Contact Committee

Kontaktausschuss

der Obersten Rechnungskontrollbehörden der EU

Prüfungskompendium

Cybersicherheit in der EU und ihren Mitgliedstaaten

Prüfung der Widerstandsfähigkeit kritischer Informationssysteme und digitaler Infrastrukturen gegenüber Cyberangriffen

Im Zeitraum 2014-2020 veröffentlichte Prüfungsberichte

DE

Dezember 2020

Der Kontaktausschuss der Obersten Rechnungskontrollbehörden (ORKB) der Europäischen Union (EU) bietet ein Forum, in dem Themen im Zusammenhang mit der öffentlichen Finanzkontrolle in der EU diskutiert und angegangen werden können. Durch die Stärkung des Dialogs und der Zusammenarbeit zwischen seinen Mitgliedern leistet der Ausschuss einen Beitrag zu einer wirksameren externen Prüfung von staatlichen Maßnahmen und Programmen der EU. Dies trägt auch dazu bei, zum Nutzen aller Bürgerinnen und Bürger der EU die Rechenschaftspflicht zu stärken, die Haushalts- und Wirtschaftsführung der EU zu verbessern und eine verantwortungsvolle Staatsführung zu festigen.

Kontakt: www.contactcommittee.eu

Inhalt

Inhalt

Vorwort

Liebe Leserin, lieber Leser!

Durch die Digitalisierung und den zunehmenden Einsatz von Informationstechnologie in allen Bereichen unseres Alltags eröffnet sich eine Fülle neuer Möglichkeiten. Gleichzeitig steigt das Risiko für Privatpersonen, Unternehmen und öffentliche Stellen, Opfer von Cyberkriminalität und Cyberangriffen zu werden. Auch die damit einhergehenden gesellschaftlichen und wirtschaftlichen Folgen nehmen zu.

In der EU fällt die Cybersicherheit in den Zuständigkeitsbereich der Mitgliedstaaten. Die EU spielt eine wichtige Rolle beim Aufbau eines gemeinsamen Regelungsrahmens innerhalb des EU-Binnenmarkts und bei der Schaffung von Bedingungen, unter denen die Mitgliedstaaten vertrauensvoll zusammenarbeiten können.

Cybersicherheit und digitale Autonomie haben sich für die EU und ihre Mitgliedstaaten zu Themen von strategischer Bedeutung entwickelt. In allen Mitgliedstaaten bestehen im öffentlichen wie im privaten Sektor weiterhin Schwachstellen im Bereich der Cybersicherheits-Governance, die allerdings unterschiedlich ausgeprägt sind. Dies schränkt unsere Möglichkeiten ein, Cyberangriffen vorzubeugen und gegebenenfalls darauf zu reagieren. Die Verbreitung von Desinformationen, oftmals von außerhalb der EU, nimmt zu, was sich während der diesjährigen COVID-19-Pandemie erneut gezeigt hat. Dies stellt eine Bedrohung für den sozialen Zusammenhalt in unseren Gesellschaften und das Vertrauen der Bürgerinnen und Bürger in unsere Demokratien dar, die nicht ignoriert werden darf.

Eine Umfrage unter den Obersten Rechnungskontrollbehörden (ORKB) der EU im Jahr 2018 ergab, dass rund die Hälfte von ihnen noch keine Prüfung zum Thema Cybersicherheit durchgeführt hatte. Seitdem haben unsere ORKB ihre Prüfungsarbeit verstärkt auf die Cybersicherheit ausgerichtet und dabei besonders den Datenschutz, die Abwehr von Cyberangriffen und den Schutz kritischer öffentlicher Versorgungssysteme in den Blick genommen. Da sich manche dieser Prüfungen unter Umständen auf sensible Informationen (aus dem Bereich der nationalen Sicherheit) erstrecken, können verständlicherweise nicht alle veröffentlicht werden.

Die COVID-19-Krise hat das wirtschaftliche und soziale Gefüge unserer Gesellschaften in diesem Jahr auf den Prüfstand gestellt. Angesichts unserer Abhängigkeit von der Informationstechnologie könnten Cyberkrisen in Zukunft durchaus pandemieartige Ausmaße annehmen. Wir müssen darauf vorbereitet sein und die Widerstandsfähigkeit kritischer Informationssysteme und digitaler Infrastrukturen gegenüber Cyberangriffen stärken.

Wir hoffen, dass der Überblick, den dieses Kompendium bietet, das Interesse der öffentlichen Prüfer in der gesamten Union an diesem kritischen Bereich weiter stärkt.

Klaus-Heiner Lehne

Präsident des Europäischen Rechnungshofs
Vorsitzender des Kontaktausschusses
und Leiter des Projekts

Zusammenfassung

I Cybersicherheit und digitale Autonomie haben sich für **die EU und ihre Mitgliedstaaten zu Themen von strategischer Bedeutung entwickelt**. Da die Bedrohung zunimmt, müssen die Anstrengungen zum Schutz unserer kritischen Informationssysteme und digitalen Infrastrukturen gegen Cyberangriffe intensiviert werden. Cybersicherheit betrifft nicht nur unsere Versorgungs-, Verteidigungs- und Gesundheitssysteme, sondern auch den Schutz der personenbezogenen Daten, der Geschäftsmodelle und des geistigen Eigentums. Letztendlich geht es bei Cybersicherheit darum, unsere demokratischen Gesellschaften, unsere Unabhängigkeit als Europäer und unsere Art des Zusammenlebens zu schützen.

II Im ersten Teil des nunmehr vorliegenden dritten Kompendiums des Kontaktausschusses wird dargelegt, **was Cybersicherheit bedeutet**. Es wird ausgeführt, inwiefern Cybersicherheit eine Herausforderung für die öffentliche Verwaltung, Unternehmen und Privatpersonen darstellt. Ferner wird das neue Phänomen der Desinformation beleuchtet, das den sozialen Zusammenhalt in unseren Gesellschaften und demokratischen Systemen zunehmend bedroht. Darüber hinaus werden die Befugnisse und Akteure der EU, ihre Strategie und Gesetzgebung im Bereich der Cybersicherheit sowie die verfügbaren EU-Mittel erläutert.

III Der zweite Teil des Kompendiums enthält eine Zusammenfassung der **Ergebnisse ausgewählter Prüfungen der Obersten Rechnungskontrollbehörden (ORKB) der zwölf an dieser Publikation beteiligten Mitgliedstaaten und des Europäischen Rechnungshofs**, die zwischen 2014 und 2020 veröffentlicht wurden. Bei diesen Prüfungen wurden wichtige Aspekte der Cybersicherheit behandelt, wie der Schutz personenbezogener Daten, die Integrität nationaler Rechenzentren, die Sicherheit der öffentlichen Versorgungssysteme sowie die Umsetzung nationaler Cybersicherheitsstrategien im weiteren Sinne.

IV Der dritte Teil enthält **detaillierte Informationen zu den ausgewählten Prüfungen** sowie eine Zusammenfassung der sonstigen Prüfungen zum Thema Cybersicherheit, die von den ORKB veröffentlicht wurden.

TEIL I – Cybersicherheit im europäischen Kontext

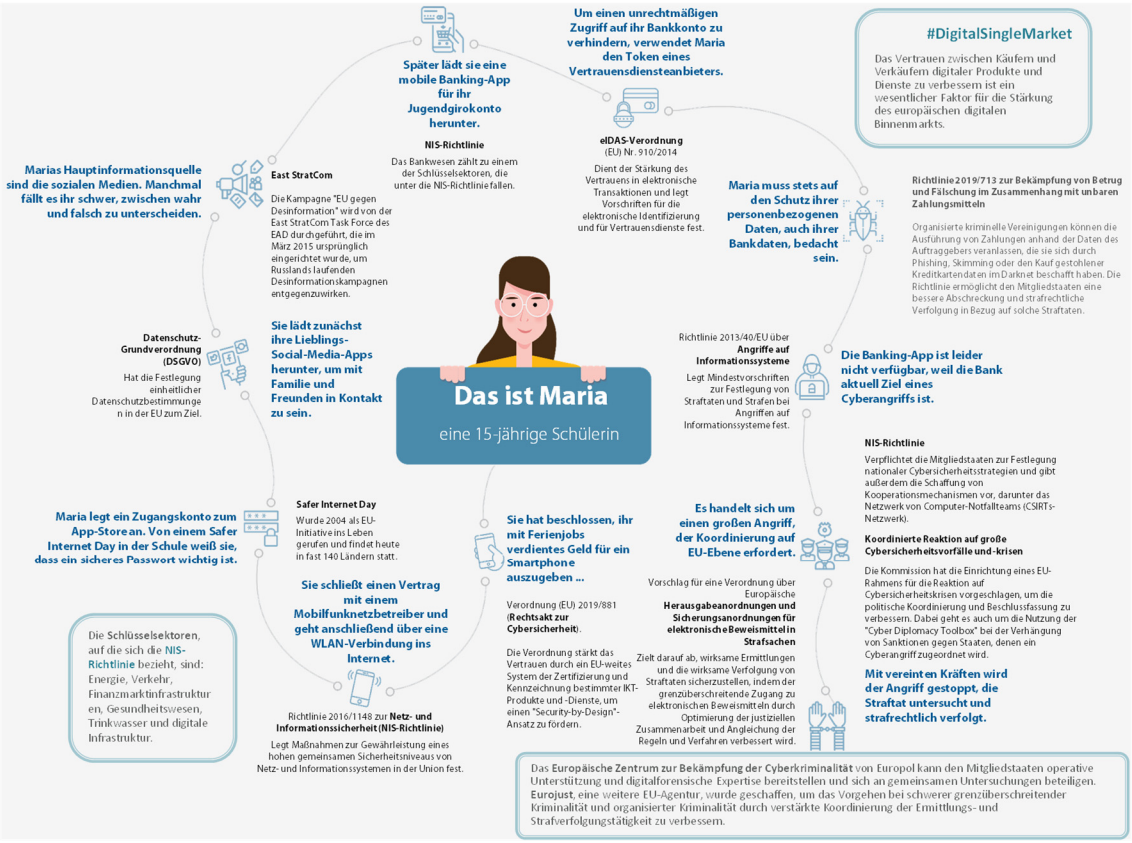
Was ist Cybersicherheit?

1 Es gibt keine einheitliche allgemein anerkannte **Definition von Cybersicherheit**. In diesem Dokument bezieht sich Cybersicherheit auf **Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen**. Dazu gehört es, Cybervorfälle zu verhüten, aufzudecken, darauf zu reagieren und etwaige Folgen zu beseitigen. Diese Vorfälle können vorsätzlich oder unbeabsichtigt herbeigeführt werden und reichen von der versehentlichen Preisgabe von Informationen bis hin zu Angriffen auf Unternehmen und kritische Infrastrukturen, zum Diebstahl personenbezogener Daten und sogar zu einer Störung demokratischer Prozesse, einschließlich der Einflussnahme auf Wahlen, sowie zu allgemeinen Desinformationskampagnen zur Beeinflussung öffentlicher Debatten.

Cybersicherheit wirkt sich auf den Alltag aller Bürgerinnen und Bürger der EU aus

2 Cybersicherheit wirkt sich auf unser aller Alltag aus, wann immer wir IT-Geräte wie Smartphones, WLAN-Netze, soziale Medien oder elektronische Bankdienstleistungen nutzen. Im Jahr 2020 ist die Frage nicht mehr, ob, sondern wie und wann Cyberangriffe stattfinden werden. Betroffen sind wir alle: **Privatpersonen, Unternehmen und die öffentliche Verwaltung**. In ***Bild 1*** wird veranschaulicht, wie die EU Cybersicherheit fördert und welchen Rahmen sie geschaffen hat, um die Bürgerinnen und Bürger bei ihren elektronischen Aktivitäten im Alltag vor Cyberangriffen zu schützen. Der Schutz kritischer Informationssysteme und digitaler Infrastrukturen vor Cyberangriffen hat sich zu einer strategischen Herausforderung entwickelt.

Bild 1 – Die EU fördert Cybersicherheit im Alltag ihrer Bürgerinnen und Bürger



Quelle: Europäischer Rechnungshof, Bildsymbole von Pixel perfect auf der Plattform www.flaticon.com.

Es gibt zahlreiche Arten von Cyberbedrohungen

3 Die zahlreichen Arten von Bedrohungen im Bereich der Cybersicherheit, denen unsere Gesellschaften ausgesetzt sind, lassen sich nach **ihren Auswirkungen auf die Daten – Preisgabe, Veränderung, Zerstörung oder Zugriffsverweigerung** – oder den verletzten zentralen Grundsätzen der Informationssicherheit einteilen (siehe ***Abbildung 1***).

Abbildung 1 – Arten von Bedrohungen und welche Grundsätze der Informationssicherheit sie gefährden

Vorhängeschloss = Sicherheit ist gewährleistet; Ausrufezeichen = Sicherheit ist gefährdet

Quelle: Europäischer Rechnungshof auf der Grundlage einer Studie des Europäischen Parlaments[1].

4 Mit jedem Gerät, das online genutzt wird oder das sich mit anderen Geräten verbindet, vergrößert sich, die sogenannte „Angriffsfläche“ im Bereich Cybersicherheit . Das exponentielle Wachstum beim "Internet der Dinge"(*Internet of Things*, IoT), bei Clouds, Big Data und der Digitalisierung der Industrie geht einher mit einer größeren Anfälligkeit, sodass Angreifer immer mehr Opfer ins Visier nehmen können. Aufgrund der Vielzahl der Angriffsarten und ihrer zunehmende Komplexität ist es schwierig, mit dieser Entwicklung Schritt zu halten[2]. In ***Kasten 1*** werden beispielhaft **mögliche Cyberangriffe** beschrieben.

---

[1] Europäisches Parlament, *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses*, Studie im Auftrag des LIBE-Ausschusses des Europäischen Parlaments, September 2015.

[2] ENISA, *ENISA Threat Landscape Report 2017*, 18. Januar 2018.

Kasten 1

Arten von Cyberangriffen

Malware (Schadsoftware) soll Geräte oder Netze beschädigen. Malware ist ein Sammelbegriff für Viren, Trojaner, Ransomware, Würmer, Adware und Spyware (z. B. NotPetya).

Ransomware verschlüsselt Daten, sodass die Nutzer auf ihre Dateien erst wieder Zugriff haben, nachdem sie Lösegeld (in der Regel in einer Kryptowährung) gezahlt haben oder eine Aktion ausgeführt wurde. Laut Europol sind Ransomware-Angriffe insgesamt am häufigsten und die Zahl der Ransomware-Varianten ist in den letzten Jahren geradezu explosionsartig gestiegen (z. B. WannaCry[3]).

Distributed-Denial-of-Service- bzw. DDoS-Angriffe, die den Ausfall von Diensten oder Ressourcen herbeiführen, indem sie diese mit Anfragen überlasten, nehmen ebenfalls zu. Ein Drittel der Organisationen hatte im Jahr 2017 mit solchen Angriffen zu tun[4].

Bei **webbasierten Angriffen** handelt es sich um eine beliebte Methode, bei der die Angreifer ihre Opfer dazu verleiten, Websysteme und -dienste zu nutzen, die als Einfallstore dienen. Darunter fällt eine Vielzahl von Angriffsmöglichkeiten. Beispielsweise wird der Nutzer bzw. das Opfer über schädliche URL oder Skripte auf die gewünschte Website weitergeleitet oder lädt schädliche Inhalte herunter (Watering-Hole-Angriffe, Drive-by-Angriffe). Auch können Schadcodes in eine legitime, aber kompromittierte Website **eingeschleust** werden. Auf diese Weise können Informationen gestohlen werden (d. h. Formjacking), um sich finanziell zu bereichern oder einfach selbst an die Informationen zu gelangen[5].

Nutzer können so manipuliert werden, dass sie unwissentlich eine Aktion ausführen oder vertrauliche Informationen preisgeben. Mithilfe dieses Tricks, dem sogenannten **Social Engineering**, kann Datendiebstahl oder Cyberspionage begangen werden. Erreichen lässt sich dies auf unterschiedlichen Wegen, eine gängige Methode ist jedoch das sogenannte **Phishing**. Dabei werden Nutzer durch E-Mails, die aus vertrauenswürdigen Quellen zu stammen scheinen, zur Preisgabe von Informationen oder zum Anklicken von Links verleitet, durch die Geräte mit Schadsoftware infiziert werden. Mehr als die Hälfte der Mitgliedstaaten berichtete über Untersuchungen im Zusammenhang mit Netzwerkangriffen[6].

Die vielleicht folgenschwerste Bedrohungsart sind fortgeschrittene, andauernde Bedrohungen, die sogenannten **Advanced Persistent Threats** (APT). Dahinter stecken raffinierte Angreifer, die langfristig Daten ausspähen, stehlen und manchmal vernichten. Es geht ihnen primär darum, so lange wie möglich unentdeckt zu bleiben. APT sind oftmals staatlich gelenkt und auf besonders

sensible Sektoren wie Technologie, Verteidigung und kritische Infrastrukturen ausgerichtet. Mindestens ein Viertel aller Cybervorfälle soll auf diese Art von **Cyberspionage** zurückzuführen sein[7].

Die wirtschaftlichen Auswirkungen von Cyberangriffen sind erheblich

5 Die Bedrohung durch **Cyberangriffe und Cyberkriminalität** hat sich in den letzten Jahren zu einem ernsthaften Problem entwickelt. Bereits 2016 verzeichneten 80 % der Unternehmen in der EU mindestens einen Cybervorfall[8]. Im Jahr 2018 gaben 40 % der Teilnehmer einer Umfrage unter im Bereich Robotik und Automatisierung tätigen Organisationen an, die Störung ihrer Betriebsabläufe sei die schwerwiegendste Folge eines Cyberangriffs auf ihre Systeme. Obwohl sie sich des Störungspotenzials von Cyberrisiken bewusst sind, verfügen viele Unternehmen über kein System, um damit umzugehen[9].

6 Seitdem sind Anzahl, Schwere und finanzieller Schaden der Cyberangriffe kontinuierlich gestiegen. Soweit sich die **finanziellen Auswirkungen** schätzen lassen, werden der Weltwirtschaft – bei einem geschätzten weltweiten BIP von

---

[3] Die Ransomware *WannaCry* nutzte Schwachstellen in einem Microsoft-Windows-Protokoll, die es möglich machten, Computer aus der Ferne zu übernehmen. Nachdem Microsoft die Sicherheitslücke erkannt hatte, stellte es einen Patch bereit. Hundertausende Computer waren jedoch nicht aktualisiert worden, und viele davon wurden später infiziert. *Quelle*: Greenberg, A., *Hold North Korea Accountable for WannaCry – and the NSA, too*, WIRED, 19. Dezember 2017.

[4] Europol, *Internet Organised Crime Threat Assessment 2018*.

[5] ENISA, *ENISA Threat Landscape 2020 – Web-based attacks*, 20. Oktober 2020.

[6] Europol, ebd., 2018.

[7] European Centre for Political Economy, *Stealing Thunder: Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?*, Occasional Paper 2/18, Februar 2018.

[8] Europol, *Internet Organised Crime Threat Assessment 2017*.

[9] PWC, Global State of Information Security Survey (GSISS), *Strengthening digital society against cyber shocks*, 2017.

138 Billionen US-Dollar im Jahr 2020 – durch Cyberkriminalität **bis 2021 Kosten von 6 Billionen US-Dollar pro Jahr** entstehen. 2015 waren es dagegen noch schätzungsweise 3 Billionen US-Dollar[10]. Die Kosten durch Cyberkriminalität entstehen unter anderem durch die Beschädigung und Vernichtung von Daten, den Diebstahl von Geldmitteln, Produktivitätsverluste, den Diebstahl von geistigem Eigentum, den Diebstahl von personenbezogenen oder Finanzdaten, Störungen des normalen Geschäftsablaufs nach einem Angriff sowie Rufschädigung. Der Europäische Ausschuss für Systemrisiken (ESRB) schätzt, dass die durchschnittlichen Kosten von Cybervorfällen von 2015 bis 2020 um 72 % gestiegen sind[11].

7 Wie eine kürzlich veröffentlichte Studie aus dem Jahr 2020 zeigt, sind **die verschiedenen Wirtschaftsbereiche in unterschiedlichem Maße von Cyberkriminalität betroffen**[12]: Bei Regierung und öffentlicher Verwaltung sowie im Technologie-, Medien- und Telekommunikationssektor war Cyberkriminalität das schwerwiegendste Betrugsphänomen (siehe ***Kasten 2***), im Finanzsektor und in den Sektoren Industrie und verarbeitendes Gewerbe steht sie an zweiter Stelle.

[10] Cybersecurity Ventures, gefördert durch die Herjavec Group, *2019 Official Annual Cybercrime Report*, 2019.

[11] Europäischer Ausschuss für Systemrisiken (ESRB), *Systemic cyber risk*, Februar 2020.

[12] PWC, *Fighting fraud: A never-ending battle – PwC's Global Economic Crime and Fraud Survey*, 2020.

Kasten 2

Finnische Psychotherapiepatienten wurden mit Gesundheitsdaten erpresst, die zwischen 2018 und 2019 gestohlen wurden

Patienten einer großen finnischen psychotherapeutischen Klinik mit Praxen im ganzen Land wurden 2020 einzeln von einem Erpresser kontaktiert, nachdem ihre personenbezogenen Daten im November 2018 und bei einem weiteren potenziellen Vorfall im März 2019 gestohlen worden waren. Darunter waren offenbar Datensätze, die eine Personenidentifikation zulassen sowie Notizen über den Inhalt der therapeutischen Sitzungen.

Der Erpresser forderte sowohl von der Klinik als auch von den Patienten Lösegeld in der Kryptowährung Bitcoin, andernfalls würden die Daten veröffentlicht. Aufgrund des Vorfalls trat die finnische Regierung zu einer Dringlichkeitssitzung zusammen[13].

8 Im Jahr 2019 wies Europol[14] nochmals auf das **hartnäckige Fortbestehen einer Reihe schwerwiegender Cyberbedrohungen** hin:

- Ransomware-Angriffe stellen nach wie vor die größte Bedrohung dar. Sie werden immer zielgerichteter ausgeführt, sind immer einträglicher und verursachen einen größeren wirtschaftlichen Schaden. Solange Ransomware Cyberkriminellen eine relativ einfache Einnahmequelle bietet und erhebliche Schäden und finanzielle Verluste verursacht, wird sie wahrscheinlich die Hauptbedrohung im Bereich der Cyberkriminalität bleiben.
- Die wichtigsten Einfallstore für Schadsoftware sind Phishing und ungeschützte Remote Desktop Protocols (RDP).
- Für Cyberkriminelle bleiben Daten das wichtigste Ziel und als Ware und Werkzeug weiterhin von wesentlicher Bedeutung.

9 Die Agentur der Europäischen Union für Cybersicherheit (ENISA) äußert sich in ihrem **Bericht aus dem Jahr 2020 "Main incidents in the EU and worldwide"**[15] in

---

[13] BBC News, *Therapy patients blackmailed for cash after clinic data breach*, 26. Oktober 2020.

[14] Europol, *Internet organised crime threat assessment (IOCTA)*, 2019.

[15] ENISA, *Main incidents in the EU and worldwide*: Januar 2019 bis April 2020, Oktober 2020.

ähnlicher Weise und nennt eine Reihe von Beispielen für Cybervorfälle (siehe ***Kasten 3***).

Kasten 3

Agentur der Europäischen Union für Cybersicherheit (ENISA): Cybervorfälle im Zeitraum 2019-2020

Bei der E-Mail-Plattform verifications.io kam es aufgrund einer ungeschützten MongoDB-Datenbank zu einer schwerwiegenden Datenschutzverletzung. Daten aus über 800 Millionen E-Mails waren betroffen, darunter sensible Informationen wie etwa Identitätsangaben (*personally identifiable information*, PII).

Mehr als 770 Millionen E-Mail-Adressen und 21 Millionen Einmal-Passwörter wurden in einem beliebten, vom Cloudservice MEGA1 gehosteten Hackingforum veröffentlicht. Unter dem Namen "Collection #1" wurde es die bedeutendste Sammlung von gestohlenen persönlichen Zugangsdaten der Geschichte.

Der Anbieter von Cloud- und Virtualisierungslösungen Citrix wurde Opfer eines gezielten Cyberangriffs. Um sich Zugriff auf die Citrix-Systeme zu verschaffen, nutzten die Angreifer mehrere kritische Softwareschwachstellen wie etwa CVE-2019-19781 aus, und setzten dabei eine Technik namens "Password Spraying" ein.

Der Cloudhost iNSYNQ19 wurde Opfer eines Ransomware-Angriffs, der zur Folge hatte, dass seine Kunden über eine Woche lang keinen Zugriff auf ihre Daten hatten und gezwungen waren, auf eigene Sicherheitskopien zurückzugreifen.

10 Laut Europol hat sich die Zahl der Cyberangriffe, die durchgeführt werden, um **dauerhafte Schäden** zu verursachen, im ersten Halbjahr 2019 verdoppelt. Betroffen war vor allem das verarbeitende Gewerbe. Dabei handelt es sich nicht um die übliche Ransomware-Angriffe, sondern um Sabotageakte, bei denen Unternehmensdaten dauerhaft gelöscht oder unwiederbringlich beschädigt werden (siehe ***Kasten 4***).

Kasten 4

Zerstörerische Ransomware – die "Germanwiper"-Angriffe von 2019

Im Jahr 2019 wurde eine Reihe von Ransomware-Angriffen aufgedeckt, bei denen in Deutschland tätige Unternehmen ins Visier genommen wurden. Die Ransomware namens *GermanWiper* ersetzt infizierte Dateien durch Nullen und Einsen, was die Wiederherstellung der Dateien unmöglich macht. Sie wurde durch E-Mail-Phishingkampagnen verbreitet. Ziel waren insbesondere Mitarbeiter von Personalabteilungen führender Unternehmen, da die Ransomware in gefälschte Bewerbungen eingebettet war[16].

Das Bewusstsein für Cyberbedrohungen steigt mit ihrer Häufigkeit

11 Dennoch war das Bewusstsein für diese Risiken bis vor Kurzem sehr gering und ihnen wurde kaum Rechnung getragen. Im Jahr 2017 hatten 69 % der Unternehmen in der EU keine oder nur eine grobe Vorstellung von ihrer **Gefährdung durch Cyberangriffe**[17], 60 % hatten noch nie eine Schätzung der **potenziellen finanziellen Verluste**[18] vorgenommen. Einer internationalen Erhebung aus dem Jahr 2018 zufolge würde außerdem ein Drittel der Unternehmen Hackern eher Lösegeld zahlen als in Informationssicherheit zu investieren[19].

---

16 Cybersecurity Insiders, *GermanWiper Ransomware attack warning for Germany*, undatiert.

17 Europäische Kommission, *Factsheet on cybersecurity*, September 2017.

18 Zu diesen Verlusten können unter anderem Folgende gehören: entgangene Einnahmen, Kosten für die Wiederherstellung beschädigter Systeme, potenzielle Haftung für gestohlene Vermögenswerte oder Informationen, Anreize für die Kundenbindung, höhere Versicherungsprämien, höhere Kosten für Schutzmaßnahmen (neue Systeme, Angestellte, Schulungen), potenzielle Begleichung von Compliance-Kosten oder Gerichtskosten.

19 NTT Security, *Risk: Value 2018 Report*.

12 Laut der **Eurobarometer-Umfrage von 2020 "Europeans' attitudes towards cyber security"**[20] nimmt bei Bürgerinnen und Bürgern das Bewusstsein und die Besorgnis in dieser Hinsicht zu:

- Die größte Sorge der Internetnutzer unter den Umfrageteilnehmern, gilt dem möglichen Missbrauch ihrer personenbezogenen Daten (46 %), der Sicherheit ihrer Onlinezahlungen (41 %), der fehlenden Möglichkeit, Artikel selbst in Augenschein zu nehmen oder sich von einer natürlichen Person beraten zu lassen (22 %), sowie der Möglichkeit, dass sie die erworbenen Waren oder Dienstleistungen unter Umständen nicht erhalten (ebenfalls 22 %).
- Mehr als drei Viertel (76 %) der Teilnehmer gehen davon aus, dass das Risiko, Opfer von Cyberkriminalität zu werden, zunimmt. Deutlich weniger (52 %) glauben jedoch, sich ausreichend davor schützen zu können – ein Rückgang um neun Prozentpunkte seit 2018.
- Dennoch sind nur etwas mehr als die Hälfte der Teilnehmer (52 %) der Meinung, dass sie über Cyberkriminalität gut informiert sind, und nur 11 % halten sich für sehr gut informiert.

