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

Prüfung der Wirksamkeit der Vorfallbewältigung beim Schutz der Bundes-IKT vor Cyberrisiken

Nationales Zentrum für Cybersicherheit

EFK-21070 | inkl. Stellungnahmen | 8. Juli 2022 | FinDel D5/2022

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	600.21070
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

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

Inhaltsverzeichnis

Prüfung der Wirksamkeit der Vorfallbewältigung beim Schutz der Bundes-IKT vor Cyberrisiken

Nationales Zentrum für Cybersicherheit

Das Wesentliche in Kürze

Als Fachstelle IKT-Sicherheit des Bundes (IKT steht für Informations- und Kommunikationstechnologie) erlässt das Nationale Zentrum für Cybersicherheit (NCSC) Vorgaben zur Cybersicherheit innerhalb der Bundesverwaltung (BV), überprüft deren Einhaltung und unterstützt die Leistungserbringer bei der Beseitigung von Schwachstellen.

Die vom Bundesrat verabschiedete Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung ist seit dem 1. Juli 2020 in Kraft. Sie bildet die rechtliche Grundlage für den Auf- und Ausbau des NCSC und regelt Struktur und Aufgaben sowie Kompetenzen der beteiligten Behörden. Darin wurde das NCSC ermächtigt, bei einem Cybervorfall der das ordnungsgemässe Funktionieren der BV gefährdet, nach Rücksprache mit den betroffenen Dienststellen, die Federführung bei der Bewältigung zu übernehmen.

Im Rahmen dieser Prüfung hat die Eidgenössische Finanzkontrolle (EFK) den entsprechenden Prozess auf seine Wirksamkeit überprüft. Dabei wurden insbesondere die Fragestellungen des zeitnahen Informationsflusses von den Informationsquellen zum NCSC, sowie die Zusammenführung dieser Informationen mit den eigenen Überwachungsergebnissen beurteilt. Des Weiteren wurden das Erkennen eines Cybervorfalls und die zeitgerechte Umsetzung von Massnahmen und der Informationsfluss zu den relevanten Stellen evaluiert.

Der Vorfallbewältigungsprozess ist definiert, publiziert und wird durchgeführt. Die Rollen und Zuständigkeiten sind grundsätzlich zugewiesen, aber die Rolle der Informatiksicherheitsbeauftragten der Organisationseinheiten (ISBO) muss gestärkt werden. Verbesserungsbedarf besteht hinsichtlich der Übersicht über die Akteure, wenn externe Leistungserbringer involviert sind. Die Rahmenbedingungen sind zwar grundsätzlich geeignet, doch die Kommunikationswege und die Aktualität von Meldungen müssen verbessert werden.

Die Meldung eines Cybervorfalls muss schneller erfolgen

Die unverzügliche Meldung eines Cybervorfalls ist wichtig, damit eine übergeordnete Analyse und Einschätzung der Gefahr gemacht werden kann. Dadurch kann die Gefahr einer lateralen Ausbreitung in der gesamten BV eingedämmt oder im besten Fall verhindert werden. Im Rahmen der Prüfung hat die EFK festgestellt, dass die Kommunikation ans NCSC noch ausgebaut werden muss. So ist die horizontale Steuerung, insbesondere der Informationsaustausch zwischen den Leistungserbringern (LE), noch nicht überall sichergestellt. Zudem müssen die Informatiksicherheitsbeauftragten der Departemente schneller informiert werden.

Herausfordernd ist auch die Koordination respektive Harmonisierung der Kategorisierung von Cybervorfällen, wenn ein solcher mehrere LE betrifft. Wenn dies nicht geschieht, be-

steht die Gefahr, dass die verschiedenen LE einen Vorfall mit unterschiedlicher Priorität angehen. Eine solche Konstellation kann auch zu inkonsistenter Kommunikation gegenüber Dritten führen.

Die Rolle des ISBO sollte gestärkt und eine Übersicht externer LE geschaffen werden

Eine wichtige Rolle, um Cybervorfälle zu melden, nehmen die ISBO ein: Als Leistungsbezüger (LB) melden sie Cybervorfälle an ihre LE, die wiederum das NCSC informieren. Da je nach Grösse der LB unterschiedliche Maturitätsniveaus bestehen, ist jedoch nicht immer eine Stellvertretung definiert. Bei Abwesenheit des ISBO kann sich die Meldung eines Cybervorfalls entsprechend verzögern und damit auch die zeitnahe Meldung an das NCSC. Dies sollte umgehend korrigiert werden.

Bei Auftreten eines Cybervorfalls kann nicht innert kurzer Zeit festgestellt werden, welche Applikationen und Services von welchem Lieferanten für welche Verwaltungseinheit (VE) betreut werden. Somit können bei der Meldung eines IT-Sicherheitsvorfalls bei einem externen LE die betroffenen VE nicht umgehend informiert werden, was grundsätzlich die Verwundbarkeit der BV erhöht. Die Erstellung eines übergreifenden Inventars sollte folglich in Betracht gezogen werden.

Werkzeuge sollten effizienter eingesetzt werden

Die Beschaffung von Überwachungswerkzeugen sollte auf Stufe BV harmonisiert werden und zentral erfolgen, um nicht unterschiedliche Werkzeuge mit denselben oder ähnlichen Funktionalitäten einzusetzen. Dadurch werden mögliche Skaleneffekte hinsichtlich der Kosten und des Know-how–Aufbaus genutzt.

Die Mustervertragsklausel muss optimiert werden

Die Beschaffungskonferenz des Bundes hat eine Mustervertragsklausel betreffend Cyberrisiken erstellt. Die vertraglichen Punkte zur Informatiksicherheit gehen in die richtige Richtung. Fristen zur Meldung von Cybervorfällen sind jedoch nicht einheitlich vorgegeben und müssten entsprechend praxistauglich definiert werden. Zudem müsste diese Klausel bei langjährigen Verträgen nachverhandelt werden.

Audit de l'efficacité de la gestion des incidents dans la protection des TIC fédérales contre les cyber-risques

Centre national pour la cybersécurité

L'essentiel en bref

Comme service spécialisé dans la sécurité des technologies de l'information et de la communication (TIC) de l'administration fédérale, le Centre national pour la cybersécurité (NCSC) édicte des directives en matière de cybersécurité au sein de l'administration fédérale, en vérifie le respect et aide les fournisseurs de prestations à éliminer les vulnérabilités.

Adoptée par le Conseil fédéral, l'Ordonnance sur la protection contre les cyber-risques dans l'administration fédérale est en vigueur depuis le 1er juillet 2020. Elle constitue la base juridique pour la création et le développement du NCSC et définit la structure, les tâches et les compétences des autorités impliquées. Le NCSC y est habilité à prendre la direction des opérations en cas de cyber-incident présentant une menace pour le bon fonctionnement de l'administration fédérale, en concertation avec les services concernés.

Lors de cet audit, le Contrôle fédéral des finances (CDF) a vérifié l'efficacité du processus en place. Il a évalué en particulier les échanges en temps réel entre les sources d'information et le NCSC ainsi que le regroupement de ces informations avec les résultats de la propre activité de surveillance du NCSC. En outre, son évaluation a porté sur l'identification d'un cyber-incident et la mise en œuvre de mesures en temps utile ainsi que sur la transmission des informations aux services concernés.

