Konfigurationen vorzunehmen, um allfällige mangelhafte Konfigurationen und unberechtigte Änderungen zu erkennen.

Stellungnahme des BIT

Die Empfehlung ist akzeptiert.

Die Empfehlung ist akzeptiert.

Das BIT wird im Rahmen der Umsetzung der WTO 20011 (Lifecycle Netzwerk-Elemente) einen Prozess etablieren, bei dem die Konfigurationen periodisch mit der Soll-Konfiguration verglichen und validiert werden. Dies stellt eine Verbesserung gegenüber den heute praktizierten regelmässigen Konfigurations-Vergleichen dar.

4 Erhaltung und Wiederherstellung der Infrastruktur nach Angriffen

4.1 Wiederherstellungsverfahren müssen regelmässig geprobt werden

Die Schutzbedarfsanalyse des OSS weist in der Einstufung der Verfügbarkeit «ITSCM / BCM notwendig» aus. Als Begründung wird angeführt: «Anwendungen des OSS Clusters sind Hilfsmittel im Wiederanlauf RZ und notwendig zur Netzwerk-Lageübersicht und für die Wiederherstellung von Netzkomponenten im Störungsfall». Zum Prüfzeitpunkt wurde noch kein Disaster Recovery Test des OSS durchgeführt.

Die gesamten Informationen des OSS befinden sich als Kopie auf [redacted] Notfallclients, die sich im [redacted], in zutrittsgeschützten Räumlichkeiten befinden. Die Aktualisierung der Notebooks erfolgt monatlich. Zudem wurden die Notebooks im Jahr 2019 von zwei Fachteams getestet. Zusätzlich werden vierteljährlich «Table-Tests» des Wiederanlaufplanes (WAP) durchgeführt, bei denen die Notwendigkeit eines Notfallclients und deren Aktualität überprüft wird. Ein Live-Test im Sinne einer Nutzung des Notfallclients im Rahmen des WAP wurde bis zum Prüfzeitpunkt nicht durchgeführt, ist jedoch ohne festgelegten Termin geplant.

Die Authentifizierung am OSS erfolgt mittels Username und Passwort, was bei einem so wichtigen System das absolute Minimum darstellt.

Beurteilung

Das OSS ist das Herzstück für den Betrieb des Netzwerkes, welches sämtliche für den Betrieb und die Wiederherstellung notwendigen Informationen beinhaltet. Das Backup auf [redacted] Notfallclients ist eine pragmatische Lösung, die aber nur sinnvoll ist, wenn mindestens nachfolgende Punkte berücksichtigt werden:

- Aktualität des Betriebssystems und der Anwendungen auf den Notebooks muss sichergestellt sein. Wenn im Ernstfall der Notebooks aufgrund von Softwareinstallationen nicht mehr performant arbeitet oder gar nicht mehr bootet kann der WAP nicht umgesetzt werden.
- Aktualität des OSS Dumps auf den Notebooks muss sichergestellt sein. Aufgrund der vielen, oft täglichen Änderungen, erscheint die Aktualisierungsperiode von einem Monat zu lang.
- Regelmässige Tests, bei denen die Notfallclients zum Einsatz kommen, müssen durchgeführt werden. Die Durchführung von «Table-Tests» ist positiv hervorzuheben. Die Erfahrung zeigt jedoch, dass sich «Table-Test» nur schwer mit einem Live-Test, d. h. einer effektiven Nutzung der Notfallclients beim WAP vergleichen lassen.
- Die Notfallclients müssen verfügbar sein. Diese in den zutrittsgeschützten Räumlichkeiten des [redacted] aufzubewahren ist grundsätzlich sinnvoll. Der EFK stellt sich jedoch die Frage, ob in einem Ernstfall die Clients genügend schnell im Datacenter Campus zur Verfügung stehen können.

Mit den Notfallclients kann ein temporärer Ausfall des OSS aufgefangen werden. Ein Desaster Recovery des OSS muss, wie im Grundschutz gefordert, periodisch geprüft werden, so dass im Ernstfall die Prozesse zur Wiederherstellung funktionieren.