Cybersicherheit ist für den sozialen Zusammenhalt und die politische Stabilität von Bedeutung

Eine neue Bedrohung: Cybersicherheit und Desinformation

13 Die vorsätzliche Verbreitung systematischer **Desinformationen im großen Stil ist für unsere Demokratien eine dringliche strategische Herausforderung**[21]**.** Desinformationen und gezielte Falschmeldungen ("Fake News") können Gesellschaften spalten, Misstrauen säen und sogar den sozialen Zusammenhalt und das Vertrauen in demokratische Prozesse untergraben (siehe ***Kasten 5***).

---

[20] Europäische Kommission, *Special Eurobarometer 499: Europeans' attitudes towards cyber security*, Januar 2020.

[21] Laut der Studie *The Global Disinformation Order* der Universität Oxford (September 2019) hat sich die Anzahl der Länder, in denen politische Desinformationskampagnen durchgeführt wurden, in den letzten zwei Jahren mehr als verdoppelt (70 Länder).

Kasten 5

Desinformation

Die Europäische Kommission definiert Desinformation als nachweislich falsche oder irreführende Informationen, die mit dem Ziel des wirtschaftlichen Gewinns oder der vorsätzlichen Täuschung der Öffentlichkeit konzipiert, vorgelegt und verbreitet werden und öffentlichen Schaden anrichten können[22]. Unter "öffentlichem Schaden" sind z. B. die Untergrabung demokratischer Prozesse oder die Bedrohung öffentlicher Güter wie Gesundheit, Umwelt und Sicherheit zu verstehen.

Im Gegensatz zu illegalen Inhalten (dazu gehören Hassrede, terroristische Inhalte oder Darstellungen von sexuellem Missbrauch von Kindern) fallen unter Desinformation legale Inhalte. Desinformation überschneidet sich deshalb mit den grundlegenden Werten der Meinungs- und Medienfreiheit der EU. Laut der Definition der Kommission handelt es sich bei irreführender Werbung, Fehlern in der Berichterstattung, Satire und Parodien oder eindeutig gekennzeichneten parteilichen Nachrichten oder Kommentaren nicht um Desinformation.

14 Mithilfe neuer Technologien und Software lässt sich Desinformation über **soziale und sonstige Onlinemedien** leicht und vergleichsweise kostengünstig verbreiten. Desinformation ist in der Regel auf sensible Themen ausgerichtet, die eine Meinungspolarisierung und Emotionalisierung bewirken und deshalb mit größerer Wahrscheinlichkeit weiterverbreitet werden. Zu diesen Themen gehören Fragen rund um Gesundheit (z. B. Kampagnen von Impfgegnern), Migration, Klimawandel und soziale Gerechtigkeit.

Desinformationskampagnen von Drittländern zur Beeinflussung demokratischer Prozesse

15 Mit Desinformationen sollen demokratische Debatten polarisiert, gesellschaftliche Spannungen verstärkt und Wahlsysteme unterminiert werden und sie haben weitreichende Auswirkungen auf Gesellschaft und Sicherheit in Europa. Letzten Endes schwächen sie das Recht auf Meinungsfreiheit und freie Meinungsäußerung. Häufig werden Desinformationskampagnen von **Akteuren in Drittländern gefördert**,

[22] Europäische Kommission, Mitteilung "Bekämpfung von Desinformation im Internet: ein europäisches Konzept" (COM(2018) 236).

die das Ziel verfolgen, unsere Gesellschaften und demokratische Systeme zu destabilisieren. In diesem Zusammenhang ist es möglich, dass im Rahmen groß angelegter Desinformationskampagnen auch Netzwerke gehackt werden. Ein Beispiel dafür ist die russische Einflussnahme auf das Referendum des Vereinigten Königreichs über den Austritt aus der Europäischen Union (siehe ***Kasten 6***).

Kasten 6

Russische Desinformationskampagne nimmt demokratische Entscheidungsprozesse ins Visier[23]

Mitte 2016 starteten Akteure aus Russland eine Kampagne zur Beeinflussung des Referendums des Vereinigten Königreichs vom Juni 2016 über den Austritt aus der EU. Laut einer Analyse von Tweets aus den letzten 48 Stunden vor der Abstimmung twitterten über 150 000 russische Accounts den Hashtag *#Brexit* und posteten über 45 000 Nachrichten über das Referendum. Am Tag des Referendums twitterten russische Accounts 1 102 Mal den Hashtag *#ReasonsToLeaveEU*.

16 Da es gilt, ein ausgewogenes Verhältnis zwischen Sicherheit einerseits und Grundrechten und -freiheiten andererseits zu finden, sodass Innovationen und ein offener Markt gestärkt werden, stellt die Bekämpfung von Desinformation eine enorme Herausforderung dar. Die EU hat eine Reihe von Maßnahmen ergriffen, um **Desinformation zu bekämpfen**.

- Im Jahr 2015 wurde beim EAD die **East StratCom Task Force** eingerichtet, um russischen Desinformationskampagnen entgegenzuwirken[24]. Experten haben sich anerkennend zur Arbeit der Taskforce hinsichtlich der Förderung der Politik der EU, der Unterstützung unabhängiger Medien in den Ländern der Europäischen

[23] Nemr, Christina und Gangware, William, *Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age*, Park Advisors, 2019.

[24] Schlussfolgerungen des Europäischen Rates (EUCO 11/15), 20. März 2015. Seitdem sind zwei Taskforces hinzugekommen, eine für den Westbalkan und eine weitere für die südliche Nachbarschaft.

Nachbarschaftspolitik sowie der Vorwegnahme, des Aufspürens und der Bekämpfung von Desinformation geäußert[25].

- Im Jahr 2018 veröffentlichte die ENISA eine **Mitteilung zur Bekämpfung von Desinformation im Internet**[26]. Sie enthält Maßnahmen, die die Vertrauenswürdigkeit von Inhalten steigern und Bemühungen zur Stärkung der Medien- und Nachrichtenkompetenz unterstützen sollen.

- Die Gemeinsame Forschungsstelle der Kommission hat auf der Grundlage bestehender Politikinstrumente einen auf Freiwilligkeit basierenden **Verhaltenskodex zur Selbstregulierung** erarbeitet, der von Onlineplattformen und der Werbewirtschaft übernommen wurde[27].

- Ein unabhängiges europäisches **Netz von Faktenprüfern** wurde eingerichtet.

Desinformation in Zeiten von COVID-19 und die Reaktion der EU

17 Auch im Zusammenhang mit der durch **COVID-19 verursachten Gesundheitskrise**[28] ist Desinformation ein Problem (in ***Kasten 7*** sind Beispiele für Desinformation in diesem Bereich aufgeführt).

[25] In einem Bericht forderte der Atlantikrat die EU auf, alle Mitgliedstaaten zur Entsendung nationaler Experten in die Taskforce zu verpflichten. Vgl.: Fried, D. und Polyakova, A., *Democratic Offense Against Disinformation*, 5. März 2018.

[26] ENISA, *Strengthening Network & Information Security & Protecting Against Online Disinformation ("Fake News")*, April 2018.

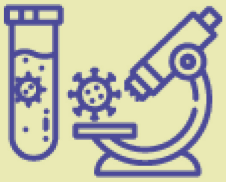
[27] JRC, *The digital transformation of news media and the rise of disinformation and fake news*, JRC Technical Reports, JRC Digital Economy Working Paper 2018-02, April 2018.

[28] Reuters Institute und Universität Oxford, *Types, Sources, and Claims of Covid-19 Misinformation*, April 2020.

Kasten 7

Beispiele für Desinformationen im Zusammenhang mit COVID-19, die von der Kommission gemeldet wurden[29]

Sensationsmeldungen wie "Bleichmittel oder reiner Alkohol helfen gegen Corona": Eine solche Verabreichung ist ganz im Gegenteil sehr gefährlich. **Die belgische Giftzentrale meldete 15 % mehr Unfälle mit Chlorbleiche.**



Verschwörungstheorien wie die Behauptung, Corona sei ein "Eliten-Projekt zur Eindämmung des Bevölkerungswachstums". Die wissenschaftlichen Erkenntnisse sind eindeutig: Corona gehört zu einer Familie von Viren, die von Tieren übertragen werden. Hierzu zählen auch andere Viren wie SARS und MERS.

Unwissenschaftliche Behauptungen wie "Corona wird über 5G verbreitet". Solch substanzlose Meldungen führten zu Anschlägen auf 5G-Sendemasten.

18 Im März 2020 veröffentlichten die Kommission, die ENISA, CERT-EU und Europol eine **gemeinsame Erklärung zu Bedrohungen im Zusammenhang mit COVID-19**[30], in der sie darlegten, dass böswillige Akteure die Herausforderungen der öffentlichen Gesundheitskrise aktiv ausnutzten und dabei Telearbeiter, Unternehmen und Privatpersonen gleichermaßen ins Visier nähmen. Darüber hinaus entwickelte die ENISA Informationskampagnen, die speziell auf Sektoren ausgerichtet sind, die während der COVID-19-Pandemie von Desinformation betroffen sind[31].

---

[29] Europäische Kommission, *Corona-Märchen – nein danke!*, undatiert.

[30] Joint Statement European Commission, ENISA, CERT-EU and Europol, *Coronavirus outbreak*, 20. März 2020.

[31] ENISA, *Informationsblätter zu COVID-19*, 2020.

Die Faktenprüfung ist ein wichtiges Instrument bei der Bekämpfung von Desinformation

19 Darüber hinaus unternahm die EU verstärkte Anstrengungen zur Unterstützung der europäischen Faktenprüfer und Forscher auf dem Gebiet der Desinformation. Insbesondere richtete sie eine **Europäische Beobachtungsstelle für digitale Medien** (European Digital Media Observatory, EDMO) ein, um das Phänomen der Desinformation zu untersuchen und zu beleuchten: Der Fokus liegt dabei auf wichtigen Akteuren, Einfallstoren, Instrumenten, Methoden, Verbreitungsdynamiken, vorrangigen Zielen und den gesellschaftlichen Auswirkungen. Andere Beispiele für EU-finanzierte Projekte zur Bekämpfung von Desinformation sind PROVENANCE, SocialTruth, EUNOMIA und WeVerify.

20 Im Jahr 2018 legte die EU ihren **Verhaltenskodex für den Bereich der Desinformation**[32] und damit die weltweit ersten Normen in Bezug auf die Selbstregulierung zur Bekämpfung von Desinformation vor. Plattformen, führende soziale Netzwerke, Werbeagenturen und die Werbewirtschaft unterzeichneten den freiwilligen Kodex im Oktober 2018. Zu den Unterzeichnern zählen Facebook, Twitter, Mozilla, Google sowie Verbände und Akteure aus der Werbewirtschaft. Microsoft unterzeichnete den Verhaltenskodex im Mai 2019. TikTok trat dem Kodex im Juni 2020 bei.

Gewährleistung der Sicherheit der Wahl zum Europäischen Parlament 2019

21 Die Legitimation der europäischen demokratischen Systeme basiert darauf, dass gut informierte Wähler ihrem demokratischen Willen in **freien und fairen Wahlen** Ausdruck verleihen. Jeder Versuch, die öffentliche Meinung böswillig und vorsätzlich zu untergraben oder zu manipulieren, stellt für die europäischen Gesellschaften daher eine ernsthafte Bedrohung dar. Wahleinmischung und Einflussnahme auf die Wahlinfrastruktur kann ein Versuch sein, die Wählergunst, den Wahlausgang oder den Wahlvorgang selbst zu beeinflussen, sowie die Stimmabgabe, Stimmenauszählung und Verkündung des Wahlergebnisses. Nach dem britischen Referendum koordinierten die Mitgliedstaaten mit Blick auf die Europawahl 2019 erstmals ihr Vorgehen zum **Schutz**

[32] *EU Code of Practice on Disinformation*. September 2018.

der Integrität demokratischer Wahlen, in diesem Fall der Wahl zum Europäischen Parlament, aber auch der nationalen Parlamentswahlen.

22 Wie bereits ausgeführt, veröffentlichte die Kommission im April 2018 die Mitteilung **"Bekämpfung von Desinformation im Internet: ein europäisches Konzept"**[33]. Darauf folgte im September 2018 ein **Wahlpaket**[34], das die Wahlen der EU und ihrer Mitgliedstaaten vor Desinformation und Cyberangriffen schützen sollte. Das Paket war auf die Themen Datenschutz, Transparenz bei politischer Werbung und Parteienfinanzierung, Cybersicherheit und Wahlen sowie Sanktionen für Parteien im Falle von Verstößen gegen Datenschutzvorschriften ausgerichtet. Darüber hinaus fand eine **gemeinsame Übung** statt, um zu prüfen, wie wirksam die Notfallreaktion- und Notfallpläne der Mitgliedstaaten und der EU im Hinblick auf den Schutz der Wahl zum Europäischen Parlament sind (siehe ***Kasten 8***).

[33] Europäische Kommission, Mitteilung "Bekämpfung von Desinformation im Internet: ein europäisches Konzept"(COM(2018) 236 final).

[34] Europäische Kommission, *Lage der Union 2018*, September 2018.

Kasten 8

ELEx19 – Schutz der Wahl zum Europäischen Parlament 2019[35]

Mit der ELex19-Übung zur Widerstandsfähigkeit der anstehenden Wahl zum Europäischen Parlament sollte ermittelt werden, wie Cybersicherheitsvorfälle, die sich womöglich auf die Wahl von 2019 ausgewirkt hätten, verhindert, aufgedeckt und in ihrer Wirkung abgeschwächt werden können.

Auf der Grundlage verschiedener Szenarien mit Cyberbedrohungen und Störfällen hat die Übung den Teilnehmern Folgendes ermöglicht:

— Überblick über das Niveau der Widerstandfähigkeit (in Bezug auf die eingeführten Strategien, verfügbaren Fähigkeiten und Kompetenzen) von Wahlsystemen in der gesamten EU;

— Verbesserung der Zusammenarbeit zwischen den zuständigen Behörden auf nationaler Ebene (einschließlich der für Wahlen zuständigen Behörden und anderer einschlägiger Einrichtungen und Agenturen);

— Prüfung bestehender Krisenmanagementpläne und einschlägiger Verfahren, um Cyberangriffe und hybride Bedrohungen, einschließlich Desinformationskampagnen, zu verhindern, aufzudecken, zu managen und darauf zu reagieren;

— Verbesserung der grenzüberschreitenden Zusammenarbeit und Stärkung der Verbindung zu den einschlägigen Kooperationsgruppen auf EU-Ebene (z. B. Kooperationsnetz für Wahlen, NIS-Kooperationsgruppe, CSIRT-Netz);

— Ermittlung aller weiteren möglichen Lücken sowie angemessener Maßnahmen zur Risikominderung, die im Vorfeld der Wahlen zum Europäischen Parlament durchgeführt werden sollten.

An dieser Übung nahmen mehr als 80 Vertreter der EU-Mitgliedstaaten sowie Beobachter des Europäischen Parlaments, der Kommission und der Agentur der Europäischen Union für Cybersicherheit teil.

[35] ENISA, *EU Member States test their cybersecurity preparedness for fair and free 2019 EU elections*, 5. April 2019.

23 Im Dezember 2018 verabschiedete der Europäische Rat schließlich den **Aktionsplan gegen Desinformation**[36], der eine koordinierte Reaktion ermöglichen und nationale Maßnahmen ergänzen soll. Die Einzelmaßnahmen in diesem Aktionsplan basierten auf vier Säulen: Ausbau der Fähigkeiten der Organe der Union, Desinformation zu erkennen, zu untersuchen und zu enthüllen, mehr koordinierte und gemeinsame Maßnahmen gegen Desinformation, Mobilisierung des Privatsektors bei der Bekämpfung von Desinformation sowie Sensibilisierung der Gesellschaft und Ausbau ihrer Widerstandsfähigkeit.

Cybersicherheit in der EU: Befugnisse, Akteure, Strategien und Gesetzgebung

Cybersicherheit fällt vornehmlich in die Zuständigkeit der Mitgliedstaaten

24 In der EU fällt die Cybersicherheit vornehmlich in die **Zuständigkeit der Mitgliedstaaten**. Dies gilt insbesondere für den Schutz sensibler Informationen im Zusammenhang mit der nationalen Sicherheit. Alle Mitgliedstaaten verfügen über eine **nationale Cybersicherheitsstrategie**, mit der sie Risiken bekämpfen, die den wirtschaftlichen und sozialen Nutzen des Cyberraums beeinträchtigen könnten. Im Hinblick auf Leistungsfähigkeit und Engagement im Bereich Cybersicherheit bestehen zwischen den Mitgliedstaaten jedoch immer noch Unterschiede.

25 Die EU spielt eine wichtige Rolle beim Aufbau eines **gemeinsamen Regelungsrahmens** innerhalb des EU-Binnenmarkts und der Schaffung von Bedingungen, unter denen die Mitgliedstaaten in verschiedenen, für die Cybersicherheit relevanten Politikbereichen – wie Justiz und Inneres, Binnenmarkt, Verkehr, öffentliche Gesundheit, Verbraucherpolitik und Forschung – wirksam zusammenarbeiten können. In den Außenbeziehungen ist die Cybersicherheit ein

[36] Europäische Kommission, Hohe Vertreterin der Union für Außen- und Sicherheitspolitik, *Aktionsplan gegen Desinformation*, JOIN(2018) 36 final. Der Plan hat folgende Schwerpunkte: Ausbau der Fähigkeiten der Organe der Union, Desinformation zu erkennen, zu untersuchen und zu enthüllen, mehr koordinierte und gemeinsame Maßnahmen gegen Desinformation, Mobilisierung des Privatsektors bei der Bekämpfung von Desinformation sowie Sensibilisierung der Gesellschaft und Ausbau ihrer Widerstandsfähigkeit.

Thema in der Diplomatie und zunehmend Teil der neu entstehenden Verteidigungs- und Sicherheitspolitik der EU.

26 Die wichtigsten **Akteure auf EU-Ebene** sind nachstehend in ***Kasten 9*** beschrieben.

Kasten 9

Die wichtigsten Akteure im Bereich der Cybersicherheit auf EU-Ebene

Ziel der **Europäischen Kommission** ist es, die Kapazitäten und die Zusammenarbeit im Bereich der Cybersicherheit auszubauen, der EU als Akteurin bei diesem Thema mehr Gewicht zu verleihen und die Cybersicherheit in andere Politikbereiche der EU zu integrieren.

Die Kommission wird von einer Reihe von EU-Agenturen unterstützt, insbesondere von der **ENISA**, **dem Europäischen Zentrum zur Bekämpfung der Cyberkriminalität (EC3)** und **CERT-EU**. Die **Agentur der Europäischen Union für Cybersicherheit** (auch bekannt als **ENISA** nach ihrem früheren Namen "European Network and Information Security Agency" (Europäische Agentur für Netz- und Informationssicherheit)) hat in erster Linie beratende Funktion und unterstützt die Gestaltung der Politik, den Kapazitätsaufbau und Sensibilisierungsmaßnahmen. Das **EC3** von Europol wurde geschaffen, um die Strafverfolgung von Cyberkriminalität in der EU zu verstärken. Bei der Kommission ist zudem ein **IT-Notfallteam (CERT-EU)** angesiedelt, das alle Organe, Einrichtungen und sonstigen Stellen der Union unterstützt.

Der **Europäische Auswärtige Dienst (EAD)** ist federführend bei der Cyberabwehr, der Cyberdiplomatie und strategischen Kommunikation. Er beherbergt Zentren für Informationsgewinnung und -analyse. Ziel der **Europäischen Verteidigungsagentur (EDA)** ist der Ausbau der Cyberabwehrfähigkeit.

Auf EU-Ebene arbeiten die Mitgliedstaaten mit dem **Rat** zusammen, der zahlreiche Gremien für Koordinierung und Informationsaustausch (darunter die Horizontale Gruppe "Fragen des Cyberraums") eingerichtet hat. Das **Europäische Parlament** ist Teil der Rechtsetzungsbehörde.

Organisationen des Privatsektors, einschließlich Industrie, Netzverwaltungsstellen und Hochschulen, tragen als Partner zur Gestaltung und Umsetzung der Politik bei – auch im Wege einer vertraglichen öffentlich-privaten Partnerschaft **(cPPP)**.

Die Cyberstrategie der EU: Cybersicherheit ist seit 2013 ein wesentliches Anliegen

27 Cybersicherheit ist spätestens seit der Verabschiedung der **Cybersicherheitsstrategie**[37] der Kommission im Jahr 2013 ein wesentliches Anliegen der Politik. In dieser Strategie sind fünf Prioritäten festgelegt:

- Stärkung der Widerstandsfähigkeit gegenüber Cyberangriffen;
- Eindämmung der Cyberkriminalität;
- Erarbeitung einer Cyberverteidigungspolitik und Aufbau von Cyberverteidigungskapazitäten;
- Entwicklung industrieller und technischer Ressourcen für die Cybersicherheit;
- Erarbeitung einer einheitlichen Cyberraumstrategie der EU auf internationaler Ebene und Förderung der Grundwerte der EU.

In den Folgejahren wurde das Thema Cybersicherheit auch in anderen EU-Strategien berücksichtigt (siehe ***Kasten 10***).

[37] Europäische Kommission, *Cybersicherheitsstrategie der Europäischen Union –ein offener, sicherer und geschützter Cyberraum*, JOIN(2013) 1 final, 7. Februar 2013.

Kasten 10

Weitere EU-Strategien, in denen das Thema Cybersicherheit berücksichtigt ist:

- **Europäische Sicherheitsagenda** (2015)[38], deren Ziel es ist, die Strafverfolgung und das Vorgehen der Justiz im Fall von Cyberkriminalität zu verbessern, in erster Linie durch Aktualisierung bestehender Strategien und Rechtsvorschriften;
- **Strategie für einen digitalen Binnenmarkt** (2015)[39], die den Zugang zu digitalen Waren und Dienstleistungen verbessern soll: Dazu muss es gelingen, Sicherheit, Vertrauen und Inklusion im Online-Bereich zu stärken;
- **Globale Strategie für die Außen- und Sicherheitspolitik der Europäischen Union** (2016)[40], in der eine Reihe von Initiativen zur Stärkung der Rolle der EU in der Welt dargelegt sind. Cybersicherheit bildet dabei zusammen mit der Widerlegung von Desinformation durch strategische Kommunikation einen Grundpfeiler.

28 Darüber hinaus veröffentlichten die Europäische Kommission und die Hohe Vertreterin der Union für Außen- und Sicherheitspolitik im Jahr 2017 eine **Gemeinsame Mitteilung zur Cybersicherheit in der EU**[41] an das Europäische Parlament und den Rat, in der sie solidere und wirksamere Strukturen zur Förderung der Cybersicherheit und zum Umgang mit Cyberangriffen, und zwar nicht nur in den Mitgliedstaaten, sondern auch in den Organen, Einrichtungen und sonstigen Stellen der EU forderten.

---

[38] Europäische Kommission, *Die Europäische Sicherheitsagenda* (COM(2015) 185 final), 28. April 2015.

[39] Europäische Kommission, *Strategie für einen digitalen Binnenmarkt für Europa* (COM(2015) 192 final), 6. Mai 2015.

[40] EAD, *Gemeinsame Vision, gemeinsames Handeln: Ein stärkeres Europa. Eine Globale Strategie für die Außen- und Sicherheitspolitik der Europäischen Union*, Juni 2016.

[41] Europäische Kommission und die Hohe Vertreterin der Union für Außen- und Sicherheitspolitik, *Gemeinsame Mitteilung "Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen"* (JOIN(2017) 450 final), 13. September 2017.

29 Im Juli 2020 überarbeitete die Europäische Kommission ihre Agenda aus dem Jahr 2015 und verabschiedete die **EU-Strategie für eine Sicherheitsunion**[42] für den Zeitraum 2020-2025, in der Cybersicherheit zur Frage von strategischer Bedeutung erklärt wird. In dieser Strategie weist die Kommission insbesondere auf sogenannte hybride Bedrohungen hin, die sowohl Cyberangriffe als auch Desinformationskampagnen umfassen und bei denen staatliche und nichtstaatliche Akteure ihr Vorgehen abstimmen, um das Informationsumfeld zu manipulieren und wichtige Infrastrukturen anzugreifen.

Die EU-Rechtsvorschriften zur Cybersicherheit: die Richtlinie zur Netz- und Informationssicherheit, die DSGVO, der Rechtsakt zur Cybersicherheit und ein neuer Sanktionsmechanismus

30 Wichtigste Säule der Cybersicherheitsstrategie von 2013 und rechtliches Kernstück ist die **Richtlinie zur Netz- und Informationssicherheit**[43] **(NIS-Richtlinie)** aus dem Jahr 2016, mit der erstmals EU-weit geltende Rechtsvorschriften zur Cybersicherheit festgelegt wurden. Gemäß dieser Richtlinie müssen die Mitgliedstaaten nationale Strategien für die Sicherheit von Netz- und Informationssystemen beschließen sowie zentrale Anlaufstellen und Computer-Notfallteams (CSIRTs)[44] einrichten. Ziel ist es, ein Mindestmaß an Harmonisierung bei den einschlägigen Fähigkeiten der Mitgliedstaaten herbeizuführen. Außerdem werden in der Richtlinie Sicherheitsanforderungen und Meldepflichten für die Betreiber wesentlicher Dienste in kritischen Sektoren und für Anbieter digitaler Dienste festgelegt.

---

[42] Europäische Kommission, *Mitteilung "EU-Strategie für eine Sicherheitsunion*, (COM(2020)605 final), 24. Juli 2020.

[43] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union.

[44] Diese Teams sind Teil der in der Richtlinie vorgesehenen Kooperationsstrukturen, nämlich des CSIRT-Netzwerks (ein aus Vertretern der CSIRT der Mitgliedstaaten und des CERT-EU bestehendes Netzwerk, dessen Sekretariatsgeschäfte von der ENISA geführt werden) und der Kooperationsgruppe (zur Unterstützung und Erleichterung der strategischen Zusammenarbeit sowie des Informationsaustauschs zwischen den Mitgliedstaaten, deren Sekretariatsgeschäfte von der Kommission geführt werden).

31 Die Mitgliedstaaten waren verpflichtet, **die NIS-Richtlinie bis Mai 2018 in nationales Recht** umzusetzen und bis November 2018 sogenannte "Betreiber wesentlicher Dienste" zu benennen. Die Europäische Kommission ist verpflichtet, das Funktionieren dieser Richtlinie regelmäßig zu überprüfen. Im Rahmen ihres zentralen politischen Ziels "Ein Europa für das digitale Zeitalter" und der Ziele der Sicherheitsunion führte die Kommission von Juli bis Oktober 2020 eine Konsultation durch, deren Ergebnisse in eine erste Bewertung und eine Ex-post-Folgenabschätzung der NIS-Richtlinie einfließen sollen.

32 Daneben trat 2016 die **Datenschutz-Grundverordnung**[45] (DSGVO) in Kraft, die seit Mai 2018 anzuwenden ist. Diese Verordnung soll die personenbezogenen Daten der EU-Bürgerinnen und -Bürger durch die Aufstellung von Regeln für ihre Verarbeitung und Verbreitung schützen. Darin werden bestimmte Rechte der betroffenen Personen und Pflichten der für die Datenverarbeitung Verantwortlichen (Anbieter digitaler Dienste) bei der Verwendung und Übermittlung von Informationen festgelegt.

33 Außerdem wird mit dem **Rechtsakt zur Cybersicherheit**[46] erstmals ein unionsweiter Rahmen für die Zertifizierung der Cybersicherheit für IKT-Produkte, -Dienste und -Prozesse eingeführt. Dies bedeutet, dass in der EU tätige Unternehmen ihre IKT-Produkte, -Prozesse und -Dienste nur einmal zertifizieren müssen, da diese Zertifizierung in der gesamten EU anerkannt wird. Durch den Rechtsakt zur Cybersicherheit der EU wurde auch die **Agentur der Europäischen Union für Cybersicherheit** eingerichtet (die Kurzform ENISA wurde von dem früheren Namen "European Network and Information Security Agency" [Europäische Agentur für Netz- und Informationssicherheit] übernommen). Die Agentur erhält das Mandat, die operative Zusammenarbeit auf Unionsebene zu stärken, indem sie den EU-Mitgliedstaaten auf Ersuchen bei der Klärung von Cybersicherheitsvorfällen Hilfe

[45] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

[46] Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik.

leistet und die Koordinierung auf Unionsebene bei massiven grenzüberschreitenden Vorfällen und Krisen in Bezug auf Cybersicherheit unterstützt.