Le processus de gestion des incidents est défini, publié et appliqué. Les rôles et responsabilités sont en principe attribués, mais le rôle des délégués à la sécurité informatique des unités administratives (DSIO) doit être renforcé. Des améliorations sont nécessaires en ce qui concerne la vue d'ensemble des acteurs lorsque des fournisseurs de prestations externes sont impliqués. Les conditions-cadres sont généralement appropriées, mais les canaux de communication et l'actualité des notifications doivent être améliorées.

La notification d'un cyber-incident doit être plus rapide

La notification immédiate d'un cyber-incident est importante, pour permettre une analyse et une évaluation globales du risque. Cela permet de limiter ou, dans le meilleur des cas, d'éviter le risque de propagation latérale dans toute l'administration fédérale. Lors de son audit, le CDF a constaté que la communication avec le NCSC doit encore être développée. Ainsi, la gestion des incidents au niveau horizontal, notamment les échanges d'informations entre fournisseurs de prestations (FP), n'est pas encore assurée partout. En outre, les délégués à la sécurité informatique des départements (DSID) doivent être informés plus vite.

La coordination ou l'harmonisation de la classification des cyber-incidents, lorsqu'ils concernent plusieurs FP, constitue également un défi. Sinon il est à craindre que les différents FP n'accordent pas la même priorité aux incidents. Une telle situation peut aussi conduire à une communication incohérente avec des tiers.

Le rôle du DSIO devrait être renforcé et une vue d'ensemble des fournisseurs de prestations externes devrait être créée

Les DSIO jouent un rôle important dans la notification des cyber-incidents : en tant que bénéficiaires de prestations (BP), ils signalent ces incidents à leurs FP, qui informent à leur tour le NCSC. Comme il existe différents niveaux de maturité en fonction de la taille des BP, il n'est toutefois pas toujours possible de définir une suppléance. En l'absence du DSIO, la notification d'un cyber-incident peut être retardée, de même que la notification immédiate au NCSC. Cette situation doit être corrigée sans délai.

En cas de cyber-incident, il n'est pas possible de déterminer rapidement quelles applications et quels services sont gérés par quel fournisseur pour quelle unité administrative (UA). Par conséquent, si un incident de sécurité informatique est signalé à un FP externe, il n'est pas possible d'informer immédiatement les UA concernées, ce qui augmente en principe la vulnérabilité de l'administration fédérale. Il faudrait donc songer à établir un inventaire général.

Les outils devraient être utilisés plus efficacement

L'acquisition d'outils de surveillance devrait être harmonisée au niveau de l'administration fédérale et centralisée pour éviter l'utilisation d'outils différents dotés de fonctions identiques ou similaires. Cela permet de profiter d'éventuelles économies d'échelles en termes de coûts et d'acquisition de savoir-faire.

La clause contractuelle type doit être optimisée

La Conférence des achats de la Confédération a élaboré une clause contractuelle type pour les cyber-risques. Les points de cette disposition concernant la sécurité informatique vont dans la bonne direction. Cependant, les délais de notification des cyber-incidents ne sont pas fixés de manière uniforme et devraient être définis en conséquence. En outre, cette clause devrait être renégociée dans les contrats de longue durée.

Texte original en allemand

Verifica concernente l'efficacia della gestione degli incidenti nella protezione dell'informatica federale dai ciber-rischi

Centro nazionale per la cibersicurezza

L'essenziale in breve

Il Centro nazionale per la cibersicurezza (NCSC), in qualità di servizio specializzato della sicurezza TIC (TIC è l'acronimo di tecnologie dell'informazione e della comunicazione), emana direttive sulla cibersicurezza in seno all'Amministrazione federale, ne verifica il rispetto e sostiene i fornitori di prestazioni nell'eliminazione di vulnerabilità.

L'ordinanza sulla protezione contro i ciber-rischi nell'Amministrazione federale, licenziata dal Consiglio federale, è in vigore dal 1° luglio 2020 e costituisce la base giuridica per l'istituzione e il potenziamento dell'NCSC. Disciplina la struttura, i compiti e le competenze delle autorità coinvolte. Essa autorizza l'NCSC, previa consultazione dei servizi interessati, ad assumersi la responsabilità principale della gestione di un ciberincidente se questo minaccia il corretto funzionamento dell'Amministrazione federale.

Nel quadro della presente verifica, il Controllo federale delle finanze (CDF) ha esaminato l'efficacia del processo. In particolare, ha controllato se lo scambio di informazioni tra le fonti e l'NCSC avviene in tempo reale e ha analizzato il modo in cui tali informazioni vengono integrate nei risultati della propria sorveglianza. Sono inoltre stati valutati l'individuazione di un ciberincidente, la tempestiva dell'attuazione di misure e il flusso di informazioni verso gli uffici interessati.

Il processo per la gestione degli incidenti è stato definito, pubblicato e viene applicato. In linea di principio i ruoli e le responsabilità sono stati attribuiti, ma il ruolo dell'incaricato della sicurezza informatica a livello di unità organizzativa (ISIU) deve essere rafforzato. Conviene altresì precisare l'elenco degli attori nel caso in cui sono interessati fornitori di prestazioni esterni. Le condizioni quadro sono adeguate, ma i canali di comunicazione e l'attualità delle notifiche devono essere migliorate.

Maggiore rapidità nel segnalare un ciberincidente

Per poter stimare i rischi ed effettuare un'analisi generale, è importante che i ciberincidenti siano segnalati immediatamente. In tal modo si può ridurre o evitare, nel migliore dei casi, il pericolo di una propagazione laterale nell'intera Amministrazione federale. Nel quadro della sua verifica, il CDF ha constatato che la comunicazione all'NCSC deve essere sviluppata ulteriormente. Ad esempio, la gestione a livello orizzontale, in particolare lo scambio di informazioni tra i fornitori di prestazioni, non è ancora garantita ovunque. Inoltre, gli incaricati della sicurezza informatica presso i dipartimenti devono essere informati con maggiore rapidità.

Un'altra sfida consiste nella classificazione dei ciberincidenti, che bisognerebbe coordinare o armonizzare quando riguardano più unità amministrative. In caso contrario vi è il rischio che le diverse unità amministrative attribuiscano all'incidente un grado di priorità diverso.

Una situazione di questo tipo potrebbe comportare anche una comunicazione non coerente con terzi.

Rafforzamento del ruolo dell'ISIU e creazione di un elenco dei fornitori di prestazioni esterni

Gli ISIU rivestono un ruolo importante nella notifica dei ciberincidenti: in qualità di beneficiari di prestazioni segnalano i ciberincidenti alla propria unità amministrativa, che provvede a informare l'NCSC. Poiché il livello di maturità dei beneficiari di prestazioni cambia a seconda delle loro dimensioni, non sempre è stata definita una supplenza. In caso di assenza dell'ISIU, la segnalazione di un ciberincidente può subire ritardi e quindi anche la conseguente segnalazione all'NCSC. Questa situazione deve essere corretta senza indugio.

In caso di ciberincidente è impossibile stabilire in tempi brevi quali siano le applicazioni e i servizi toccati, quale sia il fornitore e quale l'unità amministrativa per cui quest'ultimo li gestisce. In altre parole, in caso di segnalazione di un incidente relativo alla sicurezza informatica riguardante un fornitore di prestazioni esterno, le unità amministrative interessate non possono essere informate tempestivamente, cosa che rende l'Amministrazione federale più vulnerabile. Di conseguenza, si dovrebbe prendere in considerazione la creazione di un elenco completo.

Uso più efficiente degli strumenti

Per non impiegare strumenti di vigilanza differenti con funzionalità identiche o simili, il loro acquisto dovrebbe essere armonizzato a livello di Amministrazione federale ed effettuato centralmente. In tal modo si sfrutterebbero i possibili effetti di scala per quanto riguarda i costi e lo sviluppo del know-how.