Empfehlung 13 (Priorität 1)

Die EFK empfiehlt dem BIT, einen Desaster Recovery Test des gesamten OSS durchzuführen und diesen regelmässig zu wiederholen. Die Notfallclients sollten im Wiederanlaufplan 2022 für das Datacenter Campus mitberücksichtigt werden, d. h. sie sollten bei einem simulierten Ausfall des OSS aktiv genutzt werden.

Stellungnahme des BIT

Die Empfehlung ist akzeptiert.

Die Empfehlung ist akzeptiert.

Ein nächster Wiederanlauf-Test im RZ Campus ist am 19.06.2022 geplant. In diesem Rahmen werden Desaster-Recovery Tests des OSS durchgeführt.

Der Test der Notfallclients wird ebenfalls bei diesem Wiederanlauf durchgeführt.

4.2 Automatisierung kann kurzzeitige Ausfälle verhindern

Bei einem Ausfall eines der Datacenter müssen manuelle Arbeiten vorgenommen werden, um den Netzwerkverkehr aus den Aussenstellen umzuleiten. Dadurch entsteht ein Ausfall der Verbindungen. Die Umstellung der DNS-Einträge benötigt nach der Entdeckung des Ausfalles zwischen drei und fünf Minuten.

Beurteilung

Die manuell vorzunehmenden Tätigkeiten (DNS-Einträge für den MS VPN Zugang) können erst nach der Benachrichtigung respektive Alarmierung vorgenommen werden. Dadurch entstehen zeitliche Lücken, in der die Verbindungen zu den Rechenzentren ausbleiben. Je nach Dauer und Häufigkeit der Ausfälle kann dies die geforderte Verfügbarkeit des SD DAKO und der darüber kommunizierenden Dienste beeinträchtigen. Gemäss Schutzbedarfsanalyse SD DAKO ist pro Quartal ein Ausfall von gesamthaft zwei Stunden akzeptabel. Eine Automatisierung der Störungsbehebung ist beim BIT in Planung. Aus diesem Grund verzichtet die EFK auf eine Empfehlung.

Anhang 1: Rechtsgrundlagen

Rechtstexte
Bundesgesetz über die Eidgenössische Finanzkontrolle (Finanzkontrollgesetz, FKG) vom 28. Juni 1967 (Stand am 1. Januar 2018), SR 614.0
Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, CyRV), vom 27. Mai 2020 (Stand am 1. April 2021), SR 120.73
Verordnung über den Schutz von Informationen des Bundes (Informationsschutzverordnung, ISchV) vom 4. Juli 2007 (Stand am 1. Januar 2018), SR 510.411
Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992 (Stand am 1. Januar 2014) SR 235.1
Verordnung zum Bundesgesetz über den Datenschutz (VDSG) vom 14. Juni 1993 (Stand am 16. Oktober 2012) SR 235.11
Vorgaben
Si001 - IKT-Grundschutz Bundesverwaltung (Version 4.5)
Si003 – Netzwerksicherheit in der Bundesverwaltung (Version 3.0)
Si004 – Regelung der Zugriffe auf Ressourcen im Internet, Web Proxy Richtlinie Bundesverwaltung (Version 1.3)
Zonenpolicies Client Zonen Bund (Version 1.0)
Strategie
Strategie «Netzwerke des Bundes», November 2018

Anhang 2: Abkürzungen

BIC	BIT Internet Core
BIT	Bundesamt für Informatik und Telekommunikation
BV	Bundesverwaltung
CA Swiss Government PKI	Certificate authority - Public-Key-Infrastruktur (siehe Glossar)
CCN	Core Carrier Network
CSIRT	Computer Emergency Response Team
DNS	Domain Name System (siehe Glossar)
DTI	Bereich Digitale Transformation und IKT-Lenkung
EFK	Eidgenössische Finanzkontrolle
EEPROM	Electrically Erasable Programmable Read-Only Memory (siehe Glosar)
IDS	Intrusion Detection System (siehe Glossar)
IKT	Informations- und Kommunikationstechnik
IKT-SD	IKT-Standarddienst
IPS	Intrusion Prevention System (siehe Glossar)
ISDS-Konzept	Informationssicherheits- und Datenschutzkonzept (siehe Glossar)
LAN	Local Area Network (siehe Glossar)
LB	Leistungsbezüger
LE	Leistungserbringer
NAC	Network Access Control (siehe Glossar)
NCSC	Nationales Zentrum für Cybersicherheit
OCC	Operations Control Center
(Open-) LDAP	Lightweight Directory Access Protocol (siehe Glossar)