34 Schließlich hat der Rat im Mai 2019 ein Rechtsinstrument angenommen, mit dem die EU gezielt restriktive Maßnahmen zur **Verhinderung von Cyberangriffen**, die eine externe Bedrohung für die EU oder ihre Mitgliedstaaten darstellen, und zur Reaktion auf solche Angriffe verhängen kann[47]. Infolgedessen verfügt die EU über die rechtliche Befugnis, Sanktionen gegen natürliche und juristische Personen zu verhängen, die

- für Cyberangriffe oder versuchte Cyberangriffe verantwortlich sind;
- finanzielle, technische oder materielle Unterstützung für Cyberangriffe oder versuchte Cyberangriffe leisten oder auf andere Weise daran beteiligt sind.

Im Juli 2020 machte der Rat zum ersten Mal von diesen neuen Befugnissen Gebrauch (siehe ***Kasten 11***).

Kasten 11

Mit harten Bandagen – EU verhängt erstmals Sanktionen wegen Cyberangriffen[48]

Im Juli 2020 verhängte der Rat restriktive Maßnahmen gegen sechs natürliche und drei juristische Personen, die für verschiedene Cyberangriffe verantwortlich oder daran beteiligt waren. Dazu gehören der versuchte Cyberangriff auf die Organisation für das Verbot chemischer Waffen sowie die als "WannaCry", "NotPetya" und "Operation Cloud Hopper" bekannten Angriffe.

Zu den verhängten Sanktionen gehören unter anderem ein Reiseverbot und das Einfrieren von Vermögenswerten. Darüber hinaus dürfen natürliche und juristische Personen aus der EU den in der Liste aufgeführten natürlichen und juristischen Personen keine Mittel zur Verfügung stellen.

---

[47] Beschluss (GASP) 2019/797 des Rates vom 17. Mai 2019 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen.

[48] Beschluss (GASP) 2020/1127 des Rates vom 30. Juli 2020 zur Änderung des Beschlusses (GASP) 2019/797 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen.

Cybersicherheit und Cyberabwehr

35 In den letzten Jahren wird der Cyberraum zunehmend für militärische Zwecke[49] genutzt und als Waffe[50] eingesetzt. Er gilt heute neben Land, See, Luft und Weltraum als fünfte Dimension der Kriegsführung. Im Jahr 2014 wurde ein **EU-Politikrahmen für die Cyberabwehr** verabschiedet, der 2018 aktualisiert wurde[51]. Zu den Prioritäten in der aktualisierten Fassung von 2018 zählen unter anderem der Aufbau von Kapazitäten im Bereich der Cyberabwehr sowie der Schutz der Kommunikations- und Informationsnetze der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP) der EU. Die Cyberabwehr ist auch Teil des Rahmens für die Ständige Strukturierte Zusammenarbeit (SSZ) und der Zusammenarbeit von EU und NATO.

36 Fälle, in denen der Cyberraum zu politischen Zwecken genutzt und die Cybersicherheit der EU und der Mitgliedstaaten durch Angriffe auf den Prüfstand gestellt und unterwandert werden, häufen sich. Diese Cyberspionage- und Hackingangriffe, bei denen zielgerichtet nationale Regierungen, politische Organe und die EU-Institutionen ins Visier genommen werden, um an der Geheimhaltung unterliegende Informationen zu gelangen und diese zu sammeln, legen nahe, dass die EU und ihre Mitgliedstaaten ausgeklügelten Angriffen in den Bereichen Cyberspionage und Datenmanipulation ausgesetzt sind. Mit dem **Gemeinsamen Rahmen für die Abwehr hybrider Bedrohungen** (2016) geht die EU gegen Cyberbedrohungen von kritischen Infrastrukturen und privaten Nutzern vor und betont, Cyberangriffe könnten auch als Desinformationskampagnen in sozialen Medien erfolgen[52]. Das Bewusstsein

---

[49] Zentrum für Europäische Politische Studien, *Strengthening the EU's Cyber Defence Capabilities – Report of a CEPS Task Force*, November 2018.

[50] Die Schadsoftware hinter dem *WannaCry*-Angriff, der laut den Vereinigten Staaten, dem Vereinigten Königreich und Australien von Nordkorea ausgegangen sein soll, wurde ursprünglich von der US-amerikanischen *National Security Agency* entwickelt und geheim gehalten, um Schwachstellen in Windows zu nutzen.
Quelle: Greenberg, A., WIRED, 19. Dezember 2017. Nach den Angriffen verurteilte Microsoft die Geheimhaltung von Software-Schwachstellen durch Regierungen und wiederholte seine Forderung nach einer Digitalen Genfer Konvention.

[51] *EU-Politikrahmen für die Cyberabwehr (Aktualisierung 2018)*, 14413/18, 19. November 2018.

[52] Europäische Kommission und Europäischer Auswärtiger Dienst, *Gemeinsamer Rahmen für die Abwehr hybrider Bedrohungen – eine Antwort der Europäischen Union* (JOIN(2016) 18 final), 6. April 2016.

für hybride Bedrohungen müsse verbessert und die Zusammenarbeit zwischen der EU und der NATO verstärkt werden, was in den Gemeinsamen Erklärungen der EU und der NATO der Jahre 2016 und 2018[53] konkretisiert wurde.

Ausgaben im Bereich Cybersicherheit in der EU: nicht gebündelt und dem Bedarf nicht angemessen

Die EU-27 gibt weniger für Cybersicherheit aus als die Vereinigten Staaten

37 Die öffentlichen Ausgaben für Cybersicherheit lassen sich nur schwer schätzen, da sie sich auf mehrere Bereiche erstrecken und sich häufig nicht von allgemeinen IT-Ausgaben abgrenzen lassen[54]. Dennoch deuten die verfügbaren Daten darauf hin, dass die **öffentlichen Ausgaben für Cybersicherheit** in der EU vergleichsweise niedrig sind:

- Im Jahr 2020 waren im Haushalt der US-Bundesregierung allein für Cybersicherheit rund **17,4 Milliarden US-Dollar**[55] veranschlagt.
- Im Vergleich dazu schätzt die Kommission die öffentlichen Ausgaben für Cybersicherheit auf **1 bis 2 Milliarden Euro** pro Jahr für alle EU-Mitgliedstaaten, die zusammengenommen ein BIP erwirtschaften, dessen Höhe nahezu dem der Vereinigten Staaten entspricht[56].

---

[53] "*Joint declaration by the Presidents of the European Council and the European Commission, and the Secretary General of the North Atlantic Treaty Organization*", 8. Juli 2016 und 10. Juli 2018.

[54] Europäische Kommission, COM(2018) 630 final, 12. September 2018.

[55] The White House, *Cybersecurity budget fiscal year 2020*.

[56] Europäische Kommission, "Commission Staff Working Document: Impact Assessment Accompanying the document 'Proposal for a Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027'", SWD(2018) 305 final, 6. Juni 2018.

- Viele Mitgliedstaaten geben in Prozent des BIP schätzungsweise **ein Zehntel des Niveaus der Vereinigten Staaten** oder sogar noch weniger für Cybersicherheit aus[57].

2014-2020: EU-Ausgaben für mehrere unterschiedliche Instrumente der Cybersicherheit

38 Laut der Kommission[58] gibt es im Gesamthaushaltsplan der EU mindestens **zehn verschiedene Instrumente**, über die Angelegenheiten im Zusammenhang mit der Cybersicherheit finanziert werden können (die in finanzieller Hinsicht wichtigsten Programme sind in ***Kasten 12*** aufgeführt). Die EU-Mittel für die nichtmilitärische Cybersicherheit beliefen sich im Zeitraum 2014-2020 insgesamt auf **weniger als 200 Millionen Euro pro Jahr**. Außerdem gibt es kein unionsweites Finanzierungsinstrument, mit dem die Mitgliedstaaten bei der Koordinierung ihrer Cybersicherheitsmaßnahmen unterstützt werden.

[57] The Hague Centre for Strategic Studies, *Dutch investments in ICT and cybersecurity: putting it in perspective*, Dezember 2016.

[58] Europäische Kommission, *Impact assessment accompanying the proposal for a Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres*, SWD(2018) 403 final, 12. September 2018.

Kasten 12

EU-Programme zur Förderung von Cybersicherheitsprojekten (2014-2020)

- Im Zeitraum 2014-2020 wurden Projekten mit Bezug zur Cybersicherheit und Cyberkriminalität im Rahmen des **Forschungsprogramms Horizont 2020** rund 600 Millionen Euro zugewiesen. Dies umfasst 450 Millionen Euro für die vertragliche öffentlich-private Partnerschaft (cPPP) für Cybersicherheit im Zeitraum 2017-2020, mit der weitere 1,8 Milliarden Euro aus dem Privatsektor mobilisiert werden sollen.

- Über die **Europäischen Struktur- und Investitionsfonds (ESI-Fonds)** werden den Mitgliedstaaten bis Ende 2020 bis zu 400 Millionen Euro für Investitionen in die Cybersicherheit bereitgestellt.

- Mit der **Fazilität "Connecting Europe"** wurden Investitionen in Höhe von bis zu 30 Millionen Euro pro Jahr finanziert. Dadurch konnten unter anderem die nationalen Computer-Notfallteams (CERT), die die Mitgliedstaaten gemäß der NIS-Richtlinie einrichten müssen, zwischen 2016 und 2018 mit rund 13 Millionen Euro pro Jahr kofinanziert werden[59].

- Aus dem **Fonds für die innere Sicherheit – Polizei (ISF-P)** werden Studien, Expertentreffen und Kommunikationsmaßnahmen finanziert. Diese beliefen sich im Zeitraum 2014-2017 auf fast 62 Millionen Euro. Außerdem können die Mitgliedstaaten im Rahmen der geteilten Mittelverwaltung Finanzhilfen für Ausrüstung, Schulung, Forschung und Datenerhebung erhalten. 19 Mitgliedstaaten haben solche Finanzhilfen in Höhe von insgesamt 42 Millionen Euro in Anspruch genommen.

- Im Rahmen des **Programms "Justiz"** werden 9 Millionen Euro zur Unterstützung von Verträgen zur justiziellen Zusammenarbeit und Rechtshilfe zur Verfügung gestellt. Der Schwerpunkt lag dabei insbesondere auf dem Austausch von elektronischen Daten und Finanzinformationen.

39 Darüber hinaus wurden in den Jahren 2019 und 2020 dem **Europäischen Programm zur industriellen Entwicklung im Verteidigungsbereich** 500 Millionen Euro

[59] Artikel 9 Absatz 2 der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-Richtlinie).

aus dem EU-Haushalt zugewiesen[60]. Das Programm ist auf die Verbesserung von Koordinierung und Wirtschaftlichkeit bei den Verteidigungsausgaben der Mitgliedstaaten durch Anreize für gemeinsame Entwicklungen ausgerichtet. Ziel ist es, durch den Europäischen Verteidigungsfonds ein Investitionsvolumen von insgesamt 13 Milliarden Euro für die Verteidigungsfähigkeit nach 2020 zu generieren, wobei ein Teil auf die Cyberabwehr entfällt. Im Rahmen der **Europäischen Sicherheitsinitiative** sollte die Europäische Investitionsbank zwischen 2018 und 2020 insgesamt 6 Milliarden Euro für Projekte mit doppeltem Verwendungszweck bereitstellen (Forschung und Entwicklung sowie Cybersicherheit und zivile Sicherheit)[61].

2021-2027: Neues Programm "Digitales Europa"

40 Im Juli 2020 beschloss der Rat in seinen Schlussfolgerungen zum neuen mehrjährigen Finanzrahmen (MFR) für den Zeitraum 2021-2027, dass das **Programm "Digitales Europa"**[62] in wichtige strategische digitale Kapazitäten wie Hochleistungsrechnen künstliche Intelligenz und Cybersicherheit in der EU investieren wird. Es wird andere Instrumente – insbesondere "Horizont Europa" und die Fazilität "Connecting Europe" – bei der Unterstützung des digitalen Wandels in Europa ergänzen.

41 Darüber hinaus beschloss der Rat, dem Programm "Digitales Europa" im Zeitraum 2021-2027 6,8 Milliarden Euro bzw. rund **970 Millionen Euro pro Jahr** zuzuweisen. Dies ist ein erheblicher Anstieg im Vergleich zum Zeitraum 2014-2020, der Betrag bleibt aber weiterhin unter dem Vorschlag der Kommission (8,2 Milliarden Euro für den gleichen Zeitraum, davon 2 Milliarden Euro für die Stärkung der Cybersicherheitsbranche der EU und den Schutz der Gesellschaft insgesamt, zum Beispiel durch Unterstützung der Umsetzung der NIS-Richtlinie).

---

[60] Europäische Kommission, Verordnung (EU) 2018/1092 des Europäischen Parlaments und des Rates vom 18. Juli 2018 zur Einrichtung des Europäischen Programms zur industriellen Entwicklung im Verteidigungsbereich zwecks Förderung der Wettbewerbsfähigkeit und der Innovation in der Verteidigungsindustrie der Union (ABl. L 200 vom 7.8.2018, S. 30).

[61] Europäische Investitionsbank, *Operativer Rahmen und Operativer Gesamtplan 2018 der EIB-Gruppe*, 12.12.2017.

[62] Europäische Kommission, *Europe investing in digital: the Digital Europe Programme*, September 2020.

TEIL II – Überblick über die Arbeit der ORKB

Einleitung

42 Cybersicherheit und digitale Autonomie haben sich für die EU und ihre Mitgliedstaaten zu Themen von strategischer Bedeutung entwickelt. In allen Mitgliedstaaten bestehen im öffentlichen wie im privaten Sektor weiterhin Schwachstellen im Bereich der Cybersicherheits-Governance, die allerdings unterschiedlich ausgeprägt sind. Dies beeinträchtigt unsere Möglichkeiten, Cyberangriffen vorzubeugen und darauf zu reagieren, wenn dies erforderlich ist.

43 Eine Umfrage unter den Obersten Rechnungskontrollbehörden (ORKB) der EU aus dem Jahr 2018 ergab jedoch, dass rund die Hälfte noch nie eine Prüfung im Bereich Cybersicherheit durchgeführt hatte. Seitdem haben die ORKB ihre Prüfungsarbeit verstärkt auf die Cybersicherheit ausgerichtet und dabei besonders den Datenschutz, die Abwehr von Cyberangriffen und den Schutz kritischer öffentlicher Versorgungssysteme in den Blick genommen. Sie untersuchten auch andere Themen von hoher Relevanz. Da sich manche dieser Prüfungen unter Umständen auf sensible Informationen (aus dem Bereich der nationalen Sicherheit) erstrecken, können verständlicherweise nicht alle veröffentlicht werden.

44 Da Cybersicherheit für das Funktionieren unserer Gesellschaften und politischen Institutionen von so großer Bedeutung ist, beschloss der Kontaktausschuss, dieses Thema zum Gegenstand des diesjährigen Prüfungskompendiums zu machen. Der vorliegende zweite Teil enthält eine Zusammenfassung der Ergebnisse ausgewählter Prüfungen, die von den ORKB der 12 Mitgliedstaaten, die zu dieser Publikation beigetragen haben, und dem Europäischen Rechnungshof durchgeführt wurden. Jede dieser ORKB beteiligte sich mit einem ausgewählten Prüfungsbericht. Teil III dieses Kompendiums enthält Zusammenfassungen dieser Berichte. Die weiteren von den ORKB erwähnten Berichte zeigen, dass noch zahlreiche weitere Prüfungen zu diesem Thema durchgeführt worden sind.

Prüfungsmethoden und Prüfungsthemen

45 Was die Art der Prüfungen betrifft, auf denen die in diesem Kompendium zusammengefassten Prüfungsberichte basieren, hatten die meisten beteiligten ORKB Wirtschaftlichkeitsprüfungen zu Themen im Zusammenhang mit Cybersicherheit, zwei (die polnische und die ungarische ORKB) Compliance-Prüfungen und einer (der Hof) eine Analyse der staatlichen Maßnahmen durchgeführt.

46 Die meisten ORKB nahmen mindestens zwei Methoden zur Bewertung des Prüfungsgegenstands in ihren Prüfungsansatz auf. Dazu gehörten die Überprüfung von Strategiedokumenten oder festgelegten staatlichen Maßnahmen auf hoher (z. B. nationaler) Ebene, eine Überprüfung von Verfahren zur Beurteilung ihrer Regelkonformität mittels der bewährten COBIT-Methodik (siehe ***Kasten 13***) oder eine Überprüfung der Wirksamkeit der bestehenden IT-Managementsysteme. Ein Rechnungshof (der niederländische) setzte sogar ethische Hacker ein, um die Wirksamkeit der Cybersicherheitssysteme für Grenzkontrollen und kritische Wasserinfrastrukturen zu untersuchen. ***Kasten 14*** enthält eine systematische Zusammenfassung der Methoden und Techniken, die die verschiedenen ORKB im Rahmen ihrer Prüfungsarbeit nutzten.

Kasten 13

Was ist COBIT?

COBIT steht für *Control Objectives for Information and Related Technology* und ist ein Rahmen anerkannter bewährter Verfahren und Vorgehensweisen für das IT-Management und die IT-Governance. Festgelegt wurde COBIT von der ISACA *(Information Systems Audit and Control Association)*. Der Rahmen hilft der jeweiligen Organisation, strategische Ziele durch den wirksamen Einsatz der verfügbaren Ressourcen und die Minimierung der IT-Risiken zu erreichen. Er stellt die Verbindung zwischen Organisationsführung und IT-Governance her. Dazu werden die geschäftlichen mit den IT-Zielen verknüpft, Kennzahlen und Reifegradmodelle definiert, um zu messen, ob Ziele erreicht werden, und die Zuständigkeiten der für Unternehmens- und IT-Prozesse Verantwortlichen festgelegt.

47 Die Prüfungen zur Cybersicherheit hatten sehr unterschiedliche Themenschwerpunkte. Einige ORKB prüften sehr spezifische Bereiche von öffentlichem Interesse. Der niederländische Rechnungshof beispielsweise prüfte die Cybersicherheit der für das Land lebenswichtigen Küstenschutzanlagen und Wasserbewirtschaftungssysteme. Andere, wie die irische und die ungarische ORKB, behandelten eher Querschnittsfragen, wie die Umsetzung der nationalen Cybersicherheitsstrategie und den Schutz personenbezogener Daten und nationaler Datenbestände. Dennoch befassten sich alle ORKB mit Problemen, die sich negativ auf öffentliche Dienstleistungen oder die Infrastruktur auswirken könnten.

48 Die Rechnungshöfe Estlands und Litauens erkannten die strategische Bedeutung nationaler Datenbestände an, die für die nationale Sicherheit und den Schutz ihrer Integrität vor externen Cyberangriffen unerlässlich sind. Der dänische Rechnungshof widmete sich in einer Prüfung speziell der Frage, ob vier öffentliche Stellen vor Ransomware-Angriffen sicher waren. Die Rechnungshöfe der Niederlande, Polens und Portugals prüften die Wirksamkeit verschiedener IT-Systeme zur Unterstützung von Grenzkontrollen (am Flughafen Schiphol, bei der Leitung des polnischen Grenzschutzes und im Ministerium für Inneres und Verwaltung in Polen sowie an den portugiesischen Grenzen) und befassten sich deshalb auch mit der Sicherheit innerhalb der EU.

Prüfungszeitraum

49 Die in diesem Kompendium enthaltenen ausgewählten Prüfungsberichte wurden zwischen 2014 und 2020 veröffentlicht. In den meisten Fällen erstreckte sich der Prüfungszeitraum auf mindestens zwei Jahre, in vier Fällen (Dänemark, Estland, Frankreich und Portugal) allerdings nur auf ein Jahr.

Prüfungsziele

50 Die verschiedenen an diesem Kompendium beteiligten ORKB befassten sich in ihren Prüfungen mit einer Reihe verschiedener Risiken. Die in ihren Beiträgen behandelten Risiken umfassten die Bedrohung der Rechte einzelner Bürgerinnen und Bürger der EU durch den unsachgemäßen Umgang mit personenbezogenen Daten, das Risiko, dass öffentliche Einrichtungen wichtige öffentliche Dienstleistungen nicht erbringen können oder nur eingeschränkt leistungsfähig sind, schwerwiegende Folgen für die öffentliche Sicherheit, das Gemeinwohl und die Wirtschaft eines Mitgliedstaats sowie Cybersicherheit in der EU. Mindestens vier ORKB (Estland, Ungarn, Niederlande und Portugal) deckten in ihren in diesem Kompendium enthaltenen Prüfungsberichten mindestens drei der genannten Themen ab.

51 Cybersicherheit fällt weiterhin in den Zuständigkeitsbereich der Mitgliedstaaten. Da die Gesetzgebung der EU jedoch im Laufe der Zeit umfassender und spezifischer geworden ist, tragen die meisten der von den ORKB geprüften Einrichtungen und Stellen dennoch bereits zur Verwirklichung der strategischen Ziele für die EU-Cybersicherheit bei, wenn auch in unterschiedlichem Maße. Der irische Rechnungshof (*Office of the Comptroller and Auditor General*) prüfte beispielsweise die Umsetzung der EU-Richtlinie zur Netz- und Informationssicherheit, die die Widerstandsfähigkeit

wichtiger Netz- und Informationssysteme stärken soll, und unterbreitete Empfehlungen zu ihrer Verbesserung. Der ungarische Rechnungshof befasste sich in seiner Prüfung ebenfalls mit der Einhaltung bestehender EU-Richtlinien.

52 Aus ***Kasten 14*** geht auch hervor, ob das Ergebnis der Prüfung entweder dazu beigetragen hat, die Widerstandsfähigkeit der geprüften Stelle gegenüber Cyberangriffen zu verbessern, ob es eine Eindämmung der Cyberkriminalität bewirkt hat oder ob es zur Entwicklung einer Cyberverteidigungspolitik sowie zur Stärkung der Kompetenzen, zur Verbesserung der Entwicklung neuer Technologien und zu Fortschritten bei der Zusammenarbeit auf internationaler Ebene geführt hat, wobei es sich um die wesentlichen Ziele der Cybersicherheitsstrategie der EU handelt. Die Empfehlungen der ORKB bezogen sich in den meisten Fällen auf mehr als zwei strategische Ziele, die die EU erreichen möchte.

53 Darüber hinaus wurden durch die Prüfungsarbeit der ORKB Sicherheits- und Umsetzungslücken identifiziert, die die geprüften Stellen zu weiteren Anstrengungen veranlassten. So begannen vier in Dänemark geprüfte Stellen noch während der laufenden Prüfung mit der Implementierung mehrerer vorausschauender Sicherheitskontrollen, um den Schutz vor Ransomware-Angriffen deutlich zu verstärken, ihre Verteidigungskapazitäten auszubauen und ihre Widerstandsfähigkeit gegenüber Cyberangriffen zu stärken und dadurch in Zukunft weniger anfällig für Cyberkriminalität zu sein.

54 Des Weiteren konnte der Hof feststellen, dass die Prüfungsempfehlungen auf verschiedenen Verwaltungs- und Verantwortungsebenen vorgelegt wurden, bei Regierungen genauso wie bei Ministerien und anderen Stellen auf operativer Ebene sowie bei den Verantwortlichen für IT-Systeme.

Kasten 14

Überblick über die Prüfungsarbeiten der ORKB, die in dieses Kompendium eingeflossen sind (Teil 1)

Schwerpunktbereich		Dänemark	Estland	Irland	Frankreich	Lettland	Litauen	Ungarn	Niederlande	Polen	Portugal	Finnland	Schweden	EU (Europäischer Rechnungshof)
Art der Prüfung	Wirtschaftlichkeit	✓	✓	✓	✓	✓	✓		✓		✓	✓	✓	
	Compliance							✓		✓				
	Analyse													✓
Prüfungsansatz	Überprüfung politischer Maßnahmen	✓	✓	✓		✓	✓	✓	✓		✓	✓	✓	✓
	Überprüfung von Verfahren	✓	✓		✓		✓	✓		✓	✓	✓		
	Überprüfung von Systemen	✓			✓	✓	✓	✓	✓	✓	✓		✓	
	Bewertung der Belastbarkeit durch eine Direktprüfung								✓		✓			
Berücksichtigte Bedrohungen	Auswirkungen auf einzelne Rechte		✓		✓			✓			✓			✓
	Auswirkungen auf öffentliche Infrastruktur und Dienste	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Auswirkungen auf die nationale Sicherheit		✓	✓		✓	✓	✓	✓		✓			
	Auswirkungen auf die Sicherheit in der EU	✓							✓		✓			✓

Überblick über die Prüfungsarbeiten der ORKB, die in dieses Kompendium eingeflossen sind (Teil 2)

Schwerpunktbereich		Dänemark	Estland	Irland	Frankreich	Lettland	Litauen	Ungarn	Niederlande	Polen	Portugal	Finnland	Schweden	EU (Europäischer Rechnungshof)
Berücksichtigte strategische Ziele für die EU-Cybersicherheit	Stärkung der Widerstandsfähigkeit gegenüber Cyberangriffen	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
	Eindämmung von Cyberkriminalität	✓					✓							✓
	Entwicklung einer Cyberverteidigungspolitik und von Cyberverteidigungskapazitäten;	✓	✓	✓		✓	✓	✓	✓	✓				✓
	Entwicklung technischer Ressourcen				✓	✓			✓				✓	
	Verbesserung der internationalen Zusammenarbeit (Politik)			✓				✓						✓
Empfehlungen gerichtet an	Regierungen	✓	✓				✓					✓	✓	✓
	Operative Ebene (Ministerien und Behörden)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	IT-Systemverantwortliche	✓			✓			✓	✓	✓				

Wichtigste Prüfungsfeststellungen

55 In den folgenden Abschnitten sind die wichtigsten Prüfungsfeststellungen der ORKB zusammengefasst.

Wirtschaftlichkeitsprüfungen

56 Der **dänische Rechnungshof *(Rigsrevisionen)*** bewertete, ob die ausgewählten wesentlichen staatlichen Institutionen ausreichend vor Ransomware geschützt waren. Staatliche Institutionen sind häufiges Ziel von Cyberangriffen und Ransomware ist derzeit eine der größten Bedrohungen der Cybersicherheit. Geprüft wurden die dänische Behörde für Gesundheitsdaten, das Außenministerium, Banedanmark (das dänische Eisenbahnnetz) und die dänische Behörde für Notfallmanagement. Diese vier Institutionen wurden ausgewählt, weil sie für die Bereitstellung wesentlicher Dienste in den Bereichen Gesundheit, Außenpolitik, Verkehr und Notfallvorsorge zuständig sind, in denen die Sicherstellung des Datenzugriffs von entscheidender Bedeutung sein kann. Die Prüfung ergab, dass die vier Institutionen nicht ausreichend vor Ransomware geschützt waren. Es zeigte sich, dass mehrere gängige Sicherheitskontrollen zur Eindämmung von Angriffen von den vier Institutionen nicht implementiert worden waren. Bei der Prüfung wurde festgestellt, dass es wichtig ist, dass die Institutionen die Implementierung vorausschauender Sicherheitskontrollen ins Auge fassen, um ihre Widerstandsfähigkeit gegenüber Ransomware-Angriffen zu stärken.

57 Der **estnische Rechnungshof *(Riigikontroll)*** erkannte, dass Estland zur Bewahrung seiner Unabhängigkeit nicht nur sein Staatsgebiet verteidigen können, sondern auch die digitalen Vermögenswerte, die für den Staat von vorrangiger Bedeutung sind, schützen muss. Die digitalen Vermögenswerte, bei denen der größte Schutzbedarf besteht, sind Daten zu Bürgerinnen und Bürgern, zum Staatsgebiet und zur Gesetzgebung. Ebenfalls gesichert werden müssen Daten betreffend das Eigentum, die Immobilien und die Rechte der in Estland ansässigen Bürgerinnen und Bürger. Der estnische Rechnungshof berücksichtigte mögliche Cyberbedrohungen im Falle einer Eskalation der Sicherheitsprobleme. Solche Risikoszenarien und ein Anstieg der IT-Sicherheitsvorfälle, wie Cyberangriffe und Datenlecks, könnten die für den Staat wichtigsten Daten und Datenbanken gefährden. Deshalb ging es bei der Prüfung um die Frage, wie der Staat festlegt, welche Daten und Datenbanken für die Gewährleistung der nationalen Sicherheit unerlässlich sind. Die Prüfung ergab, dass

staatliche Behörden ISKE[63], einen dreistufigen IT-Grundschutz, zwar verpflichtend einsetzen müssen, es aber in mehreren kritischen Datenbanken weiterhin erhebliche Schwachstellen bei der Gewährleistung der Informationssicherheit gab.