Ottimizzazione del modello di clausola contrattuale

La Conferenza degli acquisti della Confederazione ha creato un modello di clausola contrattuale concernente i ciber-rischi. I punti relativi alla sicurezza informatica vanno nella giusta direzione. Tuttavia, poiché i termini per segnalare i ciberincidenti non sono specificati in maniera uniforme, bisognerebbe prevederne una definizione praticabile. Inoltre, la clausola dovrebbe poter essere rinegoziata nel caso dei contratti pluriennali.

Testo originale in tedesco

Audit of the effectiveness of incident management in protecting federal ICT from cyber-risks

National Cybersecurity Centre

Key facts

As the Confederation's specialist unit for ICT (information and communication technology) security, the National Cybersecurity Centre (NCSC) issues cybersecurity specifications within the Federal Administration, checks compliance with them and helps service providers to eliminate vulnerabilities.

The Ordinance on Protecting against Cyber-Risks in the Federal Administration adopted by the Federal Council entered into force on 1 July 2020. It provides the legal basis for the creation and expansion of the NCSC, and regulates the structure, tasks and powers of the authorities involved. The Ordinance grants the NCSC the power to take the lead in dealing with a cyberincident that jeopardises the proper functioning of the Federal Administration, after consulting the units concerned.

As part of this audit, the Swiss Federal Audit Office (SFAO) reviewed the effectiveness of the relevant process. In particular, the audit focused on issues relating to the timely flow of information from the sources to the NCSC, and on the merging of this information with the Centre's own monitoring results. In addition, the detection of cyberincidents and the timely implementation of measures, as well as the flow of information to the relevant units, was assessed.

The incident management process is clearly defined, published and applied. In general, the roles and responsibilities have been assigned but the role of IT security officer for the organisational units (ITSOO) must be strengthened. There is room for improvement as regards an overview of the participants when external service providers are involved. The framework conditions are generally appropriate but the communication channels and timeliness of reports must be improved.

Cyberincident reporting needs to be quicker

It is important that cyberincidents are reported immediately, to enable higher-level analysis and appraisal of the threat. This could allow the threat of a lateral spread across the entire Federal Administration to be contained or, at best, prevented. During the audit, the SFAO observed that communication with the NCSC needs to be expanded further. For example, horizontal management, especially the exchange of information between service providers, is not yet ensured in all areas. Moreover, the IT security officers of the departments must be informed more quickly.

The coordination/harmonisation of cyberincident categorisation also presents a challenge in cases where the incident affects more than one service provider. Where there is none, there is a risk that different service providers will assign different priorities to the same incident. Such a situation can also lead to inconsistent communication to third parties.

The role of the ITSOO should be strengthened and an overview of external service providers should be established

The ITSOOs have an important role in the reporting of cyberincidents: as service users, they report cyberincidents to their service providers, who in turn inform the NCSC. However, since there are different levels of maturity depending on the size of the service user, not all officers have assigned a deputy. Thus, in the ITSOO's absence, cyberincident reporting, and in turn the report to the NCSC, can be delayed. This situation should be corrected immediately.

In the event of a cyberincident, it cannot be ascertained quickly which applications and services from which provider, and for which administrative unit, need attention. As a result, when an IT security incident at an external service provider is reported, the affected administrative units cannot be informed immediately, which increases the vulnerability of the Federal Administration in general. Therefore, the creation of an overarching inventory should be considered.

Tools should be deployed more efficiently

The procurement of monitoring tools should be harmonised and centralised at Federal Administration level, to avoid the use of different tools with the same or similar functionalities. This would exploit economies of scale in terms of costs and knowledge base expansion.

Model contract clause must be optimised

The Federal Procurement Conference has drawn up a model contract clause on cyber-risks. The contractual provisions on information security are a step in the right direction. However, deadlines for reporting cyberincidents vary and would have to be defined in accordance with usual practice. Moreover, the clause would have to be renegotiated for long-term contracts.

Original text in German

Generelle Stellungnahme des Nationalen Zentrums für Cybersicherheit

Das NCSC dankt der EFK für die durchgeführte Prüfung zur Wirksamkeit der Vorfallbewältigung beim Schutz der Bundes-IKT vor Cyberrisiken. Es zeigt sich mit dem Bericht und den Einschätzungen der EFK einverstanden und unterstützt die im Bericht aufgezeigten Optimierungsmassnahmen im Sinne der Resilienzförderung der Infrastruktur des Bundes.

1 Auftrag und Vorgehen

1.1 Ausgangslage

Das Nationale Zentrum für Cybersicherheit (NCSC) und die Informatiksicherheitsbeauftragten der Departemente (ISBD) haben unter der Federführung der ISBD der Bundeskanzlei sowie der Mithilfe der Leistungserbringer (LE) den «Prozess zur Bewältigung von Cybervorfällen»[1] erarbeitet.

In der vorliegenden Prüfung wurde eine End-zu-End-Beurteilung dieses Prozesses durchgeführt, die sowohl verwaltungsinterne wie auch externe Akteure betrifft. Die Arbeit des NCSC resp. das Funktionieren dieses Melde- und Bearbeitungsprozesses, sollte anhand von zwei konkreten Vorfällen überprüft werden.

1.2 Prüfungsziel und -fragen

Prüfziel war die Beurteilung, ob Cybervorfälle gegen die Infrastruktur des Bundes zeitnah erkannt und abgewehrt bzw. bereinigt werden können.

Die Prüffragen lauteten:

1. Ist der Vorfallbewältigungsprozess definiert und sind die Rollen und Kompetenzen klar und zielführend zugewiesen?
2. Sind alle Akteure bekannt und in den Prozess integriert?
3. Ermöglichen die bestehenden Rahmenbedingungen (bspw. Gesetze, Technologie, usw.) die zeitgerechte und flexible Umsetzung und eine durchgängige Digitalisierung?
4. Sind die Informationsflüsse bei der Erkennung, der Abwehr resp. Bewältigung von Cyberangriffen auf die Bundesinfrastruktur durchgehend, effizient und zielführend?

1.3 Prüfungsumfang und -grundsätze

Die Prüfung konzentrierte sich auf die Umsetzbarkeit und Wirksamkeit des definierten Prozesses. Zudem wurde anhand von zwei abgeschlossenen Fällen geprüft, ob die Schnittstellen und Kommunikationswege wie geplant funktionieren.

Die Eidgenössische Finanzkontrolle (EFK) beschloss, die Prüffrage 1 bereits während der Vorbereitungsphase zu beantworten, damit eine Übersicht über die gesamte Bundesverwaltung (BV) gemacht werden konnte. Dabei wurden sämtliche Leistungserbringer (LE) Interviewt und die folgenden Fragen gestellt:

- Ist ein Cybervorfall-Prozess vorhanden?
- Sind die Rollen und Kompetenzen klar und entsprechend zugewiesen?
- Sind die Schnittstellen zur Bearbeitung von Cybervorfällen definiert?

Die Ergebnisse wurden dem NCSC in einem Brief am 30. Juni 2021 mitgeteilt und flossen in die Prüfungsdurchführung ein.

[1] https://intranet.ncsc.admin.ch/ncscintra/de/home/dokumentation/dokumente-partner/bundesverwaltung.html

Die Prüfung wurde von Christian Brunner (Revisionsleiter), Warren Paulus und Elizabeth O'Sullivan vom 14. März bis 14. April 2022 durchgeführt. Sie erfolgte unter der Federführung von Bernhard Hamberger. Der vorliegende Bericht berücksichtigt nicht die weitere Entwicklung nach der Prüfungsdurchführung.