OSS	Operating Support System
PS	Plattform Services
PS-NET	Plattform Services - Network Services
SAFe	Scaled Agile Framework® (siehe Glossar)
SI	Strategy & Innovation
SI-SUR	Abteilung Chief Security Officer
SD DAKO	Standarddienst Datenkommunikation
SDN	Software-Defined Network (siehe Glossar)
VDI	Virtual Desktop Infrastructure (siehe Glossar)
WAF	Web Application Firewall (siehe Glossar)
WAP	Wiederanlaufplan

Anhang 3: Glossar

2-Faktor-Authentifizierung	Bezeichnet den Identitätsnachweis eines Nutzers mittels einer Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten (wissen und haben).
CA Swiss Government PKI	Zertifizierungsstelle des Bundes. Die Swiss Government PKI ist einer von drei zertifizierten Schweizer Anbietern, welche die hohen Anforderungen dieser Zertifizierungen erreicht.
DevOps	Sammlung unterschiedlicher technischer Methoden und die Kultur der Zusammenarbeit zwischen Softwareentwicklung und IT-Betrieb.
Domain Name System	Wichtiger Dienst in IP-basierten Netzwerken zur Beantwortung von Anfragen und Auflösung von Namen.
Domotik	Bezeichnung der Einrichtungen, Software und Dienstleistungen für automatische Steuerung und Regelung, Überwachung und Optimierung von Gebäuden und technischen Steuerungen.
Electrically Erasable Programmable Read-Only Memory	Ein EEPROM ist ein nichtflüchtiger, elektronischer Speicherbaustein, dessen gespeicherte Information elektrisch gelöscht werden kann.
Firewall	Eine Firewall ist ein Sicherungssystem, das ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt.
Flash-Speicher	Flash-Speicher sind digitale Speicherbausteine für eine nichtflüchtige Speicherung ohne Erhaltungs-Energieverbrauch. Die genaue Bezeichnung dieses Speichertyps lautet Flash-EEPROM. Im Gegensatz zu gewöhnlichem EEPROM-Speicher lassen sich hier Bytes nicht einzeln löschen oder überschreiben.
Intrusion Detection System	Ein Intrusion Detection System bzw. Angriffserkennungssystem ist ein System zur Erkennung von Angriffen, die gegen ein Computersystem oder Rechnernetz gerichtet sind.
Intrusion Prevention System	Als Intrusion-Prevention-Systeme werden Intrusion-Detection-Systeme bezeichnet, die über die reine Generierung von Ereignissen hinaus Funktionen bereitstellen, die einen entdeckten Angriff abwehren können.
Informationssicherheits- und Datenschutz Konzept	Das ISDS-Konzept bildet die Grundlage für die Festlegung der Massnahmen für die Informationssicherheit und den Datenschutz. Es zeigt die Restrisiken auf, die mit dem Betrieb des IT-Systems und der Organisation verbunden sind.