58 Der **irische Rechnungshof *(Office of the Comptroller and Auditor General)*** überprüfte die Fortschritte, die seit der Einrichtung des irischen nationalen Zentrums für Cybersicherheit *(Irish National Cyber Security Centre)* im Hinblick auf die Cybersicherheitsmaßnahmen erzielt worden waren. Das 2011 eingerichtete Zentrum ist dem Ministerium für Umwelt, Klima und Kommunikation unterstellt. Sein Fokus liegt vor allem auf dem Schutz der staatlichen Netze und der kritischen nationalen Infrastruktur sowie der Unterstützung von Wirtschaft und Privatpersonen beim Schutz ihrer eigenen Systeme. Die Prüfung ergab, dass das nationale Zentrum für Cybersicherheit zwar eine kritische Funktion ausübt, es in den ersten vier Jahren seines Bestehens aber deutlich schlechter mit Finanzmitteln ausgestattet war als ursprünglich vorgesehen. Auch steht hinter der allgemeinen strategischen Ausrichtung des Zentrums kein strategischer Plan. Darüber hinaus mangelt es an Klarheit hinsichtlich der jeweiligen Rollen der an der Untersuchung von Cyberkriminalität und nationalen Sicherheitsvorfällen beteiligten Behörden. Außerdem müssen die Anforderungen der EU-Richtlinie zur Netz- und Informationssicherheit im Hinblick auf die Entwicklung einer nationalen Strategie noch umgesetzt werden.

59 Der **französische Rechnungshof *(Cour des comptes)*** unterzog "*Parcoursup*" einer eingehenden Prüfung. Dabei handelt es sich um eine neue digitale Plattform, die als Informationsquelle für verfügbare Universitätsstudiengänge und Zulassungsvoraussetzungen dient. Ihr Ziel ist es, die Übereinstimmung zwischen den Fähigkeiten und schulischen Leistungen der angehenden Studierenden und den Inhalten der Hochschullehrpläne zu vergrößern. Die Prüfung ergab, dass es den zuständigen Behörden gelungen ist, den Zugang zu allen postsekundären Studiengängen über die digitale Plattform zu zentralisieren, um auf den Ausbau des Hochschulbildungsangebots zu reagieren. Allerdings wurde das Vorgängersystem in aller Eile zu *Parcoursup* umgebaut, ohne dass wesentliche strukturelle Änderungen vorgenommen wurden. Deshalb wurden auch die Schwachstellen des Informationssystems im Hinblick auf Sicherheit, Leistung und Belastbarkeit nicht behoben. Die Plattform ist nach wie vor mit erheblichen Risiken in Bezug auf die

[63] ISKE ist ein für den öffentlichen Sektor in Estland entwickelter IT-Sicherheitsstandard. Für Einrichtungen auf staatlicher und kommunaler Ebene, die mit Datenbanken und Registern umgehen, ist seine Anwendung verpflichtend.

Qualität und Kontinuität öffentlicher Dienstleistungen und die Sicherheit personenbezogener Daten behaftet.

60 Der **lettische Rechnungshof *(Valsts Kontrole)*** führte eine Wirtschaftlichkeitsprüfung zur Wirtschaftlichkeit der Infrastruktur der öffentlichen Informations- und Kommunikationstechnologie (IKT) durch. Mit dieser Prüfung sollte untersucht werden, ob die öffentliche Verwaltung beim wirtschaftlichen Management der IKT-Infrastruktur einem gemeinsamen Ansatz folgte und ob die Einrichtungen die Vorteile der Zentralisierung bewertet hatten. Die Prüfung ergab, dass das Zögern der Behörden, die IKT-Infrastruktur zentral zu verwalten, dazu geführt hatte, dass mehrere Serverräume eingerichtet wurden, wodurch sich die Instandhaltungskosten deutlich erhöhten. In den meisten Serverräumen wurden Sicherheitsbedrohungen festgestellt – die Rechenzentren waren nicht ausreichend gegen unbefugten physischen Zutritt und Umweltrisiken geschützt. Darüber hinaus hatten die Einrichtungen keine Verfahren eingerichtet, um regelmäßig zu bewerten, ob es kostengünstiger wäre, die Instandhaltung der IKT-Infrastruktur intern durchzuführen, sie in Zusammenarbeit mit einer anderen Einrichtung durchzuführen oder die IKT-Instandhaltung auszulagern. Die Prüfer empfahlen, ein System zur regelmäßigen Überwachung einzurichten, mit dem die gesamte öffentliche Verwaltung als ein einziges System bewertet werden könnte.

61 Der **litauische Rechnungshof *(Valstybės kontrolė)*** erkannte die Bedeutung kritischer staatlicher elektronischer Informationsressourcen, zum Beispiel für die Verwaltung der öffentlichen Finanzen und die Steuerbehörden sowie die erbrachte Gesundheitsversorgung. Der Verlust von kritischen Informationen und die Nichtverfügbarkeit entsprechender Informationssysteme hätten möglicherweise schwerwiegende Folgen für die öffentliche Sicherheit, das Gemeinwohl und die Wirtschaft. Ziel der Prüfung war die Bewertung der Verwaltung (der allgemeinen Steuerung) sowie des Reifegrads kritischer staatlichen Informationsressourcen. Sowohl bei der Gestaltung als auch bei der Umsetzung der Politik in Bezug auf die staatlichen Informationsressourcen sowie im Verwaltungsmechanismus wurden systembedingte Probleme ermittelt. Die Prüfer gelangten zu dem Schluss, dass der niedrige Reifegrad der kritischen staatlichen Informationsressourcen auf Schwachstellen bei der Gestaltung und Umsetzung der Politik in Bezug auf die staatlichen Informationsressourcen hindeutete und diese Ressourcen damit stärker gefährdet waren. Um die Sicherheit der staatlichen Informationsressourcen zu erhöhen, muss der Verwaltungsmechanismus verbessert werden.

62 Im Jahr 2018 beschloss der **niederländische Rechnungshof (Algemene Rekenkamer)**, Prüfungen zur Cybersicherheit in Sektoren durchzuführen, die für die Gesellschaft von entscheidender Bedeutung sind. Die ersten beiden geprüften Sektoren waren die Wasserwirtschaft, die für ein Land, das in großen Teilen unter dem Meeresspiegel liegt, lebensnotwendig ist, sowie das automatische Grenzkontrollsystem, das seine Bedeutung dadurch erlangt, dass es sich beim Amsterdamer Flughafen Schiphol um ein internationales Drehkreuz und ein Tor in die Niederlande handelt. Die Ministerin für Infrastruktur und Wasserwirtschaft wies eine Reihe von Wasserinfrastrukturen, die von der Generaldirektion für öffentliche Versorgungseinrichtungen und Wasserwirtschaft (die geprüfte Stelle) verwaltet werden, als "kritische Teile" der Wasserwirtschaft aus. Viele Computersysteme, die beim Betrieb der kritischen Wasserinfrastrukturen zum Einsatz kommen, stammen noch aus den 1980er- und 1990er-Jahren, einer Zeit, als Cybersicherheit noch nicht allgemein berücksichtigt wurde. Die Verteidigungsministerin und der Minister für Justiz und Sicherheit teilen sich die Zuständigkeit für die Grenzkontrollen, die vom niederländischen Grenzschutz am Flughafen Schiphol durchgeführt werden. Beide Ministerien verfügen über IT-Systeme, die vom Grenzschutz genutzt werden. Die Systeme sind für den Flughafenbetrieb unerlässlich und werden genutzt, um hochsensible Daten zu verarbeiten. Damit sind sie ein interessantes Ziel für Cyberangriffe, mit denen Grenzkontrollen sabotiert, ausspioniert oder manipuliert werden sollen. Im Rahmen der Prüfung wurde untersucht, ob die geprüften Stellen sich auf den Umgang mit Cyberbedrohungen vorbereitet hatten und ob diesbezüglich wirksame Maßnahmen ergriffen worden waren. Im Fall der Wasserinfrastrukturen musste die geprüfte Stelle im Zusammenhang mit der Aufdeckung und Bekämpfung von Cyberbedrohungen noch weitere Anstrengungen unternehmen, um ihre eigenen Cybersicherheitsziele zu erreichen. In Bezug auf die Grenzkontrollen waren die Cybersicherheitsmaßnahmen weder angemessen noch zukunftsfähig.

63 Der **portugiesische Rechnungshof *(Tribunal de Contas)*** prüfte die Informationssysteme, die die Erteilung, Ausstellung und Nutzung des portugiesischen elektronischen Reisepasses unterstützen, insbesondere die automatische Kontrolle von Fluggästen durch das Auslesen biometrischer Daten an den portugiesischen Grenzen. Bei der Prüfung wurde die Einhaltung von EU- und nationalem Recht, internationalen Normen und Richtlinien für die Erteilung, Ausstellung und Nutzung des portugiesischen elektronischen Reisepasses sowie die Angemessenheit des nationalen Rechtsrahmens überprüft. Untersucht wurden die Wirksamkeit der wichtigsten Prozesse im Zusammenhang mit dem Lebenszyklus des portugiesischen elektronischen Reisepasses, insbesondere im Zusammenhang mit der Erteilung, Ausstellung und

Nutzung des Passes. Bei der Prüfung wurden außerdem kritische Aspekte der Leistungsfähigkeit von Informationssystemen überprüft, insbesondere die Frage, ob die Sicherheitsvorschriften im Hinblick auf die Informationssysteme zum portugiesischen elektronischen Reisepass (SIPEP) erfüllt waren.

64 Der **finnische Rechnungshof *(Valtiontalouden tarkastusvirasto)*** untersuchte, ob der Schutz der Zentralregierung vor Cyberangriffen so wirksam und kosteneffizient wie möglich war. Der Prüfungsschwerpunkt lag auf der Frage, wie die Zentralregierung mit dem Thema Cybersicherheit umgeht. Geprüft wurden unter anderem die Behörden, die bei der Zentralregierung für den Cyberschutz zuständig sind (das Büro des Ministerpräsidenten, das Finanzministerium und das Ministerium für Verkehr und Kommunikation), sowie die Behörden, die die Verantwortung für zentrale Cyberschutzaufgaben und IT-Dienste in der Zentralregierung tragen. In der finnischen Regierung ist die Zuständigkeit für den Cyberschutz dezentral organisiert, und jede Stelle ist für ihre eigene Cybersicherheit verantwortlich. Die Prüfer empfahlen dem Finanzministerium, für Cybervorfälle in den IKT-Diensten der Zentralregierung ein umfassendes Betriebsmanagementmodell auszuarbeiten und umzusetzen. Das Finanzministerium sollte außerdem herausfinden, wie die Cybersicherheit der Dienste bei der Finanzierung dieser Dienste während ihres gesamten Lebenszyklus berücksichtigt werden kann, und das operative Situationsbewusstsein erhöhen, indem es die Behörden anweist, Cybervorfälle an das Cybersicherheitszentrum zu melden.

65 Der **schwedische Rechnungshof *(Riksrevisionen)*** befasste sich mit der Verbreitung veralteter IT-Systeme in der zentralen staatlichen Verwaltung, um zu ermitteln, ob die Regierung und die Behörden geeignete Maßnahmen ergriffen hatten, um zu verhindern, dass die IT-Systeme zu einem Hindernis für eine wirksame Digitalisierung werden. Bei der Prüfung wurde festgestellt, dass es in zahlreichen staatlichen Behörden veraltete IT-Systeme gab. In vielen der geprüften Behörden war mindestens ein betriebskritisches IT-System veraltet und einem großen Teil der untersuchten Behörden fehlte der richtige Ansatz zur Entwicklung und Verwaltung der IT-Unterstützung. In zahlreichen Behörden fehlte eine allgemeine Beschreibung des Zusammenspiels von Strategien, operativen Abläufen und Systemen. Die Prüfer gelangten zu dem Schluss, dass es den meisten Behörden noch nicht gelungen war, die Probleme im Zusammenhang mit veralteten IT-Systemen wirksam anzugehen. Nach Ansicht des schwedischen Rechnungshofs ist das Problem so gravierend und weit verbreitet, dass es ein Hindernis für die kontinuierliche effiziente Digitalisierung der staatlichen Verwaltung darstellt.

Compliance-Prüfungen zum Thema Cybersicherheit

66 Der **ungarische *Rechnungshof (Állami Számvevöszék)*** erkannte, dass die Sicherheit der nationalen Datenbestände für die Gesellschaft im Hinblick auf die Erhaltung und den Schutz nationaler Werte von grundlegendem Interesse ist. Die Verbesserung der Sicherheit personenbezogener und öffentlicher Daten in den nationalen Datenbeständen Ungarns ist von wesentlicher Bedeutung, um das Vertrauen der Bürgerinnen und Bürger in den Staat zu stärken und das kontinuierliche und reibungslose Funktionieren der öffentlichen Verwaltung sicherzustellen. Der Zweck der Compliance-Prüfung zum Datenschutz in Ungarn bestand darin, zu beurteilen, ob in Ungarn ein rechtlicher und operativer Rahmen für den Datenschutz geschaffen worden war und ob die wichtigsten mit der Datenverwaltung befassten Stellen die Anforderungen an die sichere Datenverwaltung und die Auslagerung der Datenverarbeitung erfüllten. Die Prüfung ergab, dass die internen Vorschriften der für die Datenverwaltung zuständigen Stellen in Bezug auf Datenverwaltungstätigkeiten den Schutz der nationalen Datenbestände als integralen Bestandteil der nationalen Vermögenswerte in Einklang mit den zwischen 2011 und 2015 geltenden gesetzlichen Bestimmungen gewährleistet haben. Die für die Datenverarbeitung Verantwortlichen hatten die Vorschriften sowie den Datentransfer an Dritte ordnungsgemäß umgesetzt.

67 Der **polnische Rechnungshof *(Najwyższa Izba Kontroli)*** bewertete, ob die in den Systemen zur Ausführung wichtiger öffentlicher Aufgaben erfassten Daten geschützt waren. Die Prüfung erstreckte sich auf sechs Institutionen, die solche wichtigen öffentlichen Aufgaben erfüllten. Die Informationssicherheitssysteme waren nicht ausgereift genug und nicht weit genug implementiert, um ein ausreichendes Schutzniveau der in den Systemen zur Ausführung wichtiger öffentlicher Aufgaben erfassten Daten zu bieten. Die Informationssicherheitsprozesse liefen ungeordnet und – in Ermangelung von Verfahren – intuitiv ab. Nur eine der sechs geprüften Stellen hatte das Informationssicherheitssystem implementiert, allerdings muss hinzugefügt werden, dass es bei seinem Betrieb zu erheblichen Fehlern kam. Die Prüfung ergab, dass auf zentraler Ebene allgemeine Empfehlungen und Anforderungen im Zusammenhang mit der IT-Sicherheit erarbeitet und umgesetzt werden müssen, die für alle öffentlichen Einrichtungen gelten.

Analysen im Bereich der Cybersicherheit

68 Der ***Europäische Rechnungshof*** analysierte die Cybersicherheitspolitik der EU und ermittelte die wichtigsten Herausforderungen für eine wirksame Umsetzung der

Politik. Die Analyse erstreckte sich auf die Bereiche Netz- und Informationssicherheit, Cyberkriminalität, Cyberabwehr und Desinformation. Dabei wurde eine Reihe von Lücken in der Cybersicherheitsgesetzgebung der EU ermittelt und festgestellt, dass die bestehenden Rechtsvorschriften in den Mitgliedstaaten nicht kohärent umgesetzt wurden. Schließlich wurde bei der Analyse darauf hingewiesen, dass es auf EU-Ebene an zuverlässigen Daten zu Cybervorfällen und einem umfassenden Überblick über die Ausgaben der EU und der Mitgliedstaaten im Bereich Cybersicherheit mangelte. Zudem wurde festgestellt, dass es Engpässe bei der Ausstattung der für Cyberfragen zuständigen EU-Agenturen mit angemessenen Mitteln gibt, einschließlich von Problemen bei der dauerhaften Anwerbung und Bindung von Fachkräften. Eine weitere Herausforderung bestand darin, dass die Finanzierung der Cybersicherheit nur unzureichend auf die strategischen Ziele der EU abgestimmt ist.

TEIL III – Zusammenfassung der ORKB-Berichte

Dänemark
Rigsrevisionen

Schutz vor Ransomware-Angriffen

Datum der Veröffentlichung: 2017

Hyperlink zum Bericht: Zusammenfassung des Berichts (in englischer Sprache)

Prüfungsart und -zeitraum

Prüfungsart: Wirtschaftlichkeitsprüfung

Prüfungszeitraum: April-September 2017

Zusammenfassung des Berichts

Prüfungsthema

In diesem Bericht wurde die Frage erörtert, ob die ausgewählten wesentlichen staatlichen Institutionen ausreichend vor Ransomware geschützt waren.

Staatliche Institutionen sind häufiges Ziel von Cyberangriffen und Ransomware ist derzeit eine der größten Bedrohungen der Cybersicherheit. Bei Ransomware handelt es sich um Schadsoftware, die den Zugriff auf Daten blockiert. In der Regel verschlüsselt Ransomware die Daten, sodass die von dem Angriff betroffenen Institutionen sie nicht verwenden können. Die Hacker verlangen ein Lösegeld, um die Daten zu entschlüsseln und den Institutionen wieder Zugriff zu gewähren. Daraus folgt, dass Ransomware eine besondere Bedrohung für die Zugänglichkeit von Daten darstellt.

Wenn ihnen der Zugriff auf Daten plötzlich nicht mehr möglich ist, können Institutionen wichtige Dienstleistungen nur noch mühsam oder gar nicht mehr erbringen. Die von einem Ransomware-Angriff betroffenen Institutionen sind in der Regel gezwungen, ihr IT-Netz ganz oder teilweise herunterzufahren, um das Ausmaß des Angriffs zu untersuchen. Ransomware-Angriffe haben unter Umständen erhebliche wirtschaftliche Folgen, da es bei den Betroffenen zu Produktionsausfällen kommen

kann, wenn sie zum Beispiel nicht auf ihr IT-Netz zugreifen können oder über einen längeren Zeitraum erhobene oder verarbeitete Daten verloren gehen. Im Jahr 2017 mussten nach einem Ransomware-Angriff auf die britische nationale Gesundheitsbehörde 19 000 Operationen und Arzttermine abgesagt werden. Die Leitung dieser Institutionen sollte ihren Fokus deshalb auf das Risiko von Ransomware-Angriffen richten und die notwendigen Sicherheitskontrollen implementieren, um sich vor Ransomware zu schützen und die Folgen eines potenziellen Angriffs einzudämmen.

An der Studie nahmen die dänische Behörde für Gesundheitsdaten, das Außenministerium, Banedanmark (das dänische Eisenbahnnetz) und die dänische Behörde für Notfallmanagement teil. Diese vier Institutionen wurden ausgewählt, weil sie für die Bereitstellung wichtiger Dienste in den Bereichen Gesundheit, Außenpolitik, Verkehr und Notfallvorsorge zuständig sind, in denen der Zugang zu Daten von entscheidender Bedeutung sein kann. Die Behörde für Gesundheitsdaten erbringt darüber hinaus zentralisierte IT-Dienstleistungen für den Großteil der dem Gesundheitsministerium unterstehenden staatlichen Stellen.

Im Rahmen dieser Studie sollte festgestellt werden, ob die vier Institutionen ausreichend vor E-Mail-basierten Ransomware-Angriffen geschützt waren. Der dänische Rechnungshof untersuchte deshalb 20 gängige Sicherheitskontrollen, die einen Grundschutz vor Ransomware bieten. Darüber hinaus analysierte der Rechnungshof fünf Sicherheitskontrollen, die die Institutionen in Verbindung mit zukünftigen Risikobewertungen in Betracht ziehen sollten. Zu vorausschauenden Kontrollen zählen beispielsweise neue Technologien, mit denen die Anzahl gefälschter E-Mails, die bei einer Institution eingehen, gesenkt und bei ungewöhnlichen Aktivitäten auf Computern Warnungen gesendet werden. Die Studie wurde vom dänischen Rechnungshof initiiert und beruht auf den Feststellungen von vier zwischen April und September 2017 durchgeführten IT-Prüfungen. Die Studie bietet eine Momentaufnahme davon, wie gut die Institutionen vor Ransomware geschützt waren. Die Institutionen hatten Gelegenheit, nach Abschluss der IT-Prüfungen 20 gängige Sicherheitskontrollen zu implementieren. Die Ergebnisse der Studie beziehen sich deshalb nur auf den Ransomware-Schutz der Institutionen zum Zeitpunkt der vier IT-Prüfungen. Die Studie gewährt einen Einblick in die Leistung der vier Institutionen, umfasst aber weder eine vergleichende Analyse noch eine Rangliste ihres Abschneidens.

Prüfungsfeststellungen und Schlussfolgerungen

Der dänische Rechnungshof gelangte zu dem Schluss, dass die vier Institutionen nicht ausreichend vor Ransomware geschützt waren. Die Studie zeigte, dass mehrere gängige Sicherheitskontrollen zur Eindämmung von Angriffen von den vier Institutionen nicht implementiert worden waren. Insbesondere bei der Behörde für Gesundheitsdaten und bei Banedanmark gab es erhebliche Sicherheitslücken. Dies bedeutet, dass alle vier Institutionen einem erhöhten Risiko durch E-Mail-basierte Ransomware-Angriffe ausgesetzt waren, die sie an der Bereitstellung ihrer Dienste für unterschiedlich lange Zeiträume gehindert hätten. Alle vier Institutionen haben dem dänischen Rechnungshof mitgeteilt, dass sie seit der Fertigstellung der Studie daran gearbeitet haben, einige der Sicherheitskontrollen zu implementieren, um das Schutzniveau in Bezug auf Ransomware zu erhöhen.

Die Maßnahmen der Institutionen zur Verhütung von Ransomware-Angriffen, einschließlich interner und externer Bedrohungen, waren unzureichend. Ganz besonders bedenklich war, dass keine der Institutionen dafür gesorgt hatte, dass ihre Sicherheitssoftware auf dem neuesten Stand war, und dass drei Institutionen keine Positivlisten führten, damit Mitarbeiter keine Schadsoftware ausführen konnten. Dadurch steigt das Risiko, dass Ransomware einen Teil oder das gesamte IT-Netz infiziert und sich ausbreitet.

In drei dieser Institutionen schenkte die Leitung Ransomware-Angriffen nicht genug Aufmerksamkeit. Die von den Leitungsorganen der Behörde für Gesundheitsdaten und Banedanmark durchgeführten Risikobewertungen deckten nicht alle relevanten Aspekte ab. Dies bedeutet, dass den Institutionen keine aktuelle Bewertung der Bedrohung durch Ransomware vorlag und sie deshalb schlecht aufgestellt waren, um neue Angriffe zu verhüten und die Folgen zukünftiger Angriffe abzumildern. Die Leitungsorgane der Behörde für Gesundheitsdaten und von Banedanmark hatten kein ausreichendes Gewicht auf die Risikobewertung gelegt; die IT-Sicherheit in diesen beiden Institutionen basierte deshalb nicht auf den von den Leitungsorganen festgelegten Prioritäten.

Drei der Institutionen verfügten über keine ausreichenden Notfallpläne, die ihnen hätten helfen können, nach einem Ransomware-Angriff den Betrieb wieder aufzunehmen. Besonders schwer wiegt, dass drei Institutionen nicht regelmäßig überprüften, ob sie in der Lage wären, von einem Ransomware-Angriff betroffene Daten und Systeme wiederherzustellen. Dadurch steigt das Risiko, dass von diesen Institutionen verwaltete Daten im Zusammenhang mit einem Ransomware-Angriff

verloren gehen und die Institutionen für eine längere Zeit nicht in der Lage sind, ihre Dienste bereitzustellen.

Da sich die Risikoszenarien ständig ändern, ist es wichtig, dass die Institutionen die Implementierung vorausschauender Sicherheitskontrollen in Betracht ziehen, um ihre Widerstandsfähigkeit gegenüber Ransomware-Angriffe zu stärken. Dabei handelt es sich um Kontrollen, mit denen die Identität von E-Mail-Absendern leichter überprüft und potenziell schädliche E-Mails erkannt und herausgefiltert werden können. Alle vier Institutionen arbeiten derzeit an einigen der vorausschauenden Sicherheitskontrollen, die zur Verbesserung ihres Schutzes vor Ransomware-Angriffen beitragen können.

Weitere Berichte in diesem Bereich

Titel des Berichts:	"Report on the protection of research data at the Danish universities"
Hyperlink zum Bericht:	Zusammenfassung des Berichts (in englischer Sprache)
Datum der Veröffentlichung:	2019

Titel des Berichts:	"Report on the protection of IT systems and health data in three Danish regions"
Hyperlink zum Bericht:	Zusammenfassung des Berichts (in englischer Sprache)
Datum der Veröffentlichung:	2017

Titel des Berichts:	"Report on management of IT security in systems outsourced to external suppliers"
Hyperlink zum Bericht:	Zusammenfassung des Berichts (in englischer Sprache)
Datum der Veröffentlichung:	2016

Titel des Berichts:	"Report on the access to IT systems that support the provision of essential services to the Danish society"
Hyperlink zum Bericht:	Zusammenfassung des Berichts (in englischer Sprache)
Datum der Veröffentlichung:	2015

Estland
Riigikontroll

Gewährleistung der Sicherheit und Erhaltung von kritischen staatlichen Datenbanken in Estland

Datum der Veröffentlichung: Mai 2018

Hyperlink zum Bericht: Zusammenfassung des Berichts (in englischer Sprache)
Bericht (in estnischer Sprache)

Prüfungsart und -zeitraum

Prüfungsart: Wirtschaftlichkeitsprüfung

Prüfungszeitraum: 2017

Zusammenfassung des Berichts

Prüfungsthema

Um Estlands Unabhängigkeit zu bewahren, muss das Land nicht nur sein Staatsgebiet verteidigen, sondern auch seine digitalen Vermögenswerte, die für den Staat von vorrangiger Bedeutung sind, vor Ereignissen zu schützen, die die größte Bedrohung darstellen. Die digitalen Vermögenswerte, bei denen der größte Schutzbedarf besteht, sind Daten zu Bürgerinnen und Bürgern, zum Staatsgebiet und zur Gesetzgebung. Auch Daten im Zusammenhang mit Eigentum, Immobilien und Rechten der in Estland ansässigen Personen müssen gesichert werden.

Deshalb befasste sich der estnische Rechnungshof mit der Frage, wie der Staat bestimmt hatte, welche Daten und Datenbanken für die Gewährleistung der nationalen Sicherheit unerlässlich sind. Er überprüfte den Schutz der Sicherheit und Kontinuität dieser Daten und Datenbanken und erstellte eine Übersicht über die für den Schutz eingesetzten Instrumente.

Da Estland inzwischen Mitglied der NATO und der Europäischen Union ist, ist die physische Sicherheit des Landes heute besser als vor dem Beitritt. Estland muss jedoch mögliche Cyberbedrohungen im Falle einer Eskalation von Sicherheitsproblemen

berücksichtigen. Solche Risikoszenarien und eine Zunahme der Anzahl der IT-Sicherheitsvorfälle, wie Cyberangriffe und Datenlecks, könnten außerdem die Daten und Datenbanken gefährden, die für den Staat von vorrangiger Bedeutung sind. Sollten die Daten, die für den Staat von vorrangiger Bedeutung sind, unbefugt geändert oder offengelegt werden bzw. verloren gehen, könnte der Staat seine notwendigen Funktionen nicht mehr ausüben. Dazu zählen die Gewährleistung der Sicherheit der Bürgerinnen und Bürger, die Bereitstellung der Grundversorgung, die Schaffung eines wirtschaftsfreundlichen Umfelds und vieles mehr. Estland plant zunächst, rund eine Million Euro in die Speicherung kritischer Daten im Ausland zu investieren.

Prüfungsfragen

- Haben die Ministerien alle kritischen Datenbanken und Datenverarbeitungsvorschriften ermittelt?
- Sind die kritischen Datenbanken und Register ausreichend gesichert?
- Ist die langfristige Kontinuität kritischer Daten und Datenbanken gewährleistet?