1.4 Unterlagen und Auskunftserteilung

Die notwendigen Auskünfte wurden der EFK von allen involvierten Stellen umfassend und zuvorkommend erteilt. Die gewünschten Unterlagen standen dem Prüfteam vollumfänglich zur Verfügung.

1.5 Schlussbesprechung

Die Schlussbesprechung fand am 21. Juni 2022 statt. Teilgenommen haben von Seiten NCSC der Leiter Operative Cybersicherheit, der Koordinator / Controller NCS, der Leiter Informatiksicherheit Bund und die Leiterin Informatiksicherheitsvorgaben und Beratung. Seitens der EFK haben der zuständige Mandatsleiter, der zuständige Fachbereichsleiter und der Revisionsleiter teilgenommen.

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

EIDGENÖSSISCHE FINANZKONTROLLE

2 Wirksamkeit des Prozesses

Im April 2021 wurde der «Prozess zur Bewältigung von Cybervorfällen» in Kraft gesetzt. Ziel war es, in diesem Prozess die Anforderungen der Verordnung über den Schutz vor Cyberrisiken in der BV (Cyberrisikenverordnung, CyRV; SR 120.73) abzubilden. Im Rahmen dieser Prüfung wurde bei den zentralen LE der BV sowie zwei dezentralen LE der BV eine Erhebung zu einem bestehenden Cybervorfall-Prozess durchgeführt. Dabei wurden auch die Zuweisung der Rollen und Kompetenzen beurteilt. Alle LE haben einen Cybervorfall-Prozess definiert, der jedoch unterschiedlich und auf die eigenen Bedürfnisse angepasst ist. Da der übergeordnete «Prozess zur Bewältigung von Cybervorfällen» generisch gehalten ist, können die verschiedenen Prozesse jedoch gut darauf adaptiert werden. Die entsprechenden Rollen und Kompetenzen waren bei allen LE definiert und auch umgesetzt.

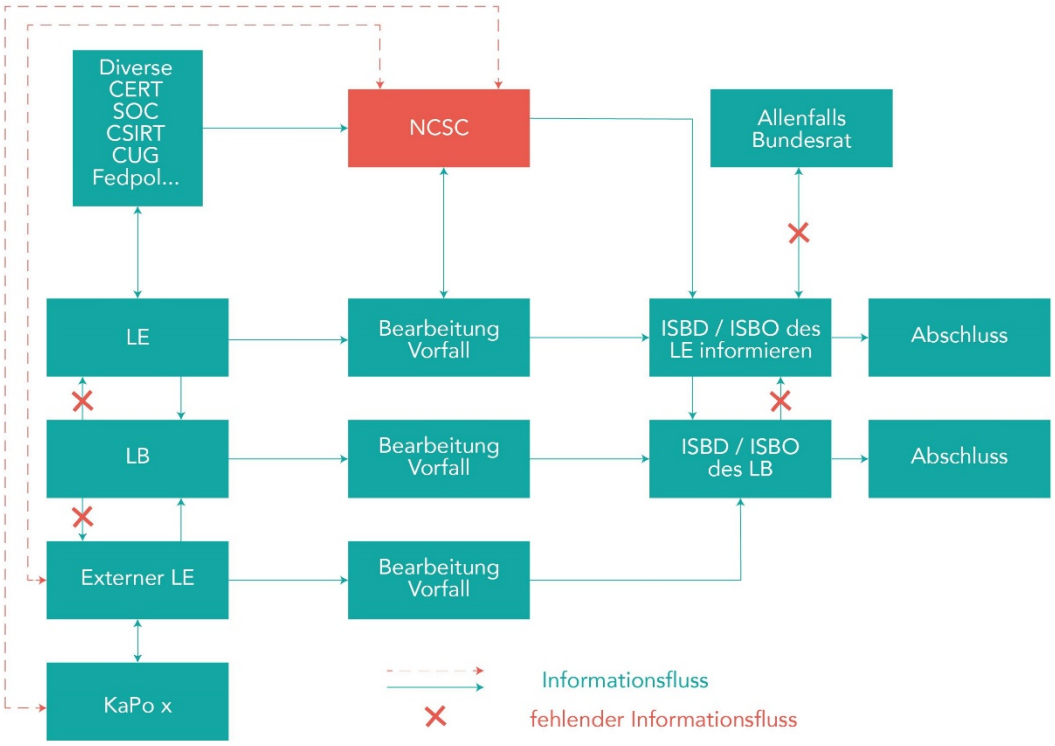
2.1 Der Informationsfluss ist nicht immer sichergestellt

Ziel des neuen Prozesses ist, dem NCSC Cybervorfälle zu melden, die das ordnungsgemässe Funktionieren der BV gefährden. Damit ist das NCSC in der Lage, nach Absprache mit den betroffenen Dienststellen, die übergeordnete Koordination bis zum Abschluss eines Vorfalls zu übernehmen[2].

Diese Meldungen sind für das NCSC sehr wichtig, um die Bedrohungslage einschätzen und aktuelle Angriffsmuster frühzeitig erkennen zu können. Um dies zu gewährleisten, müssen Vorfälle unverzüglich gemeldet werden. Entsprechend fordert die CyRV[3], dass die LE ihren Leistungsbezügern (LB) entdeckte Schwachstellen und Cybervorfälle in deren Informatikschutzobjekten unverzüglich melden.

Gemäss dem Prozess muss der LE sowohl dem LB sowie dem NCSC einen Cybervorfall melden. Anders verhält es sich beim LB. Dieser könnte auch via einen externen LE (siehe Kapitel 3) von einem Cybervorfall betroffen sein. In diesem Fall ist gemäss heutigem Prozess keine Kommunikation mit dem NCSC vorgesehen. Wenn der LE der BV nicht informiert wird, fehlt auch die Meldung ans NCSC. Die folgende Grafik stellt die Informationsflüsse vereinfacht dar:

[2] Art. 12, Abs. 5, CyRV
[3] Art. 14, Abs. 4 lit. c, CyRV



Grafik 1: Prozess zur Bewältigung von Cybervorfällen (Darstellung EFK)

Die Überarbeitung der Vorgaben ist bereits im Gange

Zum Prüfungszeitpunkt war der Entwurf der Verordnung über die Informationssicherheit in der BV und in der Armee (Informationssicherheitsverordnung, ISV) in der Ämterkonsultation. Diese soll per 1. April 2023 in Kraft treten und die CyRV ablösen. Im Art. 14, Abs. 4 werden die Kriterien zur Meldepflicht eines IT-Sicherheitsvorfalls konkreter definiert. Da die ISV noch in der Vernehmlassung ist, können die Kriterien hier noch nicht aufgeführt werden.

Zudem haben einzelne Verwaltungseinheiten (VE) ihre Vorgaben angepasst. So hat zum Beispiel das VBS die «Weisungen über die Meldung und Bewältigung von Cybervorfällen beim VBS (WeMBS VBS)» per 1. April 2022 in Kraft gesetzt. In diesen wurde in Ziff. 8, Abs. 2 die Definition zur Meldung von Vorfällen des Bereichs Digitalisierung und Cybersicherheit VBS (DCS) ans NCSC geschärft: «… erstattet dem Nationalen Zentrum für Cybersicherheit umgehend Meldung, wenn die Cybersicherheit der Bundesverwaltung (Art. 12, Abs. 5 CyRV) oder ein Informatiklieferant oder -dienstleister des Bundes betroffen ist.»