ISO/IEC 27001:2013	Die internationale Norm ISO/IEC 27001 definiert Anforderungen für Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheitsmanagementsystems (ISMS).
Legacy (-System)	Auch "Altsystem": Bezeichnet in der Informatik eine etablierte, historisch gewachsene Anwendung oder System.
Lightweight Directory Access Protocol	OpenLDAP ist eine Implementierung des LDAP, die als freie Software unter der der BSD-Lizenz ähnlichen OpenLDAP Public License veröffentlicht wird. OpenLDAP ist Bestandteil der meisten aktuellen Linux-Distributionen und läuft auch unter verschiedenen Unix-Varianten, macOS und verschiedenen Windows-Versionen.
Local Area Network	Netzwerk, das in seiner räumlichen Ausdehnung auf einen lokalen Bereich beschränkt ist.
Network Access Control	Technik, die die Abwehr von Viren, Würmern und unautorisierten Zugriffen aus dem Netzwerk heraus unterstützt. Mit NAC werden Endgeräte während der Authentifizierung auf Richtlinienkonformität geprüft.
Persistent - Non Persistent	Persistenz ist in der Informatik die Eigenschaft eines Systems, den Zustand seiner Daten, seines Objektmodells und/oder seiner logischen Verbindungen über lange Zeit – insbesondere über einen geplanten oder ungeplanten Programmabbruch hinaus – bereitzuhalten.
Proxy	Ein Proxy ist eine Kommunikationsschnittstelle in einem Netzwerk aus Rechnern in Form eines physischen Computers. Er arbeitet als Vermittler, der auf der einen Seite Anfragen entgegennimmt, um dann über seine eigene Adresse eine Verbindung zur anderen Seite herzustellen.
Scaled Agile Framework®	Das Scaled Agile Framework besteht aus einer Reihe von Organisations- und Workflow-Mustern zur Implementierung von Agile-Praktiken im gesamten Unternehmen. Das Framework ist eine Wissenssammlung mit strukturierten Leitlinien zu Rollen und Zuständigkeiten, zur Planung und Verwaltung von Aufgaben und zu förderungswürdigen Werten.
Software-Defined Network	Ansatz für Netzwerkvirtualisierung und Containerisierung, der eine Optimierung der Netzwerkressourcen und schnelle Anpassung von Netzwerken an sich ändernde Geschäftsbedürfnisse, Anwendungen und Datenverkehr ermöglicht. Der Ansatz funktioniert per Trennung der Steuerungs- und Datenebenen des Netzwerks und schafft eine softwareprogrammierbare Infrastruktur.

Virtual Desktop Infrastructure	Desktop-Virtualisierung ist ein generischer Begriff für jede Technologie, die eine Desktop-Umgebung von der Hardware trennt, die für den Zugriff auf diese Umgebung verwendet wird. VDI ist eine Art Desktop-Virtualisierung.
Web Application Firewalls	Eine Web Application Firewall ist ein Verfahren, das Webanwendungen vor Angriffen über das Hypertext Transfer Protocol schützen soll.

Priorisierung der Empfehlungen

Die Eidg. Finanzkontrolle priorisiert die Empfehlungen nach den zugrundeliegenden Risiken (1 = hoch, 2 = mittel, 3 = klein). Als Risiken gelten beispielsweise unwirtschaftliche Vorhaben, Verstösse gegen die Recht- oder Ordnungsmässigkeit, Haftungsfälle oder Reputationsschäden. Dabei werden die Auswirkungen und die Eintrittswahrscheinlichkeit beurteilt. Diese Bewertung bezieht sich auf den konkreten Prüfgegenstand (relativ) und nicht auf die Relevanz für die Bundesverwaltung insgesamt (absolut).