Prüfungsfeststellungen

Der estnische Rechnungshof legte im Hinblick auf die geprüften kritischen Datenbanken die folgenden Bemerkungen vor:

- Es fehlte an einem Maßnahmenplan bzw. an Vorschriften für die Umsetzung des Konzepts der kritischen Datenbanken. Für die Auswahl der kritischen Datenbanken waren keine Bedingungen festgelegt worden und es war nicht sicher, dass alle erforderlichen Datenbanken in den Prozess einbezogen worden waren. Der zusätzliche Schutz der Datenbanken war informell organisiert worden und war für die Eigentümer der Datenbanken nicht verpflichtend, sodass für die in den fünf kritischen Datenbanken enthaltenen Daten keine Sicherungskopien im Ausland erstellt worden waren.
- Für die kritischen Datenbanken waren keine zusätzlichen Vorschriften für die Informationssicherheit festgelegt worden. Weder das Informationssicherheitssystem ISKE (ein für den öffentlichen Sektor in Estland entwickelter Sicherheitsstandard, dessen Anwendung für Einrichtungen auf staatlicher und kommunaler Ebene, die mit Datenbanken und Registern umgehen, verpflichtend ist) noch etwaige Rechtsvorschriften oder Normen enthielten zusätzliche Anforderungen für kritische Datenbanken, zum Beispiel in

Bezug auf die Speicherung von Sicherungskopien außerhalb Estlands. Zwar waren Sicherungskopien der geprüften Datenbanken im Ausland gespeichert, aber es war nicht getestet worden, ob die Arbeit der Informationssysteme daraus wiederhergestellt werden konnte.

- Im Hinblick auf die kritischen Datenbanken stellten die Implementierung von ISKE und die damit zusammenhängenden Prüfungen ein Problem dar. Zum Zeitpunkt der Prüfung waren für zwei der 10 Datenbanken noch keine ISKE-Prüfungen durchgeführt worden. Darüber hinaus waren diese erst gegen Ende dieser Prüfung (30. November 2017) organisiert worden. Nur zwei kritische Datenbanken waren tatsächlich so häufig geprüft worden wie gesetzlich vorgeschrieben. In einigen Fällen waren außerdem die vom Prüfer festgestellten Probleme nicht in dem Zeitraum zwischen zwei ISKE-Prüfungen (zwei bis drei Jahre) behoben worden.

- Im Verlauf der Prüfung stellte der estnische Rechnungshof fest, dass eine Reihe wichtiger Informationssicherheitsmaßnahmen in einigen kritischen Datenbanken nicht implementiert worden waren. Zum Beispiel enthielten die Leitlinien zur Informationssicherheit keine Vorschriften zur regelmäßigen Bewertung der Schwachstellen von Informationssystemen, die Ereignisprotokolle wurden nicht regelmäßig überprüft oder analysiert, es gab keine Schulungsprogramme zur Informationssicherheit und keine Analysen zum Stand der Sensibilisierung für Informationssicherheit im Bereich der öffentlichen Verwaltung, die als Grundlage für solche Schulungsprogramme hätten dienen können, die Integrität der Dateien wurde in einigen Fällen nicht geprüft und es wurden keine externen Penetrationstests durchgeführt.

Schlussfolgerungen und Empfehlungen

Bei der Prüfung wurde festgestellt, dass es trotz der Implementierung von ISKE, einem dreistufigen IT-Grundschutz, dessen Einsatz in staatlichen Behörden und im Rahmen ihrer Prüfungen verpflichtend vorgeschrieben ist, in mehreren kritischen Datenbanken erhebliche Mängel bei der Gewährleistung der Informationssicherheit gab, wie etwa bei der Analyse von Protokollen, Penetrationstests und dem Schutz mobiler Geräte. Die besonderen Anforderungen an den Schutz kritischer Daten waren noch nicht festgelegt worden.

Das Ministerium für Wirtschaft und Kommunikation hatte die ersten für den Schutz kritischer Daten erforderlichen Maßnahmen zwar in die Wege geleitet, aber das

Projekt zu den kritischen Datenbanken befand sich in einer Phase, in der rechtlich verbindliche Vorschriften erforderlich waren. Darüber hinaus waren weder eine detaillierte Risikoanalyse noch ein Aktionsplan für die Zukunft vorhanden.

Von fünf kritischen Datenbanken wurden Sicherungskopien in Botschaften im Ausland aufbewahrt, doch im Falle einer physischen Zerstörung der Rechenzentren in Estland wäre die Erhaltung der kritischen Daten in den verbleibenden fünf Datenbanken nicht gewährleistet.

Es wurden zwei allgemeine Empfehlungen unterbreitet:

- Es sollten Vorschriften für den zusätzlichen Schutz kritischer Datenbanken festgelegt werden, unter anderem zur Auswahl kritischer Datenbanken, zur Verarbeitung der Daten in diesen Datenbanken und zur Erstellung von Sicherungskopien von Daten, die für den Staat von vorrangiger Bedeutung sind. Darüber hinaus sollte bewertet werden, wie zusätzliche Mittel für diese Maßnahmen bereitgestellt werden können.
- Die verschiedenen Phasen der Einrichtung dieser Datenbanken sollten im Hinblick auf die Finanzplanung und die Informationssicherheit analysiert werden. Bei der Umsetzung dieser Phasen sollten bewährte Verfahren aus dem Projektmanagement zur Anwendung kommen.

Oifig an Ard-Reachtaire Cuntas agus Ciste
Office of the Comptroller and Auditor General

Irland
Office of the Comptroller and Auditor General

Maßnahmen im Zusammenhang mit der nationalen Cybersicherheit

Datum der Veröffentlichung: September 2018

Hyperlink zum Bericht: Zusammenfassung des Berichts (in englischer Sprache)

Prüfungsart und -zeitraum

Prüfungsart: Wirtschaftlichkeitsprüfung

Prüfungszeitraum: 2011-2018

Zusammenfassung des Berichts

Prüfungsthema

In Irland ist das Ministerium für Umwelt, Klima und Kommunikation (*Department of Communications, Climate Action and Environment*) für die Cybersicherheitspolitik verantwortlich. Über das nationale Zentrum für Cybersicherheit (*National Cyber Security Centre*) ist das Ministerium darüber hinaus für die Koordinierung der staatlichen Notfallmaßnahmen im Falle eines nationalen Cybersicherheitsvorfalls zuständig.

Das nationale Zentrum für Cybersicherheit wurde 2011 gegründet. Sein Fokus liegt vor allem auf dem Schutz der staatlichen Netze und der kritischen nationalen Infrastruktur sowie der Unterstützung von Wirtschaft und Privatpersonen beim Schutz ihrer eigenen Systeme.

Prüfungsfragen

Im Rahmen dieser Untersuchung wurden die seit der Einrichtung des irischen nationalen Zentrums für Cybersicherheit im Hinblick auf die

Cybersicherheitsmaßnahmen erzielten Fortschritte analysiert. Das besondere Hauptaugenmerk lag auf Fragen im Zusammenhang mit

- dem Auftrag und der Mittelausstattung des Zentrums;
- der nationalen Cybersicherheitsstrategie (2015-2017);
- der Umsetzung der EU-Richtlinie zur Netz- und Informationssicherheit;
- Vereinbarungen zu Governance und Aufsicht.

Prüfungsfeststellungen und Schlussfolgerungen

Zwar wurden mit der Entscheidung der Regierung zur Einrichtung des nationalen Zentrums für Cybersicherheit Mittel in Höhe von 800 000 Euro jährlich genehmigt, doch die tatsächliche Mittelausstattung für den Bereich der Cybersicherheit belief sich zwischen 2012 und 2015 auf weniger als ein Drittel dieser Summe. Im Jahr 2017 wurde der Betrag auf 1,95 Millionen Euro erhöht. Die Personalausstattung des Zentrums verdoppelte sich 2017 auf 14,5 Vollzeitäquivalente. Für das Jahr 2018 wurde die Einstellung von weiteren 16 Mitarbeitern genehmigt.

In der nationalen Cybersicherheitsstrategie (2015-2017) sind 12 Maßnahmen enthalten, die während der Laufzeit der Strategie umgesetzt werden sollten. Im Mai 2018 waren vier Maßnahmen vollständig, vier teilweise und vier überhaupt nicht umgesetzt.

Die EU-Richtlinie zur Netz- und Informationssicherheit zielt darauf ab, die Widerstandsfähigkeit wichtiger Netz- und Informationssysteme zu stärken. Eine Bewertung des Fortschritts in Irland im Hinblick auf jede der drei Säulen dieser Richtlinie erbrachte folgendes Ergebnis:

- *Säule 1: Verbesserung der Kapazitäten der EU-Mitgliedstaaten im Bereich Cybersicherheit.* Teilweise umgesetzt: Die strukturellen Anforderungen wurden angegangen, aber bei der strategischen Planung gibt es noch Lücken.
- *Säule 2: Erleichterung der Zusammenarbeit der EU-Mitgliedstaaten im Bereich Cybersicherheit.* Umgesetzt.
- *Säule 3: Einführung von Sicherheitsmaßnahmen und der Pflicht zur Meldung von Sicherheitsvorfällen in wichtigen Sektoren.* Teilweise umgesetzt: Im Zusammenhang mit der Ermittlung von kritischen Netz- und

Informationssystemen, der förmlichen Benennung von Einrichtungen als Betreiber wesentlicher Dienste und dem Management der Anbieter digitaler Dienste gibt es weiterhin Handlungsbedarf.

Mit der Entscheidung der Regierung zur Einrichtung des nationalen Zentrums für Cybersicherheit (Juli 2011) wurde gleichzeitig auch die Bildung eines ressortübergreifenden Ausschusses gebilligt, der die Strategien festlegen und umsetzen sollte, um die Herausforderungen der Cybersicherheit in Irland zu bewältigen. Obwohl sich die Gruppe zwischen 2013 und 2015 fünf Mal traf, lag das Protokoll von nur einer Sitzung zur Überprüfung vor. Seit 2015 ist der Ausschuss nicht mehr zusammengekommen.

Der Umsetzungsplan für die nationale Strategie für Cybersicherheit enthält die Verpflichtung, einen jährlichen Bericht zu veröffentlichen und Ende 2017 eine formale Folgenabschätzung der Arbeit des Ausschusses durchzuführen. Diese stehen noch aus, obwohl die Arbeit des Zentrums im Jahresbericht des Ministeriums beschrieben wird.

Eine Bewertung der Leistung des Zentrums wurde vom Ministerium formell angefordert. Ein Nachweis über die Durchführung einer Bewertung wurde nicht erbracht. Vom Ministerium wurde erklärt, dass die Leistungsbewertung der Arbeit des nationalen Zentrums für Cybersicherheit Bestandteil des normalen Leistungsmanagements und der Corporate Governance des Ministeriums ist.

Die Prüfung ergab Folgendes:

- Trotz der wichtigen Funktion, die das nationale Zentrum für Cybersicherheit ausübt, war die Mittelausstattung in den ersten vier Jahren seiner Tätigkeit deutlich geringer als ursprünglich vorgesehen.
- Die allgemeine strategische Ausrichtung des Zentrums ist nicht eindeutig, da es derzeit keinen strategischen Plan gibt.
- Mehr Klarheit ist erforderlich im Hinblick auf die jeweiligen Rollen der an der Aufklärung von Cyberkriminalität und nationalen Sicherheitsvorfällen beteiligten Stellen.
- Die Anforderungen der EU-Richtlinie zur Netz- und Informationssicherheit im Hinblick auf die Entwicklung einer nationalen Strategie müssen noch umgesetzt werden.

- Obgleich Governance-Strukturen festgelegt wurden, ist nicht klar, wie die Governance-Regelungen in der Praxis funktionieren.

Es besteht ein Mangel an Transparenz hinsichtlich der Verfügbarkeit und der Kosten der Ressourcen, die für Cybersicherheit bereitgestellt werden.

Frankreich
Cour des comptes

Zugang zur Hochschulbildung: eine erste Bewertung des Gesetzes über Studienberatung und Studienerfolg

Datum der Veröffentlichung: Februar 2020

Hyperlink zum Bericht: Bericht (in französischer Sprache)

Prüfungsart und -zeitraum

Prüfungsart: Wirtschaftlichkeitsprüfung

Prüfungszeitraum: 2019-2020

Zusammenfassung des Berichts

Prüfungsthema

Das Gesetz über Studienberatung und Studienerfolg (*loi relative à l'orientation et à la réussite des étudiants* – ORE) von 2018 zielte darauf ab, die drei wichtigsten Stufen auf dem Weg junger Menschen in die Hochschulbildung zu verbessern: Beratung und Unterstützung für angehende Studierende, die über einen Abschluss der Sekundarstufe II verfügen, Auswahl des Studiengangs und Erfolg in den ersten Studienjahren. Mit dem Gesetz wurde "*Parcoursup*" eingeführt, eine neue digitale Plattform, die ein Informationsangebot zu verfügbaren Studiengängen und Zugangsvoraussetzungen bereitstellt. Ziel der Plattform ist es, die Übereinstimmung zwischen den Fähigkeiten und Leistungen der Schüler der Sekundarstufe und den Inhalten der Hochschullehrpläne zu stärken.

In den ersten zwei Jahren des ORE-Gesetzes wurde der erste Schritt auf dem Weg zur Umgestaltung des Hochschulzugangs vollzogen. Trotz zahlreicher Einschränkungen war die Einführung von "*Parcoursup*" reibungslos verlaufen, obgleich es noch an Sicherheits- und Nachhaltigkeitsgarantien mangelte und eine bessere Datennutzung angesichts der Bedeutung dieser Daten möglich gewesen wäre.

Das ORE-Gesetz wurde verabschiedet, um zwei große Probleme in der Bildungspolitik zu lösen. Das erste war die hohe Abbrecherquote unter den Hochschulstudenten. Das zweite Problem bestand darin, dass die alte digitale Plattform zu einer tief sitzenden Unzufriedenheit geführt hatte, weil das Verfahren mit einer Zufallsauswahl endete.

Für die ORE-Reform wurden Fördermittel in Höhe von 867 Millionen Euro über fünf Jahre bereitgestellt. Die Reform beruhte auf dem Konzept eines "-3/+3"-Kontinuums. Diesem liegt die Annahme zugrunde, dass der Prüfungserfolg umso größer ist, je besser die Schüler der Sekundarstufe II über den Inhalt der Hochschulstudiengänge informiert sind, da sie dann Kurse wählen würden, die ihren Fähigkeiten und Zielen am besten entsprechen. Mit dem ORE-Gesetz sollte das mangelhafte Orientierungsangebot für Schüler der Sekundarstufe II verbessert und dadurch die Zahl der Studiengangwechsel verringert werden, die nach Schätzungen des Rechnungshofs allein im ersten Studienjahr Kosten von fast 550 Millionen Euro pro Jahr verursachen.

Die Prüfer führten eine erste Bewertung des Hochschulzugangs im Zusammenhang mit dem ORE-Gesetz durch und untersuchten die Probleme, die sich beim Betrieb der Plattform im Hinblick auf die IT-Sicherheit ergeben.

Das Informationssystem war durch eine steigende Auslastung gekennzeichnet (Aufnahme aller Hochschulstudiengänge im Jahr 2020 und ein rasanter Anstieg der Nutzerzahlen innerhalb weniger Jahre). Dieser Umstand war Ausdruck des überstürzten Wechsels von der vorherigen Plattform zu "*Parcoursup*", ohne dass die Architektur geändert wurde, wodurch sich erhebliche Risiken in Bezug auf Qualität, Kontinuität, Anpassungsfähigkeit und Weiterentwicklung des Dienstes ergaben. Die Schwächen des Systems in den Bereichen Sicherheit, Leistung und Belastbarkeit waren nicht behoben worden. Der rasche Aufbau von "*Parcoursup*" war möglich, weil die Plattform in der Beta-Version von einer kleinen Gruppe hochqualifizierter und motivierter Personen verwaltet wurde, wenngleich dieser Ansatz auch bedeutete, dass es an strategischer Ausrichtung und zufriedenstellender Governance fehlte.

Die Prüfer beurteilten die Qualität des Informationssystems und die Leistungsfähigkeit der neuen Plattform "*Parcoursup*". Die Plattform wurde im Rahmen des ORE-Gesetzes mit dem Ziel eingerichtet, die Qualität der Zuweisung von Bewerbern zu Hochschulstudiengängen zu verbessern und damit die Absolventenquote zu erhöhen.

Prüfungsfeststellungen

Auch wenn "*Parcoursup*" zufriedenstellend funktionierte, war die Plattform IT-Risiken ausgesetzt, die es zu reduzieren galt. Es fehlten Garantien für die Sicherheit und Nachhaltigkeit der Plattform und bei der Datennutzung bestand Verbesserungsbedarf.

Ein altes Informationssystem

Die "*Parcoursup*"-Plattform, die die Schwerfälligkeit und Anfälligkeit ihres Vorgängersystems "*Admission Post-Bac*" (APB) zusammen mit vielen unbehobenen Risiken geerbt hatte, bot nur wenige Neuerungen. Das Informationssystem, das die strukturelle Basis von "*Parcoursup*" bildet, wurde direkt von der früheren Plattform übernommen. Als neues Zuweisungs-Tool angepriesen, war das Herzstück des Informationssystems seit der APB-Plattform jedoch nur geringfügig verändert worden. Tatsächlich waren über 72 % der Informationsinfrastruktur unverändert geblieben, da nur knapp 30 % des APB-Codes neu geschrieben worden waren.

Das IT-Fundament der Plattform war in den frühen 2000er-Jahren für die Bearbeitung von etwa einer Million Bewerbungen für rund 100 000 Studienplätze pro Jahr ausgelegt, der Umfang des Informationssystems wurde jedoch erweitert, um den jährlichen Eingang von etwa 10 Millionen Bewerbungen für rund eine Million Studienplätze zu bewältigen. "*Parcoursup*" ist somit ein altes Tool unter neuem Namen. Mit der steigenden Auslastung kamen Fragen auf, ob die Plattform in der Lage ist, ihren beabsichtigten Zweck zu erfüllen.

Ein unzureichend dokumentiertes Informationssystem

Trotz der Bemühungen des Ministeriums um Transparenz war der Quellcode von "*Parcoursup*" noch zu 99 % geschlossen. Anhand des kleinen veröffentlichten Teils ließ sich die Zuweisung der Bewerber zu Studiengängen nur schwer nachvollziehen, beurteilen und bewerten.

Wie auch das vorherige System war "*Parcoursup*" ein unzureichend dokumentiertes operatives Informationssystem. Die Ergebnisse der Prüfung des Codes legten nahe, dass die Anwendung von geringer Qualität und mit hohem Risiko behaftet war, und bei der Prüfung wurden zahlreiche kritische Verstöße festgestellt. Das System war qualitativ schlechter als andere Softwareprogramme ähnlichen Alters und wies ein hohes Absturzrisiko auf.

Bei "*Parcoursup*" wird sowohl offener als auch geschlossener Quellcode verwendet. Der offene Code wies eine weitaus höhere Rate an kritischen Verstößen auf als der geschlossene Code, was mit dem Risiko einer Betriebsstörung einherging. Auch war die

Plattform nicht sicher gegenüber Angriffen von Hackern (Sicherheitsüberprüfung des Quellcodes im Juli 2018). Dennoch gab das Ministerium Ende 2019 bekannt, dass ein Zertifizierungsverfahren für den Code von "*Parcoursup*" eingeleitet worden war.

Die vorhandene Dokumentation des Quellcodes war weder kohärent noch umfassend. Der Code von "*Parcoursup*" war ungewöhnlich komplex. Die Prüfer waren der Ansicht, dass der Quellcode umstrukturiert werden sollte, um die Anzahl der komplexen Komponenten zu reduzieren.

Die Architektur des Informationssystems "*Parcoursup*" war mit vielen Risiken behaftet; die Verwaltung der Datenbank war veraltet, das heißt sie erfolgte noch manuell. Die Schwachstelle des Systems lag in seiner starken Abhängigkeit von der Verfügbarkeit und Wachsamkeit des Bedieners. Das Ministerium räumte ein, dass mit der Architektur von "*Parcoursup*" hohe Risiken verbunden waren, die ohne eine Weiterentwicklung der Anwendung nicht behoben werden könnten.

Das Informationssystem "*Parcoursup*" war unzureichend dokumentiert und stützte sich im Wesentlichen auf das Fachwissen der Mitarbeiter der nationalen Regierungsbehörde (*Service à Compétence Nationale* – SCN). Zu Dokumentationszwecken werden Erläuterungen in die Datenbank geschrieben, die den Kern des Systems bildet, wodurch die Pflege und Weiterentwicklung des Informationssystems sowie die Nutzung der Daten erschwert wurden. Um die auf der Plattform gespeicherten Nutzerinformationen einfach extrahieren und auswerten zu können, musste zuvor eine eingehende Untersuchung durchgeführt werden. Da keine strukturierte technische Dokumentation vorlag, war der SCN bei der Erfüllung seiner strategischen Aufgaben vollständig vom Leiter des IT-Zentrums abhängig.

Sicherheitsstrategie – es besteht Verbesserungsbedarf

Angesichts der Sensibilität der im System erfassten personenbezogenen Daten ist "*Parcoursup*" im Hinblick auf die Sicherheit eine echte Herausforderung. Grundsätzlich müssen alle Organisationen, die ein Informationssystem verwalten, über ein förmliches schriftliches Sicherheitskonzept für die Informationssysteme verfügen. Obwohl "*Parcoursup*" vom französischen Premierminister als wichtiger Dienstleister anerkannt wurde, war ein solches Sicherheitskonzept für die Plattform nicht vorhanden. Es bestand sofortiger Handlungsbedarf, um dieses Konzept zu erarbeiten.

Jedes Team von "*Parcoursup*" verfügte über einen Informationssicherheitsbeauftragten, der dem IT-Zentrum zugeordnet war. Es hätte

bewährten Verfahren entsprochen, die Informationssicherheitsbeauftragten direkt dem Direktor des SCN zu unterstellen, um ihre Unabhängigkeit zu gewährleisten.

Noch Mitte 2019 war man dabei, die Konformität von "*Parcoursup*" mit der DSGVO herzustellen. Einige Maßnahmen standen noch aus, insbesondere die notwendige formale Festlegung der verschiedenen Verarbeitungsverfahren. Der Schutz personenbezogener Daten war nach wie vor unzureichend, und es wurden noch immer zu umfassende personenbezogene Daten gespeichert.

Die für "*Parcoursup*" zuständige Stelle war sowohl dem Projektleiter von "*Parcoursup*", der vom Ministerium ernannt worden war, als auch der Abteilung für Ausbildungsstrategie und studentische Angelegenheiten der Generaldirektion für höhere Bildung und berufliche Integration unterstellt, wodurch sich Loyalitätskonflikte ergaben. In wöchentlichen Sitzungen wurden praktische Fragen zum Informationssystem "*Parcoursup*" behandelt. Auch wenn diese Organisationsform den Vorteil hatte, dass im Hinblick auf die tägliche Steuerung der Studentenströme schneller reagiert werden konnte, blieb "*Parcoursup*" mit ihr ohne eine strategische Ausrichtung.

Schließlich war das System nicht ausreichend transparent. Es erlaubte trotz des enormen Potenzials keine optimale Nutzung der auf der Plattform verwalteten Daten. Die Nutzung dieses Potenzials hätte mit ziemlicher Sicherheit zu Leistungssteigerungen geführt.

Schlussfolgerungen und Empfehlungen

Den zuständigen Behörden war es mit der digitalen Plattform, auf der alle Bildungsprogramme zusammengeführt werden, gelungen, einen zentralen Zugang zu allen postsekundären Studiengängen zu schaffen, um auf die Generalisierung der Hochschulbildung zu reagieren. Das Vorgängersystem war in aller Eile zu "*Parcoursup*" umgebaut worden, jedoch ohne dass wesentliche strukturelle Änderungen vorgenommen wurden. Die Schwachstellen des Informationssystems in Bezug auf Sicherheit, Leistung und Belastbarkeit waren demnach nicht behoben worden, obwohl der Anstieg der Belastung angesichts dessen, dass letztendlich alle grundständigen Studiengänge einbezogen werden sollten, sich zwangsläufig fortsetzen würde. Auch war das System unzureichend dokumentiert, mit einem etwas hausbackenen Ansatz in der IT-Entwicklung, und seine ungewöhnliche Komplexität erhöhte die Fehlerrisiken bei operativen Änderungen. Die Plattform war daher mit erheblichen Risiken in Bezug

auf die Qualität und Kontinuität öffentlicher Dienstleistungen und die Sicherheit personenbezogener Daten behaftet.

Der *Cour des comptes* sprach die folgenden Empfehlungen aus:

- Das IT-Team des SCN sollte personell besser ausgestattet werden und die ORE-Mittel sollten umgeschichtet werden, um die personellen und finanziellen Ressourcen der Unterdirektion für Informationssysteme und statistische Forschung aufzustocken.
- Das Informationssystem sollte langfristig ausgelegt werden, indem seine dringendsten Mängel behoben, seine Architektur modernisiert oder neu entwickelt und die primären Datenbanken des Vorgängersystems sowie von "*Parcoursup*" in systematischer und strukturierter Weise dokumentiert werden.
- Für das Informationssystem "*Parcoursup*" sollte ein Sicherheitskonzept erarbeitet werden.
- Es sollte ein gemeinsames Lenkungsgremium für das Ministerium für Bildung und Jugend und das Ministerium für Hochschulbildung, Forschung und Innovation eingerichtet werden, um die Plattform "*Parcoursup*" zu überwachen und gleichzeitig Mittel aus der ORE-Finanzierung zugunsten von Maßnahmen zur "Orientierung" umzuschichten.

Lettland
Valsts Kontrole

Hat die öffentliche Verwaltung alle Möglichkeiten für ein wirtschaftliches Management der IKT-Infrastruktur genutzt?

Datum der Veröffentlichung: Juni 2019

Hyperlink zum Bericht: Zusammenfassung des Berichts (in englischer Sprache)

Prüfungsart und -zeitraum

Prüfungsart: Wirtschaftlichkeitsprüfung

Prüfungszeitraum: 2017-2019

Zusammenfassung des Berichts:

Prüfungsthema

Der lettische Rechnungshof führte eine Wirtschaftlichkeitsprüfung zur Untersuchung der Wirtschaftlichkeit der öffentlichen IKT-Infrastruktur durch. Mit dieser Prüfung sollte untersucht werden, ob die öffentliche Verwaltung beim wirtschaftlichen Management der IKT-Infrastruktur einem gemeinsamen Ansatz folgte und ob die Einrichtungen die Vorteile der Zentralisierung bewertet hatten. Darüber hinaus wurde die Sicherheit der Rechenzentren als ein wichtiger Aspekt bei der Bewertung von Optionen für die weitere Optimierungsplanung ermittelt.

Das Zögern der Behörden, die IKT-Infrastruktur zumindest auf der Ebene eines Ministeriums zentral zu verwalten, hatte dazu geführt, dass mehrere Serverräume eingerichtet wurden, wodurch sich die Instandhaltungskosten deutlich erhöhten. Bei der Prüfung der vier Ministerien wurde festgestellt, dass ihre 22 Abteilungen 38 Rechenzentren nutzten. Der nationale Rechnungshof deckte auf, dass Informationssysteme von hoher und sogar von nationaler Bedeutung in Räumlichkeiten mit einem unzureichenden Sicherheitsniveau untergebracht waren. Durch die Optimierung der Anzahl der Serverräume wäre nicht nur eine Senkung der IKT-Ausgaben möglich, sondern könnte auch ein ausreichendes Sicherheitsniveau zu

geringeren Kosten erreicht werden. Inzwischen waren in den Einrichtungen bereits Hochsicherheitsserverräume vorhanden, die aber nicht voll ausgelastet waren.

Hauptprüfungsgegenstand

Ziel der Prüfung war es, festzustellen, ob alle Voraussetzungen für ein einheitliches Management der IKT-Infrastruktur geschaffen und umgesetzt worden waren, um eine wirtschaftlichere und sicherere Nutzung der IKT-Ressourcen zu fördern.

Prüfungsfeststellungen und Schlussfolgerungen

IKT-Steuerung und -Optimierung

- Für die IKT-Entwicklung und Optimierung gab es weder auf nationaler Ebene noch in den Ministerien eine langfristige Zukunftsvision. Die Ministerien und ihre Abteilungen optimierten die IKT-Infrastruktur entsprechend ihrem Verständnis und ihrer Kapazitäten.