Herausfordernd ist die Koordination und Harmonisierung der Kategorisierung von Vorfällen (high, medium, low, usw.), wenn ein solcher mehrere LE betrifft. Falls dies nicht koordiniert wird, besteht die Gefahr, dass die verschiedenen VE einen Vorfall mit unterschiedlicher Priorität angehen. Dies kann auch zu inkonsistenter Kommunikation gegenüber Dritten führen.

Beurteilung

Die Koordination eines umfangreichen Vorfalls durch das NCSC ist zielführend. Dadurch kann sichergestellt werden, dass die Informationen mit allen Departementen geteilt, Massnahmen definiert und koordiniert umgesetzt werden können.

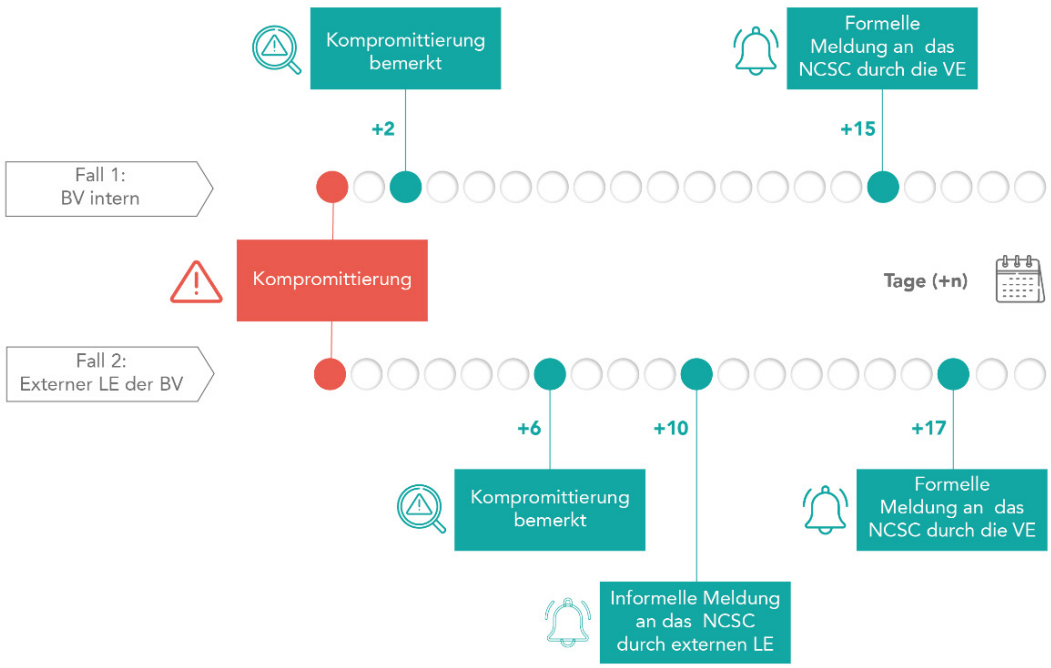
Um eine gesamtheitliche Sicht der Bedrohungen zu haben, ist das NCSC auf sämtliche Informationen angewiesen. Entsprechend ist es zu begrüssen, dass die Vorgaben angepasst und die Kriterien zur Meldepflicht eines Cybervorfalls klarer definiert werden. Die Rolle der LB sollte jedoch noch vertiefter beurteilt und, falls nötig, angepasst werden. Danach muss der Prozess an die geänderten Vorgaben angepasst werden.

Damit ein Vorfall überall dieselbe Aufmerksamkeit erhält, ist eine Anpassung und Harmonisierung der Kategorisierung zwischen den Departementen erforderlich. Hier gilt es zu klären, ob das NCSC diese Kategorisierung vornehmen sollte. Des Weiteren sollten die Verantwortlichkeiten für die Kommunikation geregelt werden.

Aufgrund der laufenden Überarbeitung der Vorgaben verzichtet die EFK auf eine Empfehlung.

2.2 Meldungen müssen rascher erfolgen

Im Rahmen dieser Prüfung hat die EFK zwei bereits abgeschlossene Fälle untersucht. Beim ersten handelte es sich um einen BV-internen Fall, beim zweiten ging es um einen externen LE, der von einem Cybervorfall betroffen war. Von der Entdeckung des Vorfalls bis zur Meldung an das NCSC dauerte es im ersten Fall 13 und im zweiten 11 Tage. Beim ersten Fall ging die VE davon aus, dass nur ihr Netz betroffen sei. Später stellte sich jedoch heraus, dass auch ein externer LE betroffen war. Im zweiten Fall wurde die Meldung vom externen LE informell direkt ans NCSC gemeldet. Die VE führte in dieser Zeit die internen Untersuchungen durch und informierte das NCSC erst danach.



Grafik 2: Zeitverlauf Meldung Cybervorfälle (Darstellung EFK)

Beurteilung

Die Bearbeitung eines Cybervorfalls kann eine gewisse Zeit in Anspruch nehmen. Es ist jedoch wichtig, dass ein Vorfall sofort nach Entdeckung dem NCSC gemeldet wird, damit eine übergeordnete Analyse und Einschätzung der Gefahr gemacht werden kann. Danach kann abgeschätzt werden, ob es eine übergeordnete Koordination braucht, oder die VE den Vorfall selber bearbeiten und bewältigen kann, um die Gefahr einer lateralen Ausbreitung in der gesamten BV zu verhindern oder einzudämmen.

In beiden Fällen kommt die EFK zum Schluss, dass die Meldezeiten zu lange dauerten und entsprechend gekürzt werden müssen. Zudem wurde im zweiten Fall das NCSC zuerst informell durch den externen LE und erst danach durch die VE informiert. Die Durchlaufzeiten zwischen Entdeckung, Kommunikation und Beginn der Störungsbehebung müssen verbessert werden.

Empfehlung 1 (Priorität 1)

Die EFK empfiehlt dem NCSC, die Verwaltungseinheiten bezüglich der Meldepflicht von Cybervorfällen zu sensibilisieren und die Abläufe und Pflichten stufengerecht aufzubereiten.

Die Empfehlung ist akzeptiert.

Stellungnahme des NCSC

Das NCSC akzeptiert diese Empfehlung. Das NCSC wird die Wirkung einer zeitnahen Meldung bei den Sensibilisierungsmassnahmen entsprechend berücksichtigen und die Optimierung der Abläufe sowie Pflichten im kontinuierlichen Verbesserungsprozess zur Meldepflicht von Cybervorfällen gebührend beachten.

2.3 Die Kommunikationswege müssen verbessert werden

Grundsätzlich sind die Abläufe und Kommunikationswege sowohl im Prozess wie auch in der CyRV definiert. Diese müssen jedoch noch optimiert werden. Im Prozess erfolgt die Meldung an die Informatiksicherheitsbeauftragten der Organisationseinheit (ISBO) respektive die ISBD relativ spät (siehe Grafik 1: Prozess zur Bewältigung von Cybervorfällen (Darstellung EFK). So ist diese Meldung erst nach dem Abschluss des Cybervorfalls vorgesehen. Ausserdem erfolgt sie gemäss Prozess erneut nur vom LE an den LB, jedoch nicht vom LB an die ISBO oder ISBD der LE.