Anhang 4: Follow-up der offenen Empfehlungen

Nr.	Empfehlung	Status und Rückmeldungen der Geprüften	Beurteilung
16501.005	Die EFK empfiehlt dem BIT, die Risikoanalysen aus Projekten mit dem übergeordneten ISDS-Konzept SD DAKO abzugleichen und die Wirksamkeit der definierten Massnahmen zu prüfen.	Im Zusammenhang mit der Transformation im BIT (Midar), wurden grössere Anpassungen u. a. für Vorhaben vorgenommen. Die früheren Toll-Gates wurden durch Security Checks abgelöst. Die sicherheitsrelevanten Aspekte werden zudem durch die jeweiligen Cyber-Champions vertreten. Die Risikoanalysen werden von SI-SUR-SEC geprüft, wenn eine Anfrage der Qualitätssicherung vorhanden ist. Das Ausbildungsprogramm für Schlüsselpersonen und -rollen innerhalb des Informations-sicherheits-Management-System u. a. die Cyber-Champions wurde aufgebaut.	Die Empfehlung ist sinngemäss umgesetzt.
18484.001	Die EFK empfiehlt dem BIT, den Bestell- oder Freigabeprozess mittels einer geeigneten Compliance-Prüfung zu ergänzen. Es sollte sichergestellt werden, dass der Betrieb einer IKT-Anwendung durch einen LE erfolgt oder eine Ausnahmegenehmigung zur Leistungserbringung durch einen LB vorliegt.	Die dafür notwendigen Prozesse sind definiert und vorbereitet. Mit dem Schreiben vom 19.12.2020 wurde Empfehlung 1 und 3 eine Nachfrist und eine Überprüfung der Empfehlung seitens Direktion BIT angefragt. Von Seite EFK wurde die Nachfrist auf 30.06.2020 per Mail-AW vom 20.12.2019 gewährt. Mit dem EDI wurde eine Abstimmung bezüglich des Betriebs durch die Ämter initialisiert. Nach Rückmeldung des EDI wird dies auf Alle Departemente ausgerollt.	Die Empfehlung ist abgeschlossen, wenn der die Compliance-Prüfung im Bestellprozess implementiert ist.
18484.002	Die EFK empfiehlt dem BIT, einen Prozess zur regelmässigen, zielgruppenorientierten Ausbildung und Sensibilisierung zum Thema Cloud-Sicherheit zu etablieren.	Das BIT wird periodische Ausbildungs- und Sensibilisierungs-Sessions zum Thema Cloud-Sicherheit durchführen. Dieser Punkt wurde mit der Einführung und Ausbildung der Cyber Champions gut abgedeckt. Die Business Unit Cloud Services hat eine spezielle Rolle, welche das Thema Cloud Security für die Plattform dediziert bearbeitet.	Die Empfehlung ist sinngemäss umgesetzt.

18484.003	Die EFK empfiehlt dem BIT, Angaben zu den Kundenanwendungen in geeigneter Form abzufragen und in das entsprechende Inventar zu überführen.	Gemäss Schreiben des BIT vom 19. Dezember 2019: «Die Empfehlung wurde auf drei Ebenen vorbereitet. 1) Informationen aus dem zentralen Server-Verwaltungswerkzeug werden automatisiert in die föderierte, zentrale CMDB überführt, dies beinhaltet auch Informationen über installierte Software. 2) Mit «Atlantica Applikation» wird ein Service zur Daten-Modellierung angeboten, welcher die Zuordnung von Abonnementen (bestellte Server) zu Anwendungen ermöglicht. Diese Daten werden ebenfalls in besagte CMDB überführt. 3) Qualitätssicherung und weiterführende Automatisierungen werden durch neu etablierte Ansprechpartner innerhalb der Atlantica-Matrix Organisation (CMDB-Team) im kontinuierlichen Verbesserungsprozess erarbeitet. »	Die Empfehlung ist sinngemäss umgesetzt.
18484.004	Die EFK empfiehlt dem BIT, eine proaktive und periodische Analyse und Auswertung der Logdaten vorzunehmen, damit Gefahren frühzeitig erkannt und entsprechende Massnahmen eingeleitet werden können.	Protokollierungseinrichtungen und Protokollinformation sind vor Manipulation und unbefugtem Zugriff geschützt. Logdaten-Analyse (splunk) erfolgt durch das CSIRT. Tätigkeiten von Systemadministratoren und Systembedienern werden aufgezeichnet und die Protokolle sind geschützt und werden regelmässig überprüft. Schutz der Protokollinformation: Die Zuständigkeiten für die Log-Managementsysteme und somit für deren Sicherheit sind an das LMS-Team übergegangen.	Die Empfehlung ist sinngemäss umgesetzt.
18484.005	Die EFK empfiehlt dem BIT, ein regelmässiges Compliance Reporting zu etablieren, um allfällige Verstösse gegen die «Nutzungsbestimmungen für Cloud-Dienste» zu erkennen und allenfalls fehlbare Kunden zu sensibilisieren.	Mittels Server Automation Software wurden, insbesondere für die Verwaltung und die Prüfung von Abweichungen, Richtlinien definiert. Diese Richtlinien werden durch Server Automation regelmässig geprüft und Abweichungen werden ausgewiesen. Die Daten: Richtlinie, Anzahl Regeln, eingehalten, nicht eingehalten werden in das erweiterte Hilfsportal exportiert und intern wie auch für End-Konsumenten zur Verwendung angeboten. Richtlinien die nicht alle Regeln einhalten werden hervorgehoben.	Die Empfehlung ist sinngemäss umgesetzt.