Zwischen 2011 und 2017 stiegen die Gesamtkosten der geprüften Einrichtungen für die Instandhaltung der IKT-Infrastruktur von 17 auf 20 Millionen Euro pro Jahr. Die Einrichtungen hatten keine Verfahren eingerichtet, um regelmäßig zu bewerten, ob es kostengünstiger wäre, die Instandhaltung der IKT-Infrastruktur selbst durchzuführen, sie in Zusammenarbeit mit einer anderen Einrichtung durchzuführen oder die IKT-Instandhaltung auszulagern. Weder die Zentralisierung noch die Dezentralisierung der IKT-Infrastruktur wird als Ziel an sich betrachtet, jedoch ist eine Analyse der spezifischen Situation und der Alternativen notwendig, um Klarheit bezüglich der bestehenden Kosten und möglicher Alternativen zu erlangen.

IKT-Sicherheit

- Im Rechtsrahmen waren die Sicherheitsanforderungen an die IKT-Infrastruktur nicht eindeutig in einem logischen System in Abhängigkeit von der Relevanz der zu verarbeitenden Informationen festgelegt. Detaillierte technische Anforderungen für den Schutz von IKT-Rechenzentren lagen nicht vor.

- Die mangelhaften Sicherheitsanforderungen hatten zur Folge, dass kostspielige Schutzmaßnahmen getroffen wurden oder der Schutz von Informationen, die von nationaler Bedeutung waren, eben nicht gewährleistet wurde. So kam es sogar vor, dass wichtige Informationssysteme in Rechenzentren mit geringer Sicherheitsstufe untergebracht waren.

- In den meisten Serverräumen wurden Sicherheitsbedrohungen festgestellt – die Rechenzentren waren nicht ausreichend gegen unbefugten physischen Zutritt und Umweltrisiken geschützt. Für die Abwehr von Sicherheitsbedrohungen waren je nach gewähltem Ansatz Mittel in Höhe von mindestens 247 000 bis 765 000 Euro erforderlich. Folgende Ansätze wurden verfolgt: 1) die Verbesserung der Serverräume, in denen wichtigere Informationssysteme untergebracht waren, und die Sicherstellung, dass wichtige IKT-Ressourcen in Rechenzentren mit höherer Sicherheitsstufe gespeichert werden, oder 2) die Verbesserung aller vorhandenen Serverräume. Letzterer Ansatz würde jedoch Investitionen erfordern, die die Prüfer nicht rechtfertigen könnten, sofern nicht die Anzahl der Rechenzentren verringert würde.

Der Rechtsrahmen war lückenhaft, da keine detaillierten Sicherheitsanforderungen für die IKT-Infrastruktur vorlagen. So gab es zum Beispiel Anforderungen an verschiedene Kriterien in Verbindung mit der logischen Sicherheit, aber keine Kriterien für die physische und ökologische Sicherheit der Infrastruktur, was sich auch auf die Verfügbarkeit der Systeme und den Datenschutz auswirkt. Wenngleich in den öffentlichen politischen Planungsdokumenten auf die Bedeutung der Sicherheit der IKT-Infrastruktur sowie auf die Notwendigkeit ihrer Stärkung hingewiesen wurde, waren von keiner Seite spezielle Maßnahmen in dieser Hinsicht geplant. Das Fehlen einer klaren, nachvollziehbaren und logischen Differenzierung der Sicherheitsanforderungen barg die Gefahr, dass für die Verarbeitung von Informationen gleicher Bedeutung und Wichtigkeit innerhalb des Landes unterschiedliche Sicherheitsanforderungen gelten.

Die Sicherheit im digitalen Raum wurde vom Staat zentral überwacht, und der Staat reagierte auf Vorfälle, die sich dort ereigneten, aber die Verantwortung für die Implementierung der Sicherheit der IT-Infrastruktur wurde den jeweiligen Leitern der einzelnen Institutionen übertragen. Somit ergaben sich große Unterschiede im Verständnis der Einrichtungen im Hinblick auf Aspekte der IKT-Sicherheit, die Beurteilung der Bedeutung der verarbeiteten Informationen und die den Einrichtungen zur Bewältigung von IKT-Sicherheitsproblemen zur Verfügung stehenden Ressourcen.

Für diese Prozesse war ein System zur regelmäßigen Überwachung erforderlich, um die gesamte öffentliche Verwaltung als ein einziges System unabhängig und nach einheitlichen Kriterien zu bewerten, divergierende Vorgehensweisen zu erkennen und ihnen durch die Ermittlung gängiger Risiken entgegenzuwirken und um vorbeugende Maßnahmen zur Abmilderung dieser Risiken zu planen.

Litauen
Valstybės Kontrolė

Verwaltung kritischer staatlicher Informationsressourcen

Datum der Veröffentlichung: Juni 2018

Hyperlink zum Bericht: Zusammenfassung des Berichts (in englischer Sprache)
Bericht (in litauischer Sprache)

Prüfungsart und -zeitraum

Prüfungsart: Wirtschaftlichkeitsprüfung

Prüfungszeitraum: 2014-2017

Zusammenfassung des Berichts

Prüfungsthema

Wichtige staatliche Funktionen, wie etwa die Verwaltung der öffentlichen Finanzen, die Steuerverwaltung und die Gesundheitsversorgung, werden ausgeübt unter Nutzung kritischer staatlicher Informationsressourcen – also kritischer elektronischer Informationen. Ein Verlust von kritischen Informationen oder die Nichtverfügbarkeit entsprechender Informationssysteme hätte möglicherweise schwerwiegende Folgen für die öffentliche Sicherheit, das Gemeinwohl und die Wirtschaft. Bei den vom litauischen Rechnungshof von 2006 bis 2016 durchgeführten Bewertungen des allgemeinen IT-Managements wurden wiederkehrende Probleme im IT-Management (Planung, Definition der Informationsarchitektur, Organisationsstruktur, Änderungen, Sicherstellung der Geschäftskontinuität, Datensicherheit, Überwachung und Bewertung des IT-Managements) ermittelt. Der Rechnungshof führte eine Prüfung kritischer staatlicher Informationsressourcen durch, um die Verwaltung und die Sicherheit dieser Ressourcen zu bewerten und Verbesserungsmaßnahmen anzuregen.

Ziel der Prüfung war die Bewertung der Verwaltung (der allgemeinen Steuerung) sowie des Reifegrads kritischer staatlichen Informationsressourcen und die Aufdeckung systembedingter Probleme.

Der Rechnungshof bewertete den Reifegrad des IT-Managements in 12 Organisationen des öffentlichen Sektors[64], die 44 staatliche Informationssysteme der Klasse 1 verwalteten. Die Prüfung wurde gemäß den Bestimmungen der öffentlichen Finanzkontrolle und den Internationalen Normen für Oberste Rechnungskontrollbehörden durchgeführt. Die Bewertung erfolgte gemäß der COBIT-Methodik[65] in den folgenden besonders risikobehafteten Bereichen: IT-Strategieplanung, Festlegung der Informationsarchitektur, IT-Risikomanagement, Änderungsmanagement, Sicherstellung der unterbrechungsfreien Leistungserbringung, Systemsicherheit, Datenverwaltung, Überwachung und Bewertung von IT-Aktivitäten, Sicherstellung des IT Managements. Die Bewertung der Prozesse umfasste das IT-Management auf Organisationsebene und auf nationaler Ebene sowie das Zusammenspiel dieser Managementebenen.

Prüfungsfeststellungen

Im Hinblick auf die Veränderungen des Reifegrads der Verwaltung kritischer staatlicher Informationsressourcen waren positive Entwicklungen erkennbar. Angesichts der wachsenden Cyberbedrohungen waren die zu beobachtenden Fortschritte jedoch zu langsam und es ergab sich die Notwendigkeit, die Sicherheit dieser Ressourcen zu erhöhen. Dies war auf die folgenden Mängel zurückzuführen.

- Das System zur Ermittlung kritischer staatlicher Informationsressourcen war nicht wirksam genug, um die Implementierung von Sicherheitslösungen zu ermöglichen, die dem tatsächlichen Bedarf entsprechen:
  - Den Bewertungen zum Nachweis der Kritikalität staatlicher Informationsressourcen mangelte es an Objektivität, Änderungen wurden nicht immer Neubewertungen unterzogen, dieser Prozess wurde nicht auf

[64] Staatliche Steuerinspektion, staatliches Zentrum für Register, Ministerium für Informationstechnologie und Kommunikation, Verwaltung des staatlichen Sozialversicherungsfonds, staatliches Informationszentrum für Landwirtschaft und ländliches Gewerbe, Zentrum der Zollinformationssysteme, staatliches Lebensmittel- und Veterinäramt, Parlament (Seimas) der Republik Litauen, Finanzministerium, Ausschuss für die Entwicklung der Informationsgesellschaft, staatlicher Patientenfonds, staatliches Forstamt.

[65] COBIT (*Control Objectives for Information and Related Technologies* – Kontrollziele für Informations- und verwandte Technologien) ist ein Standard der ISACA, einer internationalen Organisation, die bewährte Verfahren für das IT-Management festlegt.

nationaler Ebene überwacht und mit den Richtlinien zur Bestimmung der Kritikalität wurde keine wirksame Umsetzung sichergestellt.

— Das System zur Ermittlung kritischer staatlicher Informationsressourcen und kritischer Informationsinfrastrukturen war nicht standardisiert; Ressourcen und Infrastrukturen wurden je nach Bedeutung der Informationen und Dienste auf unterschiedliche Weise ermittelt, wodurch der Prozess der Ermittlung dieser Ressourcen erschwert wurde.

— Es war keine nationale Informationsarchitektur entwickelt worden, um die staatlichen Informationssysteme und ihre Zusammenhänge darzustellen, den Umfang der kritischen staatlichen Informationsressourcen aufzuzeigen und fundierte Entscheidungen über die Bedeutung dieser Ressourcen zu treffen.

o Die staatlichen Informationsressourcen hätten unter stärkerer Berücksichtigung der bewährten Verfahren und Standards des IT-Managements verwaltet werden müssen, um die integrierte Verbesserung des IT-Bereichs zu erreichen, was zu schnelleren Fortschritten bei der Verwaltung der kritischen staatlichen Informationsressourcen beitragen würde:

— Die IT-Planung war nicht nachhaltig: Die geplanten IT-Tools wurden in unterschiedlichen Dokumenten dargestellt, es fehlte ein systematischer Ansatz aufgrund einer übermäßig hohen Anzahl von Strategiedokumenten, was es schwierig machte, die wichtigsten Prioritäten zu ermitteln und Ressourcen bereitzustellen, um die größten Bedrohungen zu bewältigen.

— Durch die IT-Überwachung wurde nicht sichergestellt, dass die Organisationen die Wirtschaftlichkeit von IT-Vorgängen messen und die von den Verwaltern der kritischen staatlichen Informationsressourcen durchgeführten Prüfungen den tatsächlichen Reifegrad des IT-Managements aufzeigen. Das staatliche IT-Management wurde nicht auf nationaler Ebene überprüft, und Probleme im Zusammenhang mit dem IT-Management wurden nicht systematisch analysiert. Zwar wurde extra ein System zur Überwachung der Übereinstimmung der staatlichen Informationsressourcen mit den Anforderungen der elektronischen Informationssicherheit geschaffen, um die Einhaltung der Sicherheitsvorschriften zu erleichtern, jedoch wurden die Funktionen dieses Systems nicht ausreichend genutzt.

o Die Maßnahmen, mit denen die Widerstandsfähigkeit kritischer Informationsressourcen gegenüber Cyberbedrohungen sichergestellt werden

sollte, waren nicht wirksam genug; daher bestand weiterhin ein Risiko für die Anfälligkeit dieser Ressourcen:

— Die Wirksamkeit der Bewertung von IT-Sicherheitsrisiken musste erhöht werden, da nicht alle einschlägigen Risiken ermittelt wurden und ihre Bewertungsmethodik nicht den neuesten Verfahren des IT-Management entsprach; die zeitgerechte Steuerung nicht hinnehmbarer Risiken war nicht gewährleistet.

— Von organisatorischen Sicherheitsmaßnahmen, die geeignet sind, Cyberbedrohungen zu verringern, wurde nicht systematisch Gebrauch gemacht. Unzureichende Sicherheitsprüfungen, lückenhafte Schulungen der Mitarbeiter während der Entwicklung, Nachrüstung und Änderung der Informationssysteme; nicht verwaltete sichere Softwarekonfigurationen und -upgrades sowie die unsachgemäße Verwaltung von Dateien zur Gewährleistung der IT-Geschäftskontinuität und von Backup-Dateien bedrohten die Wiederherstellung des Geschäftsbetriebs; Messungen der Sicherheitsleistung waren unzureichend und trugen nicht zur Verbesserung der Sicherheit bei.

Schlussfolgerungen

Im Durchschnitt erreichte das IT-Management der in den letzten zehn Jahren geprüften öffentlichen Stellen den ersten von fünf Reifegraden[66] und lag zum Zeitpunkt der Erstellung des Berichts bei einem Wert von 1,7. Dieser niedrige Reifegrad der kritischen staatlichen Informationsressourcen wies auf Schwachstellen bei der Ausgestaltung und Umsetzung der Politik im Bereich der staatlichen Informationsressourcen hin, die die Anfälligkeit dieser Ressourcen erhöhte. Um die Sicherheit dieser Ressourcen zu erhöhen, muss der Mechanismus zur Verwaltung der staatlichen Informationsressourcen verbessert werden, damit er so weit wie möglich den bewährten Verfahren entspricht. Die Prüfer stellten außerdem fest, dass die Maßnahmen zur Gewährleistung der Widerstandsfähigkeit der kritischen Informationsressourcen gegenüber Cyberbedrohungen nicht wirksam genug waren. Aus diesem Grund muss die Bewertung der IT-Sicherheitsrisiken wirksamer gestaltet werden, indem Sicherheitsprüfungen bei der Einrichtung und Modernisierung von

[66] In Anlehnung an die COBIT-Methodik.

Informationssystemen und die Schulung des Personals stärker in den Fokus gerückt werden.

Weitere Berichte in diesem Bereich

Titel des Berichts:	"Is Cybercrime Combatted Effectively"
Hyperlink zum Bericht:	Zusammenfassender Bericht (in englischer Sprache) Bericht (in litauischer Sprache)
Datum der Veröffentlichung:	2020

Titel des Berichts:	"Environment of Cyber Security in Lithuania"
Hyperlink zum Bericht:	Zusammenfassung des Berichts (in englischer Sprache) Bericht (in litauischer Sprache)
Datum der Veröffentlichung:	2015

Ungarn
Állami Számvevöszék/State Audit Office

Prüfung zum Datenschutz – Prüfung des nationalen Datenschutzrahmens und bestimmter vorrangiger Datensätze im Rahmen der internationalen Zusammenarbeit

Datum der Veröffentlichung: März 2017

Hyperlink zum Bericht: Bericht (in ungarischer Sprache)

Prüfungsart und -zeitraum

Prüfungsart: Compliance

Prüfungszeitraum: 2011-2015

Zusammenfassung des Berichts

Prüfungsthema

Die Sicherheit der nationalen Datenbestände ist in jedem Land von grundlegendem Interesse für die Gesellschaft, um nationale Werte zu bewahren und zu schützen. Demzufolge ist die Verbesserung der Sicherheit personenbezogener und öffentlicher Daten in den nationalen Datenbeständen Ungarns von wesentlicher Bedeutung, um das Vertrauen der Bürgerinnen und Bürger in den Staat zu stärken und das kontinuierliche und reibungslose Funktionieren der öffentlichen Verwaltung sicherzustellen. Der Schutz der Daten und das Sicherheitsnetz, das durch den Rechtsrahmen für seine Durchsetzung gewährleistet wird, sind deshalb von zentraler Bedeutung für die Gesellschaft.

Im Bereich des Datenschutzes spielen die öffentlichen Verwaltungsbehörden eine Schlüsselrolle bei der Verwaltung der größten und sensibelsten Datenregister, die zu den nationalen Datenbeständen gehören. Die Verantwortlichen für die Datenverarbeitung in den Registern arbeiten bei der Ausübung ihrer Tätigkeit eng zusammen. Sie übertragen regelmäßig Register, die große Datenmengen enthalten, und müssen dabei die gesetzlichen Datenschutzanforderungen beachten. Der Einsatz elektronischer Informationssystemen bei der Verwaltung und Verarbeitung von Daten

ist mittlerweile unverzichtbar, und der ordnungsgemäße und zuverlässige Betrieb dieser Systeme muss durch zweckmäßig konzipierte und ordnungsgemäß durchgeführte Kontrollen sichergestellt werden.

Der ungarische Rechnungshof legt bei seinen Prüfungen größten Wert auf den Datenschutz. Er führte von 2011 bis 2015 umfassende Prüfungen zum Datenschutz durch und veröffentlichte seinen Bericht im ersten Quartal 2017. Die Prüfungsarbeit deckte auch Aspekte parallel laufender internationaler Prüfungen ab, die in Zusammenarbeit mit der EUROSAI-Arbeitsgruppe IT-Prüfung durchgeführt wurden und vornehmlich auf die Einhaltung der bestehenden Richtlinien der Europäischen Union ausgerichtet waren.

Der Zweck der Compliance-Prüfung zum Datenschutz in Ungarn bestand darin, zu beurteilen, ob in Ungarn ein rechtlicher und operativer Rahmen für den Datenschutz geschaffen worden war und ob die wichtigsten mit der Datenverwaltung befassten Stellen die Anforderungen an die sichere Datenverwaltung und die Auslagerung der Datenverarbeitung erfüllten. Der Schwerpunkt der Prüfung lag insbesondere auf dem Schutz personenbezogener Daten und nationaler Datenbestände.

Im Rahmen der Prüfung bewertete der ungarische Rechnungshof die Datenverwaltung von sechs mit der Datenverwaltung befassten Stellen (zum Beispiel: Steuerbehörde, Staatskasse, Krankenversicherung, Rentenzahlung, Bildungsamt, personenbezogene Daten und Adressen, Datensätze zu Fahrzeugen und Strecken und für die Verwaltung strafrechtlich relevanter Daten zuständige Behörden) sowie auch die Tätigkeiten der Datenschutzbehörde und der Behörde für Informationssicherheit.

Besonderes Augenmerk wurde bei der Prüfung auf das Mandat der für die Datenverwaltung zuständigen Stellen gelegt, insbesondere bei der Datenübermittlung an Dritte. Bei der Prüfung der internen Kontrollen der Datenverwaltung und Datenverarbeitung wurde bewertet, ob aktuelle Vorschriften zu den Aufgaben, Verantwortlichkeiten und Kompetenzen, zum Personalmanagement und zu den Abläufen vorhanden sind.

Im Hinblick auf die bei der Datenverwaltung eingesetzten elektronischen Systeme bewertete der Rechnungshof die damit verbundenen Sicherheitsmaßnahmen, einschließlich der Bereiche physischer Schutz, Zugriffsrechte, Protokollierung, Sicherheitsbewertungsverfahren, System- und Kommunikationssicherheit sowie die Einhaltung der Sicherheitsklassifizierung der Organisation insgesamt.

Die Auslagerung der Datenverarbeitung wurde anhand der abgeschlossenen Verträge geprüft, wobei untersucht wurde, ob die für die Datenverwaltung zuständigen Stellen die Auftragsverarbeiter verpflichtet hatten, die Anforderungen an die Datenverarbeitungstätigkeiten in Übereinstimmung mit den gesetzlichen Vorschriften zu erfüllen.

Prüfungsfeststellungen und Schlussfolgerungen

Aufgrund der Prüfung stellte der ungarische Rechnungshof fest, dass die internen Vorschriften der für die Datenverwaltung zuständigen Stellen in Bezug auf Datenverwaltungstätigkeiten den Schutz der nationalen Datenbestände als integralen Bestandteil der nationalen Vermögenswerte in Einklang mit den zwischen 2011 und 2015 geltenden gesetzlichen Bestimmungen gewährleistet haben. Die für die Datenverarbeitung Verantwortlichen hatten die Anforderungen an die sichere Datenverwaltung und die Auslagerung der Datenverarbeitung in der Praxis ordnungsgemäß angewendet. Die Weitergabe von Daten an Dritte erfolgte mit dem entsprechenden Mandat und einer klaren Abgrenzung der Verantwortlichkeiten und Befugnisse.

Im Hinblick auf einige für die Datenverarbeitung Verantwortliche wurde festgestellt, dass die Sicherheitsklassifizierung der elektronischen Systeme und der Organisation insgesamt zwar nicht immer den gesetzlichen Anforderungen entsprach, das Ausmaß der Mängel die Sicherheit der verarbeiteten Daten jedoch nicht wesentlich beeinträchtigte. Auf der Grundlage der im Prüfungsbericht enthaltenen Empfehlungen beseitigten die für die Datenverwaltung zuständigen Stellen die Mängel im Rahmen von Aktionsplänen, die vom ungarischen Rechnungshof genehmigt worden waren.

Der Rechnungshof stellte im Zusammenhang mit der internationalen Prüfung, die parallel in Zusammenarbeit mit der EUROSAI-Arbeitsgruppe IT-Prüfung durchgeführt wurde, fest, dass die ungarische Datenschutzgesetzgebung im Einklang mit der bestehenden EU-Richtlinie steht.

Abschließend kann festgehalten werden, dass der ungarische Rechnungshof mit der Prüfung des Datenschutzes zur verantwortungsvollen Staatsführung und zum Schutz der nationalen Datenbestände beigetragen hat.

Weitere Berichte in diesem Bereich

Titel des Berichts:	"Report – Follow-up audits – Data protection audit – Audit of the domestic data protection framework and certain key data records in the framework of international cooperation"
Hyperlink zum Bericht:	Bericht (in ungarischer Sprache)
Datum der Veröffentlichung:	2020

Niederlande
Algemene Rekenkamer/Court of Audit

Cybersicherheit von kritischen Wasserbewirtschaftungsstrukturen und Grenzkontrollen in den Niederlanden

Datum der Veröffentlichung: März 2019 und April 2020

Hyperlink zu den Berichten: Summary of report on cyber security and critical water structures Report (in englischer Sprache)
Summary of report on cyber security and automated border controls Report (in englischer Sprache)

Prüfungsart und -zeitraum

Prüfungsart: Wirtschaftlichkeitsprüfung

Prüfungszeitraum: 2018-2020

Zusammenfassung des Berichts

Prüfungsthema

Der niederländische Rechnungshof beschloss 2018, die Cybersicherheit in Sektoren zu überprüfen, die für die Gesellschaft von entscheidender Bedeutung sind. Aufgrund seiner langjährigen Erfahrungen in der Prüfung der Einhaltung von Informationssicherheitsvorschriften in der Zentralregierung war der Rechnungshof der Ansicht, dass die Prüfung der *Wirtschaftlichkeit* von Politiken und Maßnahmen in der Praxis einen Mehrwert darstellt. Die ersten beiden geprüften Sektoren waren die Wasserwirtschaft, die für ein Land, das in großen Teilen unter dem Meeresspiegel liegt, lebensnotwendig ist, sowie das automatische Grenzkontrollsystem, das seine Bedeutung dadurch erlangt, dass es sich beim Amsterdamer Flughafen Schiphol um ein internationales Drehkreuz und ein Tor in die Niederlande handelt.

Die Ministerin für Infrastruktur und Wasserwirtschaft wies eine Reihe von Wasserinfrastrukturen, die von der Generaldirektion für öffentliche

Versorgungseinrichtungen und Wasserwirtschaft (die geprüfte Stelle) verwaltet werden, als "kritische Teile" der Wasserwirtschaft aus. Viele Computersysteme, die beim Betrieb der kritischen Wasserinfrastrukturen zum Einsatz kommen, stammen noch aus den 1980er- und 1990er-Jahren, einer Zeit, als Cybersicherheit noch nicht allgemein berücksichtigt wurde. Diese Systeme waren ursprünglich für den eigenständigen Betrieb konzipiert, wurden aber nach und nach mit größeren Computernetzwerken verbunden, um sie beispielsweise fernsteuern zu können. Diese Entwicklung machte die Systeme anfälliger für Cyberbedrohungen.

Die Verteidigungsministerin und der Minister für Justiz und Sicherheit teilen sich die Verantwortung für die Grenzkontrollen, die vom niederländischen Grenzschutz am Flughafen Schiphol durchgeführt werden. Beide Ministerien (die geprüften Stellen) verfügen über IT-Systeme, die vom Grenzschutz genutzt werden. Die Systeme sind für den Flughafenbetrieb unerlässlich und werden genutzt, um hochsensible Daten zu verarbeiten. Damit sind sie ein interessantes Ziel für Cyberangriffe, mit denen Grenzkontrollen sabotiert, ausspioniert oder manipuliert werden sollen.

Bei den Prüfungen wurde untersucht, wie die geprüften Stellen sich auf den Umgang mit Cyberbedrohungen vorbereitet hatten und ob diesbezüglich wirksame Maßnahmen ergriffen worden waren.

Im Rahmen der Prüfungen sollten die folgenden Fragen beantwortet werden:

- Wie *schützen* die geprüften Stellen ihre Systeme vor Cyberbedrohungen und *verhindern* Cyberangriffe?
- Wie *erkennen* die geprüften Stellen Cyberbedrohungen und -angriffe?
- Wie *reagieren* die geprüften Stellen in einer Situation, in der ein Cyberangriff stattfindet?

Ein vorrangiger Schwerpunkt bei beiden Prüfungen war die Wirksamkeit. In enger Zusammenarbeit mit den Prüfern führten ethische Hacker Testangriffe auf kritische Wasserinfrastrukturen und eines der Grenzkontrollsysteme durch. Alle Ergebnisse der Prüfung waren selbstverständlich vor der Veröffentlichung der Berichte redaktionell bearbeitet worden, und es wurden keine technischen Details bekannt gegeben.

Die beiden Prüfungen unterschieden sich hauptsächlich darin, dass sich die Prüfung der Wasserinfrastrukturen darauf konzentrierte, wie die geprüfte Stelle ihre Ziele erreicht hatte, während die Prüfung der Grenzkontrollen auf dem NIST-Cybersecurity-Regelwerk beruhte.

Prüfungsfeststellungen

Zunächst wurde bei beiden Prüfungen festgestellt, dass die geprüften Stellen für Cyberbedrohungen sensibilisiert waren und an der Umsetzung eines diesbezüglichen professionellen Ansatzes arbeiteten.

Im Fall der Wasserinfrastrukturen bestand für die geprüfte Stelle jedoch die Notwendigkeit, ihre Anstrengungen sowohl bei der Aufdeckung als auch bei der Bekämpfung von Cyberbedrohungen zu verstärken, um ihre eigenen Cybersicherheitsziele zu erreichen. Die geprüfte Stelle hatte bereits ein *Security Operations Centre* (SOC) eingerichtet, um Cyberangriffe zu erkennen und abzuwehren. Jedoch war das für Ende 2017 gesetzte Ziel, alle gegen kritische Wasserinfrastrukturen gerichteten Cyberangriffe sofort aufzudecken, bis Herbst 2018 noch nicht erreicht. Damit bestand das Risiko, einen auf eine kritische Wasserinfrastruktur gerichteten Cyberangriff nicht oder zu spät zu erkennen. Außerdem zeigte die Überprüfung, die an einer der kritischen Wasserinfrastrukturen durchgeführt wurde, dass der physische Zugang zu dieser Wasserinfrastruktur durchaus möglich war. Die Hacker konnten sich Zugang zum Kontrollraum verschaffen und fanden sich mit ungesicherten Arbeitsstationen allein. Schließlich hatte die geprüfte Stelle auch kein Szenario für eine durch einen Cyberangriff verursachte Krise entwickelt, und Informationen, wie darauf zu reagieren wäre, fehlten oder waren nicht aktualisiert. Das Vorhandensein aktueller Informationen könnte für eine schnelle und wirksame Reaktion auf eine Krisensituation entscheidend sein.