Generell besteht eine gute Zusammenarbeit der verschiedenen grösseren Organisationen, weil sich die Leute kennen und in regelmässigem persönlichem Kontakt stehen. Dies ist aber bei kleineren VE nicht der Fall. Gerade diese kleineren VE sind aber auf eine rasche Reaktion und Hilfestellung des NCSC angewiesen. Hier ist der unverzügliche Informationsfluss zum NCSC gefährdet.

Die Schnittstellen sind definiert, dennoch müssen einige noch optimiert werden. Die horizontale Steuerung, d. h. der Informationsaustausch zwischen den LE ist noch nicht überall sichergestellt.

Beurteilung

Der Meldefluss im Prozess muss verbessert und systematisiert werden. Die Information der ISBO oder ISBD der LE sollte unverzüglich geschehen. Dies umso mehr, wenn ein Vorfall die gesamte BV betreffen könnte und die Leitung der VE oder gegebenenfalls der Bundesrat

informiert werden muss. Dies sollte durch den eigenen ISBO respektive ISBD geschehen und nicht über Dritte.

Empfehlung 2 (Priorität 1)

Die EFK empfiehlt dem NCSC, den Meldefluss (Information) an die ISBO bzw. ISBD anzupassen, damit die Informationen rascher an die Informatiksicherheitsbeauftragten gelangen. Dabei sollen auch Verantwortlichkeiten für die Kommunikation bei einem VE-übergreifenden Vorfall definiert werden.

Die Empfehlung ist akzeptiert.

Stellungnahme des NCSC

Das NCSC akzeptiert diese Empfehlung. Der Meldefluss soll dahingehend verbessert werden, damit die Sicherheitsverantwortlichen zeitnah über die sie betreffende, aber auch über relevante VE-übergreifende Sicherheitsvorfälle informiert werden.

3 Externe Partner sind nur schwer zu kontrollieren

3.1 Eine Meldepflicht ist erst in neuen Verträgen vorgesehen

Einer der analysierten Cybervorfälle betraf einen externen Dienstleister der BV. Die EFK stellte fest, dass in den Verträgen keine Meldepflicht für solche Vorfälle vereinbart war. Dies ist umso kritischer da dieser LE Software für den Betrieb von kritischer Infrastruktur programmierte. Der externe LE hat den Vorfall jedoch proaktiv dem LB gemeldet. Zudem erfolgte auch eine direkte informelle Meldung an das NCSC.

Bei externen LE kann nicht sichergestellt werden, dass ein Sicherheitsvorfall beim Dienstleister den LB gemeldet wird. Gemäss CyRV[4] sind die VE aber verpflichtet, beim Bezug von Leistungen eines externen LE die Informatiksicherheitsvorgaben als Teil des Vertrags aufzunehmen. Dafür hat die Beschaffungskonferenz des Bundes (BKB) im September 2020 die «Mustervertragsklausel der BKB betreffend Cyberrisiken[5]» erstellt. Diese wird auf der Homepage bei den allgemeinen Geschäftsbedingungen des Bundes zur Verfügung gestellt. Dort ist unter anderem auch ein Auditrecht sowie die Meldepflicht bei Vorfällen niedergeschrieben. Bei allen älteren Verträgen ist das Thema nicht systematisch adressiert. Zudem ist nicht geregelt, ob und wie externe LE das NCSC informieren sollen.

Im untersuchten Fall mit dem externen LE wurde der Cybervorfall bei der zuständigen Kantonspolizei (KaPo) zur Anzeige gebracht. In einer solchen Situation hat das NCSC keine Möglichkeiten, weitere Informationen zu erhalten oder sich zum Vorgehen auszutauschen. Wenn der externe LE nicht bereit ist, die Ergebnisse der Untersuchungen der KaPo mit seinem LB respektive dem NCSC zu teilen, bleibt unklar, ob und welche weiteren Schritte unternommen wurden.

Beurteilung

Die neu bereitgestellten Vertragsklauseln zur Cybersicherheit gehen in die richtige Richtung. Die Fristen zur Meldung von Cybervorfällen sind jedoch nicht einheitlich vorgegeben und müssen in jedem Vertrag einzeln definiert werden. Es ist fraglich, ob bei den LB das Wissen vorhanden ist, um solche Fristen praxistauglich festzulegen. Ausserdem müssten diese Vertragsklauseln auch bei langjährigen Verträgen nachverhandelt werden.

Eine Meldung des externen LE parallel direkt ans NCSC würde einen unnötigen Zwischenschritt und Verzögerungen im Meldeprozess vermeiden. Es sollte eine Möglichkeit geschaffen werden, damit die externen LE Cybervorfälle direkt ans NCSC melden müssen.

Das NCSC hat zum Prüfungszeitpunkt die Vernehmlassung zur Einführung einer Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen eröffnet. Eine solche würde in das Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG)[6] integriert. Dort würde in Art. 74b, lit. s der beschriebene Fall abgedeckt. Eine solche

[4] Art. 14, Ziff. 3 lit. d, CyRV

[5] https://www.bkb.admin.ch/dam/bkb/de/dokumente/Oeffentliches_Beschaffungswesen/Mustervertragsklausel_Cybersecurity_20200901_d.pdf.download.pdf/Mustervertragsklausel_Cybersecurity_20200901_d.pdf

[6] https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-86768.html#:~:text=Vernehmlassung%20zur%20Einf%C3%BChrung%20einer%20Meldepflicht%20f%C3%BCr%20Cyberangriffe%20er%C3%B6ffnet,-Der%20Bundesrat&text=Bern%2C%2012.01.2022%20%2D%20An,Cyberangriffe%20bei%20kritischen%20Infrastrukturen%20er%C3%B6ffnet.

Meldepflicht würde dem NCSC einen besseren Überblick über Cybervorfälle ermöglichen und seine Handlungsfähigkeit verbessern.

Aus Sicht der EFK wäre es sinnvoll, mit dem externen LE vertraglich festzulegen, dass Ergebnisse aus polizeilichen Untersuchungen – soweit diese dem externen LE überhaupt bekannt werden – dem NCSC mitgeteilt werden müssen.

Empfehlung 3 (Priorität 1)

Die EFK empfiehlt dem NCSC, in Zusammenarbeit mit dem Bundesamt für Bauten und Logistik, die Mustervertragsklausel der BKB genau zu analysieren und bei Bedarf der BKB entsprechende Änderungen vorzuschlagen. Zudem sollte definiert werden, unter welchen Bedingungen eine Meldepflicht von Cybervorfällen bei langjährigen Verträgen nachverhandelt werden muss.

Die Empfehlung ist akzeptiert.

Stellungnahme des NCSC

Das NCSC unterstützt diese Empfehlung und wird in Zusammenarbeit mit dem BBL das Optimierungspotential an den Vorlagen vor allem aus den gewonnen Erkenntnissen analysieren, die Rahmenbedingungen für Nachverhandlungen prüfen und Änderungen vorschlagen.

3.2 Eine Übersicht der externen Dienstleister ist nicht vorhanden

Im Rahmen der Prüfung konstatierte die EFK, dass innerhalb der VE nur mit grossem Aufwand festgestellt werden kann, welche externen LE vorhanden sind. Eine BV-weite Übersicht aller externen LE fehlt gänzlich. Auf der Ebene der Departemente ist es umso schwieriger festzustellen, welche VE durch einen externen LE bedient werden. Wenn ein externer LE von einem Cybervorfall betroffen ist, kann nicht innerhalb nützlicher Frist erhoben werden, welche weiteren VE, Applikationen und Services potenziell betroffen sind.

Zusätzlich ist für die LE des Bundes nicht ersichtlich, ob einer ihrer LB noch weitere externe LE hat, welche einen Einfluss auf die IT-Sicherheit haben könnten.