18484.006	Die EFK empfiehlt dem BIT, die Durchführung von regelmässigen Sicherheits-Audits und -prüfungen zu planen, um aktuelle Bedrohungen frühzeitig erkennen zu können. Mindestens jährlich empfiehlt sich, eine Prüfung der vom BIT betriebenen Anwendungen und der Basisinfrastruktur durchzuführen.	Die Cloud-Plattform und die Gastsysteme wurden regelmässig mit dem Nessus-Werkzeug gescannt. Diese Scans werden auch weiterhin regelmässig durchgeführt. Der Bereich Sicherheit und Risikomanagement des BIT hat auf der Cloud bereits ein Sicherheitsaudit durchgeführt. Zudem trägt auch die Einführung der EFS (s. Empfehlung Nr. 4 durch das verbesserte Security Monitoring zur Zielsetzung der EFK-Empfehlung («aktuelle Bedrohungen frühzeitig erkennen») wesentlich bei.	Die Empfehlung ist sinngemäss umgesetzt.

18484.007	Die EFK empfiehlt dem BIT, im Sinne eines zusätzlichen Service, seinen Kunden die Möglichkeit zur Überprüfung der durch die LE betriebenen Anwendungen durch entsprechende Scans anzubieten. Dies im Sinne einer vorgeschlagenen Option im Provisionierungsprozess, welche der Kunde aktiv abwählen muss (Opt-out Option).	Das BIT wird im Bestellprozess für Server die entsprechenden Scan-Optionen einbauen. Die notwendigen betrieblichen Prozesse werden ebenfalls eingerichtet. Das BIT plant ab 2020 regelmässige Vulnerability Scans von im Internet erreichbaren Web-Anwendungen und -Services einzuführen. Dies schliesst solche ein, die auf der Cloud-Infrastruktur betrieben werden (ohne Opt-out für Kunden). 2019 hat das CSIRT und die Test-Automation ein Proof of Concept für solche automatisierten Scans durchgeführt. Der PoC hat die Machbarkeit bestätigt und gezeigt, dass dies auch möglich ist, ohne Ausfälle zu generieren. Es konnten zudem bereits im PoC etliche Schwachstellen erkannt und den Anwendungsverantwortlichen gemeldet werden. Ein manuelles Security Assessment kann natürlich tiefer gehen und wird durch diese automatisierten Scans im Internet nicht obsolet. Für rein intern zugängliche Web-Anwendungen gilt zudem weiterhin die Grundschutzanforderung 12.6.2, welche den Anwendungsverantwortlichen verpflichtet, Web-Scans zu machen. Diese können bereits heute via MAC vom Kunden bestellt werden. Das CSIRT BIT hat ab dem 3. Quartal 2019 das Scannen von Webanwendungen der BV fortgesetzt und hierfür eine Lösung auf Basis des durchgeführten Proof-of-concept aufgebaut. In den vergangenen 4 Berichtsperioden (Q3 2019 bis Q2 2020) hat das CSIRT insgesamt 400 Incidents zu erkannten Schwachstellen bearbeitet. In den vorangehenden 4 Berichtsperioden (Q3 2018 bis Q2 2019) waren dies lediglich 85. Die massive Zunahme ist aufgrund der erkannten Schwachstellen in Webanwendungen zu erklären. Das CSIRT scannte dabei nicht nur Webanwendungen der BV, die beim BIT gehostet werden, sondern auch solche mit externem Hosting. Aktuell ist das BIT an der Beschaffung eines externen Vulnerability Scan Services für das regelmässige Scannen von Webanwendungen, die über das Internet erreichbar sind.	Die Empfehlung ist sinngemäss umgesetzt.