Im Bereich der Grenzkontrollen waren die Cybersicherheitsmaßnahmen weder angemessen noch zukunftsfähig. Erstens mussten wichtige Grenzkontrollsysteme vor der Inbetriebnahme formell genehmigt werden, um sicherzustellen, dass alle Cybersicherheitsmaßnahmen umgesetzt wurden. Der niederländische Rechnungshof stellte fest, dass zwei der drei Systeme ohne Genehmigung betrieben wurden, was bedeutete, dass nicht gewährleistet war, dass die notwendigen Sicherheitsmaßnahmen vorhanden waren. Zweitens war ein SOC betriebsfähig, mit dem jedoch keines der Systeme direkt verbunden war. Obwohl die generische Infrastruktur mit dem SOC verbunden war, bestand dennoch das Risiko, dass Cyberangriffe unbemerkt blieben oder zu spät erkannt wurden. Drittens wurden die Sicherheitsüberprüfungen nicht regelmäßig durchgeführt. Tatsächlich war nur eines der drei Systeme in der Vergangenheit überprüft worden – und das auch nur in geringem Umfang. Schließlich war, genau wie bei der ersten Prüfung, kein gezieltes Szenario für eine durch einen Cyberangriff verursachte Krise entwickelt worden.

Während der Sicherheitsüberprüfung eines der Systeme, das zuvor noch nie geprüft worden war, fanden ethische Hacker eine Reihe von Schwachstellen. Diese Schwachstellen könnten mit der Hilfe eines böswilligen und unbefugten Insiders ausgenutzt werden, um einen Cyberangriff zu starten und dabei auf Informationen im System zuzugreifen, diese zu kopieren und sogar zu manipulieren. Diese Ergebnisse zeigen, wie wichtig regelmäßige Sicherheitsüberprüfungen sind.

Angesichts der fortschreitenden Automatisierung der Abläufe an den Grenzen sind die Feststellungen aus den Prüfungen besorgniserregend. In naher Zukunft wird eine steigende Anzahl von Grenzkontrollsystemen immer mehr Daten über eine wachsende Menge von Verbindungen verarbeiten. Damit wird sich das Risiko von Cyberangriffen erhöhen; aus diesem Grund war der verwendete Ansatz nicht zukunftsfähig.

Schlussfolgerungen

Im Fall der Wasserinfrastrukturen hinderten ein paar grundlegende Umstände die geprüfte Stelle daran, die letzten Schritte in Richtung Cybersicherheit zu unternehmen. So war zum Beispiel das Ausmaß der Bedrohung unklar, wodurch es schwierig war zu beurteilen, ob die ergriffenen Maßnahmen und die zugewiesenen finanziellen Mittel ausreichend waren. Außerdem hatte die für Cybersicherheit zuständige zentrale Abteilung kein Mandat, notwendige Cybersicherheitsmaßnahmen in den dezentralen Wasserinfrastrukturen umzusetzen. Die Prüfungsempfehlungen wurden in dieser Hinsicht befolgt und halfen der Organisation in der weiteren Entwicklung.

Im Bereich der Grenzkontrollen war eine eindeutige Ursache für das unzureichende Niveau der Cybersicherheit nicht ersichtlich. Die Untersuchungen im Rahmen der Prüfung ergaben vollständige und detaillierte Verfahren und Richtlinien im Hinblick auf die Cybersicherheit sowie ausreichendes Fachwissen und qualifiziertes Personal. Daher lag der Fokus der Prüfungsempfehlungen hauptsächlich darauf, dass jede mögliche Maßnahme tatsächlich umgesetzt wird.

Beide Prüfungen erregten große Aufmerksamkeit im Parlament und in den Medien. Die Prüfungen sensibilisierten für die Bedeutung von Cybersicherheit in Verbindung mit kritischen Infrastrukturen und zeigten den geprüften Stellen auf, wie sie ihre Cybersicherheit verbessern können. Die enge Zusammenarbeit mit der geprüften Stelle war eine grundlegende Voraussetzung, um ihre Situation vollumfänglich zu verstehen und die mit der Untersuchung und Überprüfung der Cybersicherheit verbundenen Risiken zu bewältigen.

Eine dritte Prüfung in dieser Reihe ist ebenfalls geplant. Darüber hinaus ist das Informationssicherheitsniveau der niederländischen Regierung ein Kernelement des jährlichen Compliance-Prüfungszyklus. Im Laufe der Jahre hat der niederländische Rechnungshof festgestellt, dass viele Ministerien im Hinblick auf Maßnahmen für Informationssicherheit Nachholbedarf haben. Der niederländische Rechnungshof nutzt derzeit die Erfahrungen, die er während seiner Cybersicherheitsprüfungen gesammelt hat, um seine Sicht auf die Prüfung der Informationssicherheit zu erweitern, indem er über Dokumente und Richtlinien hinausschaut und die tatsächliche Wirksamkeit von Maßnahmen prüft.

Weitere Berichte in diesem Bereich

Titel des Berichts:	"Staat van de rijksverantwoording 2019", Kapitel 3
Hyperlink zum Bericht:	Bericht (in niederländischer Sprache)
Datum der Veröffentlichung:	2020

Titel des Berichts:	"Focus on digital home working"
Hyperlink zum Bericht:	Bericht (in niederländischer Sprache)
Datum der Veröffentlichung:	2020

Polen
Najwyższa Izba Kontroli

Gewährleistung der Sicherheit des Betriebs von IT-Systemen, die zur Erfüllung öffentlicher Aufgaben eingesetzt werden

Datum der Veröffentlichung: 2016

Hyperlink zum Bericht: Bericht (in polnischer Sprache)

Prüfungsart und -zeitraum

Prüfungsart: Compliance

Prüfungszeitraum: 2014-2015

Zusammenfassung des Berichts

Prüfungsthema

Mit der Prüfung sollte beurteilt werden, ob die in den Systemen der geprüften Stellen zur Umsetzung wichtiger öffentlicher Aufgaben erfassten Daten sicher waren. Die Prüfung erstreckte sich auf sechs Institutionen, die solche wichtigen öffentlichen Aufgaben erfüllten. Im Anschluss an die Analyse wurde in jeder der Institutionen ein maßgebliches IT-System ausgewählt, das dann einer eingehenden Untersuchung unterzogen wurde. Bei der Prüfung wurde die Version 4.1 der COBIT-Methode (Control Objectives for Information and Related Technology – Kontrollziele für Informations- und verwandte Technologien) angewendet.

Diese Prüfung erfolgte im Nachgang zu der 2015 durchgeführten Prüfung der Erfüllung der Aufgaben im Bereich Cybersicherheit durch die öffentlichen Stellen in Polen[67], deren Ergebnisse auf systembedingte Probleme hingedeutet hatten. Die Prüfung von 2016 zeigte unter anderem, dass die staatliche Verwaltung bis dahin keine Maßnahmen ergriffen hatte, um die IT-Sicherheit auf nationaler Ebene zu gewährleisten. Die Prüfer gelangten zu dem Schluss, dass die Aktivitäten der

[67] https://www.nik.gov.pl/kontrole/P/14/043/

öffentlichen Stellen im Zusammenhang mit dem Schutz des Cyberraums nur auf fragmentierte Weise und ohne einen systematischen Ansatz erfolgt waren. In Ermangelung zentraler Regelungen zur Gewährleistung der konkreten Sicherheitsbedingungen für spezifische IT-Systeme, die für die Funktionsfähigkeit des Staates von grundlegender Bedeutung sind, sollte mit der Prüfung untersucht werden, ob die Institutionen, von denen die für die Erfüllung wichtiger öffentlicher Aufgaben eingesetzten IT-Systeme verwaltet werden, sichergestellt haben, dass diese Aufgaben sicher ausgeführt werden konnten.

Eine weitere Systemprüfung im Hinblick auf die Cybersicherheit mit dem Titel "Cybersecurity in Poland" wurde 2019 genehmigt, jedoch sind die Ergebnisse vertraulich.

Prüfungsfragen

Die Teilziele wurden in zwei Bewertungsbereiche unterteilt, um Antworten auf konkrete Fragen zu erhalten.

Im Bereich der unterstützenden IT-Sicherheit wurde auf der Ebene der gesamten Organisation geprüft, ob u. a.

- ein IT-Sicherheitsmanagement durchgeführt wurde;
- Pläne zur Gewährleistung der IT-Sicherheit umgesetzt wurden;
- die IT-Sicherheit geprüft, überwacht und kontrolliert wurde;
- IT-Sicherheitsvorfälle definiert wurden;
- die Informationstechnologie mit kryptografischen Schlüsseln verwaltet wurde;
- ein Schutz vor Schadsoftware und Patching und deren Erkennung implementiert wurden;
- die Netzwerksicherheit gewährleistet wurde.

Im Bereich der Sicherheitsunterstützung wurde auf der Ebene der ausgewählten Systeme untersucht, ob u. a.

- die Identität und Accounts der Nutzer verwaltet wurden;
- Sicherheitstechnologien und sensible Daten geschützt wurden.

Prüfungsfeststellungen und Schlussfolgerungen

Die Informationssicherheitssysteme waren nicht ausgereift genug und nicht weit genug implementiert, um ein ausreichendes Schutzniveau der in den Systemen zur Ausführung wichtiger öffentlicher Aufgaben erfassten Daten zu bieten. Die Informationssicherheitsprozesse liefen ungeordnet und – in Ermangelung von Verfahren – intuitiv ab. Nur eine der sechs geprüften Stellen hatte das Informationssicherheitssystem implementiert, und es muss hinzugefügt werden, dass es bei dessen Betrieb zu erheblichen Fehlern kam. Mit einer Ausnahme hatten in allen geprüften Stellen die Arbeiten zur Gewährleistung angemessener Sicherheitsbedingungen für die in den IT-Systemen verarbeiteten Informationen noch nicht das entsprechende Niveau erreicht, da sie erst kurz zuvor aufgenommen worden waren und sich noch im Anfangsstadium befanden, was auch für die Erarbeitung der erforderlichen formalen Grundlagen galt. Gearbeitet wurde auf der Grundlage von vereinfachten oder informellen Vereinbarungen, die auf bewährten Verfahren oder den bisherigen Erfahrungen der IT-Mitarbeiter beruhten.

Gemäß der Methodik COBIT 4.1 lag der Reifegrad des Prozesses des Informationssicherheitsmanagements in den verschiedenen geprüften Stellen zwischen (1) initial/ad hoc und (3) definiert auf einer Skala von null bis fünf, wobei fünf der Höchstwert war.

Die Verantwortung für die Sicherstellung der IT-Sicherheit in den geprüften Stellen lag beim Sicherheitskoordinator, der in der Praxis jedoch nicht über die Befugnis verfügte, den gesamten Prozess zu steuern. Die anfallenden Aufgaben wurden zudem oft von nur einer einzigen Person ausgeführt. Zwar waren spezialisierte Teams ernannt oder Vereinbarungen mit externen Auftragnehmern geschlossen worden, die notwendige Analyse, ob die erbrachten Leistungen den Sicherheitsbedürfnissen einer Stelle entsprechen, wurde jedoch nicht durchgeführt. Die Einsicht der geprüften Stellen in die Notwendigkeit, die IT-Sicherheit sicherzustellen, war lückenhaft und begrenzt. Die Datensicherheit wurde hauptsächlich als Verantwortung und Domäne der IT-Abteilung und nicht als die aller Organisationseinheiten mit gesetzlich bestimmten Aufgaben angesehen, was die Entwicklung eines kohärenten IT-Sicherheitsmanagementsystems für die gesamte Institution stark behinderte.

Ein qualitätsbezogener Vergleich der Art und Weise, wie die Verpflichtungen zur Gewährleistung der Informationssicherheit auf der Ebene der gesamten Organisationen wie auch auf der Ebene der ausgewählten Systeme erfüllt wurden, ergab, dass die Qualität der Umsetzung im letzteren Fall höher war. Gründe dafür sind möglicherweise die Auswirkungen der praktischen Kenntnisse und der Einbindung des

technischen Personals der mittleren Ebene auf die Gewährleistung der Sicherheit, die verstärkte Nutzung kommerzieller, auf marktüblichen Standards beruhender IT-Systeme innerhalb der öffentlichen Verwaltung und die weiterentwickelten Lösungen zur Gewährleistung der Sicherheit. Durch die Anwendung solcher Lösungen sowie von Erfahrungen aus der Vergangenheit und bewährten Verfahren war es möglich, ein gewisses Maß an Sicherheit beim Betrieb der verschiedenen Systeme unter den Bedingungen begrenzter Ressourcen, organisatorischer Unzulänglichkeiten oder "nicht funktionierender" Vorschriften aufrechtzuerhalten. Dieser Zustand kann jedoch nicht das Ziel sein, denn in Zeiten einer dynamisch wachsenden Bedrohungslage kann die Sicherheit von IT-Systemen nicht auf Maßnahmen beruhen, die ungeordnet gehandhabt werden und nur auf die Bewältigung unmittelbarer Schwierigkeiten ausgerichtet sind.

Prüfungsschlussfolgerungen

Es müssen allgemeine Empfehlungen und Vorschriften für die IT-Sicherheit, die für alle öffentlichen Stellen gelten, auf zentraler Ebene entwickelt und umgesetzt werden. Eine systemische Lösung ist erforderlich, bei der die Ergebnisse von IT-Sicherheitsprüfungen in einer Weise offengelegt werden, die den Bürgerinnen und Bürgern den Zugang zu Informationen über die Tätigkeiten der öffentlichen Stellen ermöglicht, während der Zugang zu Einzelheiten der Maßnahmen und Methoden, die zur Gewährleistung der Sicherheit der verarbeiteten Informationen eingesetzt werden, beschränkt wird.

Weitere Berichte in diesem Bereich

Titel des Berichts:	"Information security management by regional authorities"
Hyperlink zum Bericht:	Bericht (in polnischer Sprache)
Datum der Veröffentlichung:	2019

Titel des Berichts:	"Cybersecurity in Poland (classified information)"
Hyperlink zum Bericht:	*Nicht öffentlich zugänglich*
Datum der Genehmigung:	2019

Titel des Berichts:	"Ensuring the security of IT systems by regional authorities in Podlaskie Voivodeship"
Hyperlink zum Bericht:	Bericht (in polnischer Sprache)
Datum der Veröffentlichung:	2018

Titel des Berichts:	"Prevention and combat of cyber-bullying among children and young people"
Hyperlink zum Bericht:	Bericht (in polnischer Sprache)
Datum der Veröffentlichung:	2017

Titel des Berichts:	"Public bodies' performance of cybersecurity tasks in Poland"
Hyperlink zum Bericht:	Bericht (in polnischer Sprache)
Datum der Veröffentlichung:	2015

Titel des Berichts:	"Implementation of selected requirements on information systems, electronic information exchange and National Interoperability Framework based on the example of some municipality councils and cities with district rights"
Hyperlink zum Bericht:	Bericht (in polnischer Sprache)
Datum der Veröffentlichung:	2015

Portugal
Tribunal de Contas

Prüfung des portugiesischen elektronischen Reisepasses

Datum der Veröffentlichung: 2014

Hyperlink zum Bericht: Bericht (in portugiesischer Sprache)

Prüfungsart und -zeitraum

Prüfungsart: Wirtschaftlichkeitsprüfung

Prüfungszeitraum: 2013

Zusammenfassung des Berichts

Prüfungsthema

Die operative Prüfung des portugiesischen elektronischen Reisepasses (PEP) richtete sich auf die Wirksamkeit der Informationssysteme, die seine Erteilung, Ausstellung und Nutzung unterstützen, insbesondere bei den automatisierten Passagierkontrollen durch das Auslesen biometrischer Daten an den portugiesischen Grenzen[68].

Die wichtigsten Prüfungsziele waren:

- die Überprüfung, dass der portugiesische elektronische Reisepass im Hinblick auf die Erteilung, Ausstellung und Nutzung EU- und nationalen Rechtsvorschriften sowie internationalen Normen und Richtlinien entspricht und dass der nationale Rechtsrahmen angemessen ist;

[68] Der Hof bezieht sich auf die automatischen Grenzkontrollsysteme (ABC-Systeme) von Frontex (Europäische Agentur für die Grenz- und Küstenwache).

- die Untersuchung der Wirksamkeit der wichtigsten Prozesse im Zusammenhang mit dem Lebenszyklus des portugiesischen elektronischen Reisepasses, insbesondere im Hinblick auf die Erteilung, Ausstellung und Nutzung;
- die Untersuchung kritischer Aspekte der Leistung von Informationssystemen, insbesondere der Frage, ob die Sicherheitsanforderungen an die Informationssysteme für den portugiesischen elektronischen Reisepass (SIPEP) erfüllt waren.

Zu den wichtigsten Risikobereichen gehörten:

- physischer Verlust/Diebstahl und/oder Verlust/Diebstahl von elektronischen Informationen;
- Missbrauch vertraulicher Informationen;
- Compliance-Risiko (Nichteinhaltung gesetzlicher und anderer rechtlicher Anforderungen).

Prüfungszeitraum: 1. Januar 2013-31. Dezember 2013 (mit eventueller Ausweitung auf frühere und spätere Jahre).

Prüfungsfeststellungen und Schlussfolgerungen

Der portugiesische elektronische Reisepass (PEP) wird in drei Kategorien ausgestellt: gewöhnlicher Reisepass[69], Diplomatenpass oder Sonderpass. Es gibt auch einen Reisepass für Nicht-Staatsangehörige, mit dem eingeschränkte Privilegien gewährt werden.

Das Ausstellungssystem umfasst mehrere Antragsformulare und verschiedene Stellen, die für die Datenerfassung und die Erteilung der Pässe zuständig sind, aber nur eine ausstellende Stelle (die für die Herstellung, Personalisierung und Lieferung verantwortlich ist).

[69] Etwa 99 % der Gesamtzahl.

An diesem Prozess sind mehrere Behörden (PEP-Stellen) beteiligt. Die folgenden Stellen erfassen Daten und erteilen Pässe:

- Festland Portugal: *Serviço de Estrangeiros e Fronteiras* (SEF)[70] und die Registrierungsdienste des Instituto dos Registos e do Notariado (IRN)[71];
- autonome Regionen Azoren[72] und Madeira: Dienststellen des jeweiligen *Vice-Presidência do Governo Regional*[73]; Ausland: die portugiesischen Konsulate;
- *Imprensa Nacional – Casa da Moeda,* S.A. (INCM)[74] stellt die Pässe her und liefert sie aus.

Die wichtigsten Prozesse werden hauptsächlich durch das SIPEP (das zentrale Beantragungssystem für die Ausstellung portugiesischer Pässe) unterstützt. Das SIPEP ermöglicht die Erfassung, Speicherung, Verarbeitung, Validierung und Bereitstellung der erforderlichen Informationen in Verbindung mit der Erteilung des Reisepasses, löst den von der INCM durchgeführten Personalisierungsprozess aus und stellt die Verbindung mit anderen Systemanwendungen sicher, indem es alle PEP-Stellen koordiniert, die an der physischen und logistischen Registrierung der erfassten Daten beteiligt sind.

Die PEP-Stellen sind organisatorisch so strukturiert, dass sie die mit dem Reisepass verbundenen gesetzlichen Ziele erfüllen können. Auf der Antrags- und Erfassungsebene stützt sich das System noch immer in hohem Maße auf menschliches Personal. Das SIPEP enthält jedoch auch eine Reihe von automatischen Verarbeitungsfunktionen und Validierungskontrollen.

Da mit den Verfahren Kontrollfunktionen und Funktionen zur Verhinderung von Datenmanipulation sichergestellt werden, die zum Teil eigenständig und ohne menschliches Zutun ausgeführt werden können, hat das SIPEP im Hinblick auf die

---

[70] Einwanderungs- und Grenzbehörde.

[71] Melderegister und Notariat (nur Abholung).

[72] Und die Dienststellen der *Agência para a Modernização e Qualidade do Serviço ao Cidadão, I. P. (RIAC)* – Agentur für die Modernisierung und die Qualität des Dienstes am Bürger, öffentliche Einrichtung (nur Abholung).

[73] Vizepräsidium der Regionalregierung.

[74] Nationale Druckerei und Münzprägeanstalt, öffentliches Unternehmen.

Organisation und das Informationssystem erhebliche Auswirkungen, insbesondere auf: (i) das Verständnis und die Festlegung der Normen, Prozesse und benötigten Daten und (ii) die Festlegung der Anforderungen des Informationssystems.

Die effiziente und wirksame Datenerfassung wird durch das Zusammenspiel des SIPEP mit anderen Informationssystemen[75] gemäß den gesetzlichen Vorschriften sichergestellt.

Es wurde ein – wenngleich nicht umfassend dokumentierter – Rahmen für die Gesamtsteuerung der IT-Aktivitäten (Governance, Entwicklung und Beschaffung, IT-Vorgänge, Geschäftskontinuität und Notfallwiederherstellung, Informationssicherheit) eingerichtet, mit dem die Entwicklung, der Betrieb, die Verwaltung und die Instandhaltung des SIPEP sichergestellt wird.

Aktivitätsindikatoren (2013):

- Es wurden etwa 500 000 elektronische Reisepässe ausgestellt, davon etwa 63 % vom SEF, 33 % von den portugiesischen Konsulaten und 4 % von den Regionalregierungen.
- Die Einnahmen aus der Ausstellung der Reisepässe beliefen sich auf rund 37 Millionen Euro, die überwiegend von der INCM (43 %), dem SEF (32 %) und dem *Ministério dos Negócios Estrangeiros (MNE)*[76] (17 %) generiert wurden.

Für das Jahr 2013 konnten die im SIPEP durchgeführten Überprüfungen die Einhaltung der gesetzlich festgelegten maximalen Lieferzeit (vom Datum der Beantragung bis zur Bereitstellung des Reisepasses zur Abholung an der Lieferstelle) nicht bestätigen, da das tatsächliche Lieferdatum an der Lieferstelle nicht immer zeitnah registriert wurde.

Vom SEF, MNE, der RIAC und der INCM wurden Investitionen in Verbindung mit dem Erwerb von Ausrüstung für die Erfassung biometrischer Daten und Unterschriften (Kiosk), Ausrüstung für automatische Grenzkontrollsysteme (ABC) und dem Kauf sowie der Instandhaltung von IT-Systemen, Dienstleistungen und technischer Unterstützung in einer Gesamthöhe von 11 Millionen Euro getätigt, von denen der höchste Betrag vom SEF verausgabt wurde.

---

[75] Dabei handelt es sich um die folgenden Systeme: Integriertes Informationssystem des SEF (SIISEF), nationales Schengener Informationssystem (NSIS), zivile Identifikationsdatenbank, Strafregisterdatenbank.

[76] Außenministerium.

Vor dem elektronischen Reisepass lag der Preis für den (nicht-biometrischen) Pass der Portugiesischen Republik bei 22,44 Euro; im Jahr 2006 betrug der Preis für den gewöhnlichen (biometrischen) Reisepass 60 Euro, der dann 2011 auf 65 Euro stieg.

Anträge auf Erteilung eines portugiesischen elektronischen Reisepasses

Anträge auf Erteilung eines portugiesischen elektronischen Reisepasses werden persönlich von den zuständigen Stellen bearbeitet, die die Antragsunterlagen entgegennehmen, die biografischen und biometrischen Daten der Antragsteller erfassen, die Gebühren einziehen und später den ausgestellten Reisepass zustellen.

Das zugrundeliegende System (SIPEP) validiert die Richtigkeit und Qualität der Daten durch virtuelle Kontrollen und Quervergleiche mit anderen Informationssystemen, insbesondere der zivilen Identifikationsdatenbank, um sicherzustellen, dass der Antrag regelkonform und für die Erteilung und Ausstellung des elektronischen Reisepasses geeignet ist.

Damit einhergehende Statusänderungen werden in Protokolldateien aufgezeichnet, wodurch die Nachvollziehbarkeit, Integrität und Nichtabstreitbarkeit der Transaktionen gewährleistet wird.

Die Datenübertragung zwischen den Datenerfassungsstellen (in Portugal und im Ausland) und dem SEF erfolgt über ein VPN (Virtuelles Privates Netz), das auf der Basis einer Zugangsverwaltung gemäß den vom SEF kontrollierten Zugangsdaten implementiert ist[77].

Der Antrag auf Erteilung eines gewöhnlichen elektronischen Reisepasses wird mit einem anderen Verfahren bearbeitet, wenn er von Personen gestellt wird, deren Rechte be- bzw. eingeschränkt sind, wie z. B. (i) Personen, die ihre Rechte nicht selbst ausüben können (Minderjährige, geschäftsunfähige oder unerlaubte Personen), (ii) Personen, die aufgrund gerichtlicher oder polizeilicher Maßnahmen ausgeschlossen sind (Vorstrafe, anhängiges Gerichtsverfahren oder Einziehung von Dokumenten) und (iii) Personen, die einen Antrag auf Erteilung eines zweiten elektronischen Reisepasses stellen und dabei ein nationales oder berechtigtes Interesse geltend machen.

[77] Das SIPEP ist (über das Internet) auf nationaler/regionaler und internationaler Ebene für Dienststellen, die auf dem Festland, in den autonomen Regionen der Azoren und Madeira sowie im Ausland (portugiesische Konsulate) ansässig sind, zugänglich.

Erteilung des portugiesischen elektronischen Reisepasses

Die Entscheidung zur Erteilung des gewöhnlichen elektronischen Reisepasses kann

- automatisiert erfolgen – automatische Genehmigung durch das SIPEP-Antragssystem, nachdem die Identität des Antragstellers festgestellt und geprüft wurde, dass keine Vorstrafen vorliegen (durch Abgleich mit der zivilen Identifikations- und Strafregisterdatenbank des IRN) und keine Gerichtsverfahren anhängig sind (trifft nur für das SEF bei Beantragungen des elektronischen Reisepasses auf dem Festland zu[78]),

- vorbehaltlich der Annahme/Genehmigung durch andere Stellen (Regionalregierungen und konsularische Vertretungen) im Einzelfall oder in Fällen, in denen die Anforderungen des SEF keine automatische Genehmigung zulassen[79].

Ausstellung des portugiesischen elektronischen Reisepasses

Für die Ausstellung des portugiesischen elektronischen Reisepasses, einschließlich der Herstellung, Personalisierung und Lieferung, ist die INCM zuständig. Sobald die Lieferung des Reisepasses im SIPEP erfasst ist, wird der Passstatus auf "gültig" geändert.

Die Gebühren für den Reisepass sind je nach benötigtem Servicegrad unterschiedlich. Um den Servicegrad zu messen, muss das SIPEP den tatsächlichen Liefertermin des Reisepasses berücksichtigen.

Die Lieferung des Reisepasses erfolgt durch einen beauftragten Transportdienst.

---

[78] Hierbei handelt es sich um eine automatisierte Funktionalität des SIPEP-Antragssystems zur Genehmigung (intern als "Autorisierung" bezeichnet) eines Antrags (außer für einen zweiten elektronischen Reisepass) für volljährige Bürgerinnen und Bürger, die einen gültigen Bürgerausweis besitzen, gegen die keine Gerichtsverfahren anhängig sind und die keinem Verbot oder Ausschluss unterliegen. Von den vom SEF genehmigten gewöhnlichen elektronischen Reisepässen wurden etwa 60 % mit automatischen Validierungsverfahren und Genehmigungsentscheidungen erteilt, der Rest unterlag der Prüfung und Genehmigung durch die *Direção Central de Imigração e Documentação (DCID)*.

[79] Insbesondere in Fällen von Antragstellern, die nicht in der Lage sind, ihre Rechte auszuüben (Minderjährige, geschäftsunfähige oder unerlaubte Personen), die aufgrund von gerichtlichen oder polizeilichen Maßnahmen ausgeschlossen sind oder deren Antrag von der DCID im Einzelfall geprüft wird.

Ablauf des portugiesischen elektronischen Reisepasses

Gibt ein Antragsteller einen noch gültigen elektronischen Reisepass vorzeitig ab, sollte dieser deaktiviert werden, um seine weitere Nutzung zu verhindern, was dem Status "nicht nutzbar" des Passdatensatzes im SIPEP-Antragssystem entspricht.

Finnland
Valtiontalouden Tarkastusvirasto

Vorkehrungen zum Schutz vor Cyberangriffen

Datum der Veröffentlichung: 2017

Hyperlink zum Bericht: Bericht (in finnischer Sprache)

Prüfungsart und -zeitraum

Prüfungsart: Wirtschaftlichkeitsprüfung

Prüfungszeitraum: 2016-2017

Zusammenfassung des Berichts

Prüfungsthema

Mit der Prüfung sollte untersucht werden, ob der Schutz der Zentralregierung vor Cyberangriffen so wirksam und kosteneffizient wie möglich geregelt war. Der Prüfungsschwerpunkt lag auf der Frage, wie die Zentralregierung die Cybersicherheit organisierte und verwaltete. Die Ergebnisse der Prüfung dienten der Verbesserung der Wirksamkeit und Effizienz der Cybersicherheit in der Zentralregierung. Die Prüfung wurde vom 22. September 2016 bis zum 4. September 2017 durchgeführt. Im Herbst 2019 fand eine Weiterverfolgungsprüfung statt. In der Weiterverfolgungsprüfung untersuchte der finnische Rechnungshof die Maßnahmen, die aufgrund der Feststellungen und Empfehlungen der vorangegangenen Prüfung ergriffen wurden.