Das Schwachstellenmanagement kann nicht gezielt informieren

Das NCSC hat ein Team aufgebaut, welches sich mit der Entdeckung von Schwachstellen befasst. Wenn eine Schwachstelle entdeckt wurde, melden sie dies den VE weiter. Dies wird sehr geschätzt. Da aber nicht bekannt ist wer die verwundbaren Systeme im Einsatz hat, wird die Information an alle VE weitergeleitet, sodass viel Zeit in die Abklärungen gesteckt werden muss, ob die VE überhaupt von der Schwachstelle betroffen ist.

Beurteilung

Im Falle eines Cybervorfalls geht viel wertvolle Zeit verloren, um herauszufinden, wer davon überhaupt betroffen ist. Eine BV-übergreifende Übersicht der externen Dienstleister existiert nicht, was die Information und Bewältigung erschwert. Ausserdem gibt es auch keine zentrale Übersicht, welche Applikationen und Services von welchen Lieferanten betreut werden. Somit können bei einer Meldung eines Cybervorfalls nicht alle betroffenen VE umgehend informiert werden, was die Verwundbarkeit der BV erhöht. Ein übergreifendes Inventar aller externen LE könnte hier Abhilfe schaffen und dem Schwachstellenmanagement helfen, Informationen zielgerichteter weiterzuleiten. Basis könnte z. B. das IKT-Cockpit oder das Vertragsmanagement des Bundes sein.

Empfehlung 4 (Priorität 1)

Die EFK empfiehlt dem NCSC zusammen mit den Departementen und der BK, die Führung einer bundesweiten Übersicht der externen IT-Leistungserbringer zu prüfen und die angebotenen Dienstleistungen und Services zu erheben.

Die Empfehlung ist akzeptiert.

Stellungnahme des NCSC

Das NCSC unterstützt diese Empfehlung auch im Sinne einer aktuellen Inventarführung der Informatikschutzobjekte durch die Verwaltungseinheiten gemäss CyRV Art. 14 Abs. 3 Bst. a. In Zusammenarbeit mit den Departementen und der BK werden die vorhandenen Informationen zur Führung einer bundesweiten Übersicht von externen IT-Leistungserbringern sowie deren Dienstleistungen so weit möglich geprüft.

3.3 Fehlende Abschlussmeldungen nähren die Unsicherheit

Beim überprüften externen LE konnte der Vorfall ohne Folgen für die BV erfolgreich abgeschlossen werden. Es erfolgte jedoch keine Rückmeldung seitens NCSC an die betroffenen LB und die anderen betroffenen LE. Entsprechend blieb ungeklärt, ob der Vorfall sachgerecht abgeschlossen wurde und es blieb ein gewisser Reputationsschaden hinsichtlich des externen LE bestehen. Dieser hat sich daraufhin entschlossen, sich durch einen externen Dienstleister überprüfen zu lassen und den Bericht dem NCSC abzugeben. Dieser Bericht wurde jedoch vom NCSC nicht an die VE weitergeleitet.

Beurteilung

Nach Abschluss eines schwerwiegenden Cybervorfalls bei einem externen LE sollte eine unabhängige Überprüfung möglich sein. Entsprechende Berichte sollten danach den betroffenen LE und LB zur Verfügung gestellt werden. Somit können die anderen LE und LB sicher sein, dass der Vorfall abgeschlossen und sachgerecht reagiert worden ist. Zudem wird dadurch der Reputationsschaden für den externen LE kleiner, was zu einer tieferen Hemmschwelle bezüglich der rechtzeitigen Meldung eines Vorfalls beitragen sollte. Ein analoges Vorgehen wäre auch bei internen LE sinnvoll.

Empfehlung 5 (Priorität 2)

Die EFK empfiehlt dem NCSC, nach erfolgter Vorfallbewältigung, die Abschlussmeldung zusammen mit einen allfälligen externen Auditbericht an die involvierten Stellen weiterzuleiten.

Die Empfehlung ist akzeptiert.

Stellungnahme des NCSC

Das NCSC akzeptiert diese Empfehlung. Die Abschlussmeldung sowie deren begleitenden Sicherheitsmassnahmen werden bei der Optimierung des Vorfallbewältigungsprozesses entsprechend berücksichtigt.

4 Organisation und Überwachung

4.1 Werkzeuge können effizienter eingesetzt werden

Das NCSC betreibt das Computer Emergency Response Team (GovCERT). Dieses ist die nationale Fachstelle für die technische Vorfallbewältigung, die Analyse technischer Fragestellungen, die Einschätzungen der Bedrohungslage(n) aus technischer Sicht und die technische Unterstützung der nationalen Anlaufstelle. Die Kommunikation und die Meldungen an das NCSC und ans GovCERT erfolgen per E-Mail. Sollte eine Reaktion nicht zeitnah erfolgen, wird das NCSC in der Regel telefonisch kontaktiert. Die weitere Kommunikation findet danach über eine gesicherte Plattform mittels einer Chatfunktion statt. Auf dieser werden nicht nur die Informationen ausgetauscht, sondern auch gleich die Vorfälle archiviert. Auf der Plattform können verschiedene, voneinander unabhängige Gruppen erstellt werden. Somit können bei Bedarf weitere Akteure zur Bewältigung des Vorfalls hinzugezogen werden.

Die verschiedenen Security Operations Center (SOC), Cyber Fusion Center (CFC), Computer Security Incident Response Team (CSIRT) und CERT arbeiten mit unterschiedlichen Werkzeugen. Dies hat damit zu tun, dass Informationen betreffend Cybervorfällen nicht für die Öffentlichkeit bestimmt sind und somit geschützt werden müssen. Der Zugriff auf die Informationen und Werkzeuge sollte entsprechend klein gehalten werden. Eine durchgängige Digitalisierung ist folglich nicht gegeben. Die verschiedenen LE bearbeiten die Vorfälle mit den Werkzeugen und Ticketingsystemen ihrer VE und benutzen den Chat des GovCERT, um übergreifende Informationen zu teilen.

Anders sieht es bei den Überwachungswerkzeugen aus. Hier benutzen viele VE dieselben oder ähnliche Anwendungen. Da jede VE ihre Werkzeuge selber beschafft, gibt es mehrere Verträge mit denselben Lieferanten.

Beurteilung

Ideal wäre ein Werkzeug, in welchem alle Cybervorfälle BV-weit abgearbeitet werden könnten. Herausfordernd ist sicherzustellen, dass nur diejenigen Personen auf geschützte Daten Zugriff haben, die sie benötigen. Zudem müssen redundante Meldekanäle bereitgestellt werden. Zum Prüfzeitpunkt ist das NCSC in der Evaluation eines neuen Werkzeuges, in welchem die Vorfälle künftig abgearbeitet werden können.

Bei den Überwachungswerkzeugen wäre eine Harmonisierung auf Stufe BV sinnvoll. Durch eine zentrale Beschaffung kann sichergestellt werden, dass nicht unterschiedliche Werkzeuge mit denselben oder ähnlichen Funktionalitäten eingesetzt werden. Damit werden Skaleneffekte hinsichtlich der Kosten und des Know-how-Aufbaus möglich.

Empfehlung 6 (Priorität 1)

Die EFK empfiehlt dem NCSC in Zusammenarbeit mit der BK und dem BBL, eine Harmonisierung der Überwachungswerkzeuge innerhalb der BV zu prüfen und allfällige Synergien bei der Beschaffung und Ausbildung zu nutzen.

Die Empfehlung ist akzeptiert.

Stellungnahme des NCSC

Das NCSC unterstützt die Empfehlung. In Zusammenarbeit mit der Bundeskanzlei und dem BBL wird im Sinne der Nutzung von Synergiepotentialen eine Harmonisierung der Überwachungswerkzeuge geprüft.

4.2 Die Organisation der Detektion von Vorfällen ist zielführend

In der Vergangenheit wurden in der BV verschiedene Sicherheitsorganisationen (siehe Kapitel 4.1) aufgebaut und erweitert, sodass die Entdeckungsrate von Cybervorfällen verbessert werden konnte. Zudem wurde die Detektionsfähigkeit durch Überwachungswerkzeuge ausgebaut. Des Weiteren findet ein regelmässiger Austausch der oben erwähnten Teams statt.

Die LB befinden sich je nach Grösse auf unterschiedlichen Maturitätsstufen. Bei kleineren VE ist die Rolle des ISBO zum Teil nur mit wenigen Stellenprozenten besetzt und eine Stellvertretung fehlt. Angesichtes dessen kann ein Cybervorfall bei Abwesenheit des ISBO nicht zeitgerecht bearbeitet werden, eine Meldung an den ISBD und das NCSC erfolgt ebenso verspätet.

Beurteilung

Die aktuelle gute Zusammenarbeit der verschiedenen Akteure ist eine Grundvoraussetzung, um die Sicherheit auf einem hohen Stand zu halten.

Die Rolle des ISBO wird in der ISV geschärft und es wird eine Stellvertreter-Regelung gefordert. Da die ISV noch nicht in Kraft ist, sollte dies bereits jetzt geregelt werden.

Empfehlung 7 (Priorität 1)

Die EFK empfiehlt dem NCSC, die explizite Benennung der Stellvertretung des ISBO von den Departementen einzufordern.

Die Empfehlung ist akzeptiert.

Stellungnahme des NCSC

Das NCSC akzeptiert die Empfehlung. Die explizite Benennung der Stellvertretung der ISBOs wird geprüft und falls nötig bei den Departementen eingefordert.

Anhang 1: Rechtsgrundlagen

Rechtstexte
Bundesgesetz über die Eidgenössische Finanzkontrolle (Finanzkontrollgesetz, FKG) vom 28. Juni 1967 (Stand am 1. Januar 2021), SR 614.0
Bundesgesetz über den Datenschutz vom 19. Juni 1992 (Stand am 1. März 2019), SR 235.1
Verordnung zum Bundesgesetz über den Datenschutz (VDSG) vom 14. Juni 1993 (Stand am 16. Oktober 2012), SR 235.11
Verordnung über den Schutz von Informationen des Bundes (Informationsschutzverordnung, ISchV) vom 4. Juli 2007 (Stand am 1. Januar 2021), SR 510.411
Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, CyRV) vom 27. Mai 2020 (Stand am 1. April 2021), SR 120.73
Verordnungen / Strategien
V001 – Verordnung über die digitale Transformation und die Informatik vom 25. November 2020
SN002 – Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) 2018–2022 vom 18.4.2018[7]
Dokumente
Prozess zur Bewältigung von Cybervorfällen (https://intranet.ncsc.admin.ch/ncscintra/de/home/dokumentation/dokumente-partner/bundesverwaltung.html)
Mustervertragsklausel der BKB betreffend Cyberrisiken (https://www.bkb.admin.ch/bkb/de/home/themen/cyberrisiken.html)

[7] https://www.ncsc.admin.ch/ncsc/de/home/strategie.html

Anhang 2: Abkürzungen

AGB	Allgemeine Geschäftsbedingungen (des Bundes)
AI-S	Ausschuss Informatiksicherheit (siehe Glossar)
BKB	Beschaffungskonferenz des Bundes
BR	Bundesrat
BV	Bundesverwaltung
CERT (GovCERT)	Computer Emergency Response Team (siehe Glossar)
CFC	Cyber Fusion Center (siehe Glossar)
CSIRT	Computer Security Incident Response Team (siehe Glossar)
EFK	Eidgenössische Finanzkontrolle
Fedpol	Bundesamt für Polizei
ISBD	Informatiksicherheitsbeauftragte der Departemente
ISBO	Informatiksicherheitsbeauftragte der Organisationseinheit
ISG	Informationssicherheitsgesetz
ISV	Informationssicherheitsverordnung
IT	Informationstechnologie
IKT	Informations- und Kommunikationstechnologie
KaPo	Kantonspolizei
LB	Leistungsbezüger
LE	Leistungserbringer
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken
NCSC	Nationales Zentrum für Cybersicherheit
SOC	Security Operations Center (siehe Glossar)
VE	Verwaltungseinheit

Anhang 3: Glossar

Ausschuss Informatiksicherheit	Der Ausschuss Informatiksicherheit (A-IS) fungiert als Konsultativorgan für das NCSC betreffend Informatiksicherheitsfragen in der Bundesverwaltung (Art. 10 Abs. 4 CyRV). Er nimmt Stellung zu informatiksicherheitsrelevanten Entwürfen für Informatik-Beschlüsse Bund des NCSC. Er kann zu weiteren Informatikgeschäften, die der Absprache zwischen den Departementen und der Bundeskanzlei bedürfen, Stellung nehmen. Der A-IS setzt sich aus einer Vertreterin oder einem Vertreter des Nationalen Zentrums für Cybersicherheit (NCSC), den Informatiksicherheitsbeauftragten der Departemente und der Bundeskanzlei sowie der oder dem Informatiksicherheitsbeauftragten der Standarddienste der Informations- und Kommunikationstechnik (IKT) zusammen. Die Vertreterin oder der Vertreter des NCSC hat den Vorsitz. (Quelle NCSC)
Computer Emergency Response Team	Ein CERT ist eine Gruppe von Informationssicherheitsexperten, die für den Schutz vor, die Erkennung von und die Reaktion auf Cybersecurity-Vorfälle einer Organisation verantwortlich sind.[8]
Computer Security Incident Response Team	Ein Computer Security Incident Response Team, oder abgekürzt CSIRT, ist eine Organisation, die Informationen über Sicherheitsvorfälle sammelt, Analysen durchführt und auf Anfragen reagiert. Grundsätzlich sind CERT und CSIRT ähnlich aufgestellt.
Cyber Fusion Center	Ein Cyber Fusion Center bringt die SOC-Strategie voran. Es verkörpert das SOC, aber auch die physische Sicherheit, das Anti-Fraud-Management, den IT-Betrieb und andere Funktionen.[9]
Security Operations Center	Das Security Operations Center überwacht die IT-Infrastruktur rund um die Uhr gegen Cyberbedrohungen. Durch die permanente Überwachung sowie präventive Massnahmen gegen Cyberbedrohungen garantiert das SOC die Verfügbarkeit und Sicherheit des Firmennetzwerkes, inklusive der geschäftskritischen Applikationen.

[8] Quelle: https://whatis.techtarget.com/de/definition/Computer-Security-Incident-Response-Team-CSIRT (Stand 15.04.2022)

[9] Quelle: https://www.infopoint-security.de/it-security-im-wandel-vom-security-operations-center-zum-cyber-fusion-center/a27334/#:~:text=Ein%20Cyber%20Fusion%20Center%20bringt,September. (Stand 15.04.2022)

Priorisierung der Empfehlungen

Die Eidg. Finanzkontrolle priorisiert die Empfehlungen nach den zugrunde liegenden 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).