Geprüft wurden unter anderem die Behörden, die bei der Zentralregierung für den Cyberschutz zuständig sind (das Büro des Ministerpräsidenten, das Finanzministerium, das Ministerium für Verkehr und Kommunikation), sowie die Behörden, die die Verantwortung für zentrale Cyberschutzaufgaben und IT-Dienste in der Zentralregierung tragen (das nationale Cybersicherheitszentrum der finnischen Agentur für Verkehr und Kommunikation, das staatliche IKT-Zentrum *Valtori* und die Agentur für Digital- und Bevölkerungsdaten). Die Wirksamkeit der

Handlungsempfehlungen wurde auch im Rahmen einer Untersuchung der zentralen staatlichen Stellen, die elektronische Dienstleistungen anbieten, bewertet (die Agentur für Digital- und Bevölkerungsdaten, die finnische Agentur für Verkehr und Kommunikation *Traficom*, das Amt für Beitreibung und Vollstreckung und das Justizministerium als dessen Aufsichtsbehörde sowie das IKT-Servicezentrum des Justizministeriums).

Prüfungsfragen

Die folgenden Prüfungsfragen wurden gestellt, um die Organisation der Cybersicherheit zu bewerten:

- Hat die geprüfte Stelle bei der Organisation der Cybersicherheit den wirtschaftlichen Aspekt ausreichend berücksichtigt?
- Wird die Cybersicherheit der Systeme durch das Situationsbewusstsein der geprüften Stelle im Bereich der Cybersicherheit unterstützt?
- Ist die geprüfte Stelle ausreichend in der Lage, auf Cybervorfälle zu reagieren?

Das Prüfungsthema "Vorkehrungen zum Schutz vor Cyberangriffen" war Bestandteil der Prüfungsthematik "Sicherstellung der operativen Zuverlässigkeit der Informationsgesellschaft" im Prüfungsplan des finnischen Rechnungshofs für den Zeitraum 2016-2020. Im Hinblick auf die Bedeutung für die Staatsfinanzen lässt sich das Prüfungsthema insofern rechtfertigen, als Betriebsunterbrechungen und Datenschutzverletzungen mit Nachteilen verbunden sind und sich eine schwache Cybersicherheit negativ auf Geschäftstätigkeiten auswirkt. Die Prüfung wurde parallel zur Prüfung "Steuerung der operativen Zuverlässigkeit elektronischer Dienstleistungen" durchgeführt, die zur gleichen Thematik gehört. Das Prüfungsmaterial bestand im Wesentlichen aus Dokumenten und Befragungen der für die betreffende Tätigkeit zuständigen Behörden.

Prüfungsfeststellungen und Schlussfolgerungen

In der finnischen Cybersicherheitsstrategie sind die wichtigsten Ziele und Maßnahmen festgelegt, um die Herausforderungen der Cyberumgebung zu bewältigen und ihr Funktionieren zu gewährleisten. Es wurden und werden Anstrengungen unternommen, um die Cybersicherheitsstrategie im Rahmen eines Durchführungsprogramms umzusetzen, dessen Fortschritt jährlich evaluiert wird. Der Sicherheitsausschuss ist ein Kooperationsgremium innerhalb des

Verteidigungsministeriums, das die Umsetzung der Cybersicherheitsstrategie überwacht und koordiniert.

Eine wirksame Organisation der Cybersicherheit setzt ein Risikomanagement voraus, das, um erfolgreich zu sein, wirksame Managementstrukturen und -regelungen erfordert, mit denen das Risikomanagement auf allen Ebenen der Organisation in die Abläufe integriert wird. Wie viele andere Länder sind auch Finnland und seine Zentralregierung nicht autark, was ihre Ressourcen für den Cyberschutz angeht. Die Zahl der Rechtsvorschriften der Europäischen Union hat im Laufe der Zeit zugenommen und ihre Rechtsverbindlichkeit ebenso. In der finnischen Regierung ist die Zuständigkeit für den Cyberschutz dezentral organisiert, und jede Stelle ist für ihre eigene Cybersicherheit verantwortlich. In der Zentralregierung ist die Zuweisung von Zuständigkeiten bei etwaigen Cybervorfällen im Hinblick auf deren Art, Umfang und Umsetzung komplex geregelt.

Aufgrund dieser Komplexität ist es möglich, dass die Reaktion auf eine Anomalie zu langsam erfolgt, und die knappen finanziellen Mittel haben die Umsetzung der finnischen Cybersicherheitsstrategie eingeschränkt. Auf der Grundlage der Prüfungsfeststellungen kam der nationale Rechnungshof zu folgenden Schlussfolgerungen und unterbreitete folgende Empfehlungen für die Organisation der Cybersicherheit in der Zentralregierung:

Das operative Management weitreichender Cybersicherheitsvorfälle war nicht definiert

Eine Planung des operativen Managements weitreichender Cybersicherheitsvorfälle und eine Aufteilung der damit verbundenen Zuständigkeiten könnten schnellere Reaktionen und eine angemessene Koordination und Ressourcenzuweisung zur Ergreifung von Gegenmaßnahmen ermöglichen. Im aktuellen Betriebsmodell ist jede Behörde für ihren eigenen Cyberschutz verantwortlich. Die Fachkenntnisse im Bereich des Cyberschutzes sind jedoch nicht ausreichend, wodurch es schwieriger ist, den Cyberschutz intern oder durch Auslagerung umzusetzen.

Einige Ziele der Cybersicherheitsstrategie wurden nicht erreicht

Das Durchführungsprogramm für die finnische Cybersicherheitsstrategie hat zu Verbesserungen beim Cyberschutz geführt. Einige Ziele des ersten Durchführungsprogramms wurden nicht erreicht, weil das Engagement für die Maßnahmen unterschiedlich ausfiel und nicht zentral verbessert werden konnte. Das neue Umsetzungsprogramm enthielt nur Maßnahmen, zu denen sich die zuständigen

Behörden und andere Akteure verpflichtet hatten. Es bestand eine Wechselwirkung zwischen Engagement und verfügbaren Ressourcen.

Die Angemessenheit von Finanzierungslösungen für den Cyberschutz war nicht klar

Die Unterschiede bei der Entwicklung des Cyberschutzes waren teilweise darauf zurückzuführen, dass den Organisationen in unterschiedlichem Umfang Entwicklungsressourcen zur Verfügung standen. In den Vorschriften zur Aufstellung des staatlichen Haushaltsplans oder zum Aufstellungsprozess waren keine Verfahren festgelegt, mit denen sichergestellt wurde, dass den wichtigsten Zielen für den Cyberschutz Mittel zugewiesen werden. Die Behörden und Institutionen wiesen die Mittel für Cybersicherheit als nicht näher bezeichneten Teil der operativen Ausgaben der jeweiligen Behörde oder Institution im Haushalt aus. Die in der finnischen Cybersicherheitsstrategie beschriebenen Maßnahmen wurden nur im Rahmen der zur Verfügung stehenden Mittel umgesetzt.

Cyberschutz sollte auch bei Änderungen in der IKT-Organisation berücksichtigt werden

Änderungen in der IKT-Organisation der Zentralregierung hatten Auswirkungen auf die Vorkehrungen zum Schutz vor Cyberangriffen. Die Cybersicherheit zentral vom IKT-Zentrum *Valtori* entwickeln zu lassen, hatte sich als schwierig erwiesen. Es gab Mängel bei der Bewertung der Angemessenheit der praktischen Verfahren zum Schutz vor Cyberangriffen und bei der Umsetzung der neuen Vorkehrungen.

Das Situationsbewusstsein sollte im Hinblick auf Cybersicherheitsoperationen verbessert werden

Das Cybersicherheitszentrum sorgte für die Aufrechterhaltung des landesweiten Situationsbewusstseins im Bereich der Cybersicherheit. Zum Zeitpunkt der Prüfung gab es keine Verpflichtung, Cybersicherheitsvorfälle an das Cybersicherheitszentrum zu melden. Die Situation würde sich verbessern, wenn staatliche Stellen verpflichtet würden, Vorfälle zu melden, und wenn die Reichweite von zentralisierten Verfahren zur Aufdeckung von Cybervorfällen erhöht würde.

Auf der Grundlage der vorstehenden Feststellungen empfiehlt der finnische Rechnungshof dem Finanzministerium, für Cybervorfälle in den IKT-Diensten der Zentralregierung ein umfassendes Betriebsmanagementmodell auszuarbeiten und umzusetzen. Das Finanzministerium sollte auch ermitteln, wie die Cybersicherheit der Dienste bei der Finanzierung dieser Dienste während ihres gesamten Lebenszyklus berücksichtigt werden kann, und das operative Situationsbewusstsein erhöhen, indem

es die Behörden anweist, Cybervorfälle an das Cybersicherheitszentrum zu melden. Es wurde empfohlen, dass das IKT-Zentrum *Valtori* die Implementierung, Bewertung und Entwicklung von Cybersicherheitsverfahren und die Aufdeckung von Cybervorfällen verbessern sollte.

Bei der Weiterverfolgungsprüfung wurde untersucht, wie die während der vorangegangenen Prüfung ausgesprochenen Empfehlungen umgesetzt worden waren. Der finnische Rechnungshof vertrat die Auffassung, dass das Finanzministerium als zuständige Behörde für die Umsetzung der Empfehlungen keine ausreichenden Maßnahmen ergriffen hatte, um den Empfehlungen nachzukommen. Allerdings wurde die Cybersicherheit in Finnland auch durch Maßnahmen anderer Behörden – zusätzlich zu denen des Finanzministeriums – verstärkt. Zudem wurde das strategische Management der Cybersicherheit im Hinblick auf das Modell eines Cybersicherheitsdirektors geändert. Im Vorschlag für den Haushaltsplan 2020 erhöhte die Regierung die Mittel für die zentralen staatlichen Behörden, die eine Schlüsselrolle bei der Stärkung der Cybersicherheit spielen. Darüber hinaus ergriff das IKT-Zentrum *Valtori* Maßnahmen, die der Empfehlung des nationalen Rechnungshofs entsprachen. Abschließend stellte der nationale Rechnungshof fest, dass eine Weiterverfolgungsprüfung aufgrund nicht umgesetzter Empfehlungen notwendig und eine völlig neue Prüfung in diesem Bereich angesichts der laufenden Veränderungen der Cybersicherheitsvorkehrungen und der digitalen Betriebsumgebung sowie der damit verbundenen Risiken und der Bedeutung der Cybersicherheit für die Staatsfinanzen und die Gesellschaft gerechtfertigt war.

Schweden
Riksrevisionen

Veraltete IT-Systeme – ein Hindernis für eine wirksame Digitalisierung

Datum der Veröffentlichung: 2019

Hyperlink zum Bericht: Zusammenfassung des Berichts (in englischer Sprache)
Bericht (in schwedischer Sprache)

Prüfungsart und -zeitraum

Prüfungsart: Wirtschaftlichkeitsprüfung

Prüfungszeitraum: 2018-2019

Zusammenfassung des Berichts

Prüfungsthema

Veraltete betriebskritische IT-Systeme bergen ein hohes Risiko für Effizienzprobleme, da Organisationen verhältnismäßig mehr Ressourcen aufwenden müssen, nur um das System instand zu halten. Somit besteht guter Grund zu der Annahme, dass veraltete IT-Systeme ein hohes Risiko für eine schlechte Verwaltung öffentlicher Mittel mit sich bringen. Zudem wird die Innovationsfähigkeit einer Behörde, die eine Voraussetzung für die Entwicklung neuer IT-Systeme darstellt, durch veraltete IT-Systeme zum Teil blockiert. Veraltete IT-Systeme führen jedoch nicht nur zu Risiken für einzelne Behörden. Probleme innerhalb einer Behörde können sich auch erheblich auf ihre Fähigkeit auswirken, ihre Tätigkeiten mit einer anderen Behörde oder einem privaten Akteur zu koordinieren. Außerdem bergen veraltete IT-Systeme Risiken im Hinblick auf die Informationssicherheit.

Definition des Hauptthemas der Prüfung/Prüfungsfragen/Kontext

Ziel der Prüfung war es, die Verbreitung veralteter IT-Systeme in der zentralen staatlichen Verwaltung zu untersuchen und zu ermitteln, ob die Behörden und die Regierung geeignete Maßnahmen ergriffen hatten, um zu verhindern, dass diese Systeme zu einem Hindernis für die wirksame Digitalisierung werden. Die folgenden Prüfungsfragen wurden gestellt:

- Haben die Behörden geeignete Maßnahmen ergriffen, um die mit veralteten IT-Systemen verbundenen Probleme zu lösen?
- Hat die Regierung geeignete Maßnahmen ergriffen, um die mit veralteten IT-Systemen verbundenen Probleme zu lösen?

Prüfungsfeststellungen und Schlussfolgerungen

- Bei der Prüfung wurde festgestellt, dass es in zahlreichen staatlichen Behörden veraltete IT-Systeme gab. In vielen Behörden war zudem mindestens ein betriebskritisches IT-System veraltet. Nach Kenntnis des schwedischen Rechnungshofs handelt es sich hierbei um neue Informationen, und das Ausmaß des Problems in der zentralen staatlichen Verwaltung war bislang unbekannt. Rund 80 % der Behörden gaben an, bei mindestens einem ihrer betriebskritischen Systeme Schwierigkeiten zu haben, das Niveau der Informationssicherheit aufrechtzuerhalten. Mehr als jede zehnte Behörde antwortete, dass dies auf alle oder auf die Mehrheit der Systeme zutreffe.
- Einem großen Teil der untersuchten Behörden fehlte der richtige Ansatz zur Entwicklung und Verwaltung der IT-Unterstützung. Die vorhandenen Instrumente für die operative Entwicklung wurden nicht genutzt, um zu ermitteln, wie die IT-Unterstützung am besten zur Erreichung der Ziele der Haupttätigkeiten beitragen kann. Somit fehlte bei einem Großteil der geprüften Behörden eine allgemeine Beschreibung des Zusammenspiels von Strategien, operativen Abläufen und Systemen. Dies wiederum bedeutete, dass es für sie schwierig war zu analysieren und zu verstehen, wie sich Veränderungen auf die Ziele der Organisation auswirken, und es ihnen folglich schwerer fiel, festzulegen, welche Situation künftig angestrebt werden sollte.
- Mehr als die Hälfte der Behörden gab an, dass keine genehmigten Vorgaben dazu vorlagen, wie sie – von der Systementwicklung bis zur Ausmusterung (gewöhnlich als Lebenszyklusmanagement bezeichnet) – mit ihren IT-Systemen verfahren und

diesbezügliche Entscheidungen treffen sollten. Dem schwedischen Rechnungshof zufolge war dies ein Hinweis darauf, dass das Lebenszyklusmanagement nicht auf strukturierte und methodische Weise durchgeführt wurde. Defizite gab es auch bei der Risikoanalyse und bei der Fähigkeit, die IT-Kosten so detailliert aufzuschlüsseln, wie es für eine fundierte Entscheidungsfindung notwendig ist.

- Fast 60 Prozent der Behörden verfügten lediglich bei einem oder einigen wenigen betriebskritischen Systemen über Lebenszyklusplänе für die Systementwicklung. Da Lebenszyklusplänе und sonstige Planungsunterlagen in vielen Behörden fehlten und das tatsächlich umgesetzte Lebenszyklusmanagement Mängel aufwies, konnte nicht davon ausgegangen werden, dass die Behörden im Allgemeinen eine bewusste und eindeutige Haltung zu ihren IT-Systemen entwickelt hatten.

- Der Bewertung des schwedischen Rechnungshofs zufolge waren die beteiligten Ministerien und damit auch die Regierung weder über die Verbreitung noch die Folgen veralteter IT-Systeme ausreichend informiert.

Die Prüfer gelangten zu dem Schluss, dass es den meisten Behörden zum Zeitpunkt der Prüfung nicht wirklich gelungen war, die Probleme im Zusammenhang mit veralteten IT-Systemen wirksam anzugehen. Nach Auffassung des schwedischen Rechnungshofs ist das Problem so gravierend und weit verbreitet, dass es ein Hindernis für die kontinuierliche effiziente Digitalisierung der staatlichen Verwaltung darstellt. Die Prüfung zeigte auch, dass es der Regierung an Kenntnis über die Existenz und die Folgen der Probleme mit veralteten IT-Systemen fehlte. Außerdem hatte die Regierung keine Maßnahmen ergriffen, um das Problem der veralteten IT-Systeme zielgerichteter anzugehen. Der schwedische Rechnungshof kam in seiner Bewertung daher zu dem Schluss, dass nicht davon auszugehen ist, dass die Regierung ausreichende Maßnahmen ergriffen hat, um sicherzustellen, dass die Probleme gemindert oder beseitigt werden.

Weitere Berichte in diesem Bereich

Titel des Berichts:	"Making it easier to start a business – government efforts to promote a digital process" (RiR 2019:14)
Hyperlink zum Bericht:	Zusammenfassung des Berichts (in englischer Sprache) Bericht (in schwedischer Sprache)
Datum der Veröffentlichung:	2019

Titel des Berichts:	"Digitalisation of public administration – Simpler, more transparent and effective administration" (RiR 2016:14)
Hyperlink zum Bericht:	Zusammenfassung des Berichts (in englischer Sprache) Bericht (in schwedischer Sprache)
Datum der Veröffentlichung:	2016

Titel des Berichts:	"Information security work at nine agencies" (RIR 2016:8)
Hyperlink zum Bericht:	Zusammenfassung des Berichts (in englischer Sprache) Bericht (in schwedischer Sprache)
Datum der Veröffentlichung:	2016

Titel des Berichts:	"Cybercrime – police and prosecutors can be more efficient" (RiR 2015:21)
Hyperlink zum Bericht:	Zusammenfassung des Berichts (in englischer Sprache) Bericht (in schwedischer Sprache)
Datum der Veröffentlichung:	2015

Europäische Union
Europäischer Rechnungshof

Themenpapier: Herausforderungen für eine wirksame Cybersicherheitspolitik

Datum der Veröffentlichung: 2018

Hyperlink zum Bericht: Bericht (in 23 Sprachen verfügbar)

Prüfungsart und -zeitraum

Prüfungsart: Analyse

Prüfungszeitraum: April bis September 2018

Zusammenfassung des Berichts

Thema der Analyse

Dieses Themenpapier stellt keinen Prüfungsbericht dar. Es soll vielmehr einen Überblick über die komplexe Politik der EU im Bereich der Cybersicherheit bieten und aufzeigen, wo die größten Herausforderungen für die wirksame Umsetzung der Politik liegen. Betrachtet werden Netz- und Informationssicherheit, Cyberkriminalität, Cyberabwehr und Desinformation.

Die Analyse des Hofes basiert auf der Untersuchung von amtlichen Dokumenten, Positionspapieren und Studien von Dritten, die öffentlich zugänglich waren. Die Bestandsaufnahme fand zwischen April und September 2018 statt, wobei die bis Dezember 2018 eingetretenen Entwicklungen berücksichtigt wurden. Zusätzlich wurde eine Erhebung bei den Rechnungskontrollbehörden der Mitgliedstaaten sowie eine Befragung wichtiger Akteure aus den EU-Organen und Vertreter des Privatsektors durchgeführt.

Es gibt keine einheitliche Definition von "Cybersicherheit". Ganz allgemein handelt es sich um alle Vorkehrungen und Maßnahmen zum Schutz von Informationssystemen und deren Nutzern vor unbefugten Zugriffen, vor Angriffen und vor Schaden, um die Vertraulichkeit, Integrität und Verfügbarkeit von Daten zu gewährleisten. Cybersicherheit bedeutet, Cybervorfälle zu verhindern oder sie aufzudecken, darauf zu

reagieren und deren Folgen zu beseitigen. Vorfälle können vorsätzlich oder unbeabsichtigt herbeigeführt werden und reichen von der unbeabsichtigten Preisgabe von Informationen bis zu Angriffen auf Unternehmen und kritische Infrastrukturen, zum Diebstahl personenbezogener Daten und sogar zur Störung demokratischer Prozesse.

Eckpfeiler der EU-Politik ist die Cybersicherheitsstrategie 2013. Sie soll das digitale Umfeld in der EU – bei gleichzeitiger Wahrung der Grundwerte und Grundfreiheiten – zum sichersten weltweit machen. Die Strategie verfolgt fünf Kernziele: i) Erhöhung der Widerstandsfähigkeit gegenüber Cyberangriffen, ii) Eindämmung der Cyberkriminalität, iii) Entwicklung einer Cyberverteidigungspolitik und Aufbau von Cyberverteidigungskapazitäten, iv) Entwicklung der industriellen und technischen Ressourcen für die Cybersicherheit und v) Erarbeitung einer internationalen Cyberraumstrategie im Einklang mit den Grundwerten der EU.

Feststellungen

Die Auswirkungen einer unzureichenden Vorbereitung auf einen Cyberangriff lassen sich wegen des Mangels an zuverlässigen Daten nur schwer erfassen. Der durch Cyberkriminalität verursachte wirtschaftliche Schaden ist zwischen 2013 und 2017 um das Fünffache gestiegen. Betroffen waren Staaten und Unternehmen, große ebenso wie kleine. Die prognostizierte Zunahme bei den Prämien für Cyberversicherungen von 3 Milliarden Euro im Jahr 2018 auf 8,9 Milliarden Euro im Jahr 2020 ist Ausdruck dieser Entwicklung. Obwohl 80 % der EU-Unternehmen im Jahr 2016 mindestens einen Cybersicherheitsvorfall verzeichneten, ist das Risikobewusstsein immer noch erschreckend niedrig. Von den Unternehmen in der EU haben 69 % keine oder nur eine grobe Vorstellung von ihrem Gefährdungspotenzial durch Cyberkriminalität, 60 % haben noch nie eine Schätzung der potenziellen finanziellen Verluste vorgenommen. Einer internationalen Erhebung zufolge würde ein Drittel der Unternehmen eher den Hackern Lösegeld zahlen als in Informationssicherheit zu investieren.

Der Hof gelangte zu folgenden Feststellungen:

- Das Cyberökosystem der EU ist komplex und vielschichtig – zahlreiche Akteure sind daran beteiligt. Die einzelnen Bausteine des Systems zusammenzuführen ist ein schwieriges Unterfangen.

- Die EU beabsichtigt, das weltweit sicherste Online-Umfeld zu werden. Damit dieses ehrgeizige Ziel erreicht werden kann, sind erhebliche Anstrengungen aller Beteiligten, einschließlich einer soliden und angemessen verwalteten Finanzgrundlage, erforderlich. Zahlenmaterial gibt es kaum. Schätzungen zufolge

belaufen sich die öffentlichen Ausgaben der EU für Cybersicherheit auf 1 bis 2 Milliarden Euro jährlich. Im Vergleich dazu betragen die für das Jahr 2019 veranschlagten Ausgaben der US-Bundesregierung rund 21 Milliarden US-Dollar.

- Governance im Bereich der Informationssicherheit bedeutet die Schaffung von Strukturen und Strategien zur Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Daten. Sie ist mehr als nur eine Frage der Technik und erfordert effektive Führung, stabile Prozesse und auf die Ziele der Organisation abgestimmte Strategien.

- Die Mitgliedstaaten wenden im Bereich der Cybersicherheits-Governance unterschiedliche Modelle an, und in den einzelnen Mitgliedstaaten ist die Zuständigkeit für Cybersicherheit oft auf mehrere Stellen verteilt. Diese Unterschiede könnten die Zusammenarbeit behindern, die notwendig ist, um auf groß angelegte, grenzübergreifende Sicherheitsvorfälle zu reagieren und Informationen über Bedrohungen auf nationaler Ebene – oder gar EU-Ebene – auszutauschen.

- Die Konzeption einer wirksamen Reaktion auf Cyberangriffe ist entscheidend, um sie so früh wie möglich zu unterbinden. Besonders wichtig ist, dass kritische Sektoren, die Mitgliedstaaten und die EU-Organe schnell und koordiniert reagieren können. Dies setzt voraus, dass die Angriffe frühzeitig aufgedeckt werden.

Empfehlungen

Die Analyse des Hofes zeigt, dass ein Übergang zu einer Leistungskultur mit integrierten Evaluierungsverfahren erforderlich ist, um eine angemessene Evaluierung und Rechenschaftspflicht sicherzustellen. Einige rechtliche Lücken bestehen noch und die geltenden Rechtsvorschriften werden von den Mitgliedstaaten nicht kohärent umgesetzt. Dadurch können die Rechtsvorschriften möglicherweise nicht voll und ganz greifen.

Eine weitere vom Hof ausgemachte Herausforderung betrifft die Angleichung des Investitionsniveaus an die strategischen Ziele, die eine Erhöhung der Investitionen und Auswirkungen erfordert. Dies gestaltet sich schwieriger, wenn die EU und ihre Mitgliedstaaten keinen klaren Überblick über die EU-Ausgaben für Cybersicherheit haben. Zudem gab es Engpässe bei der Ausstattung der für Cyberfragen zuständigen EU-Agenturen mit angemessenen Mitteln sowie Probleme bei der Anwerbung und dauerhaften Bindung von Talenten.

Akronyme und Abkürzungen

APT: *Advanced Persistent Threat* (fortgeschrittene, andauernde Bedrohung)

BIP: Bruttoinlandsprodukt

CERT-EU: *Computer Emergency Response Team for the EU institutions, bodies and agencies* (IT-Notfallteam für die Organe, Einrichtungen und sonstigen Stellen der EU)

COBIT: *Control Objectives for Information and Related Technology* (Kontrollziele für Informations- und verwandte Technologien)

COVID-19: Coronavirus-Krankheit-2019

cPPP: *contractual Public-Private Partnership* (vertragliche öffentlich-private Partnerschaft)

CSIRT: *Computer Security Incident Response Team* (Computer-Notfallteam)

DDoS: *Distributed Denial of Service* (verteilter Dienstverweigerungsangriff)

DSGVO: Datenschutz-Grundverordnung

EAD: Europäischer Auswärtiger Dienst

EC3: *Europol's European Cybercrime Centre* (Europäisches Zentrum zur Bekämpfung der Cyberkriminalität von Europol)

EDA: *European Defence Agency* (Europäische Verteidigungsagentur)

ENISA: Agentur der Europäischen Union für Cybersicherheit

ESI-Fonds: Europäische Struktur- und Investitionsfonds

ESRB: *European Systemic Risk Board* (Europäischer Ausschuss für Systemrisiken)

EU: Europäische Union

EuRH: Europäischer Rechnungshof

Europol: Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung

GSVP: Gemeinsame Sicherheits- und Verteidigungspolitik

IKT: Informations- und Kommunikationstechnologie

IoT: *Internet of Things* (Internet der Dinge)

ISACA: *Information Systems Audit and Control Association* (Berufsverband für IT-Revisoren, Informationssicherheitsmanager und IT-Governance-Experten)

ISF-P: Fonds für die innere Sicherheit – Polizei

IT: Informationstechnologie

MERS: *Middle East Respiratory Syndrome* (Nahost-Atemwegssyndrom)

MFR: Mehrjähriger Finanzrahmen

NATO: *North Atlantic Treaty Organization* (Nordatlantikvertrags-Organisation)

NIS-Richtlinie: Richtlinie zur Netz- und Informationssicherheit

ORKB: Oberste Rechnungskontrollbehörden

RDP: *Remote Desktop Protocol*

SARS: *Severe acute respiratory syndrome* (schweres akutes Atemwegssyndrom)

SSZ: Ständige Strukturierte Zusammenarbeit

URL: *Uniform Resource Locator* (Internetadresse)

US: *United States* (Vereinigte Staaten)

Glossar

5G: Technologiestandard der fünften Generation für Breitband-Mobilfunknetze, der seit 2019 zunehmend von Mobilfunkunternehmen weltweit eingesetzt wird, und geplanter Nachfolger der 4G-Netze, mit denen die meisten aktuellen Handys verbunden sind. Die höhere Geschwindigkeit wird u. a. durch die Verwendung von Funkwellen erzielt, die eine höhere Frequenz aufweisen als bei den bisherigen Mobilfunknetzen.

***Advanced Persistent Threats* (fortgeschrittene, andauernde Bedrohungen):** Angriffe, bei denen sich eine unautorisierte Person Zugang zu einem System oder Netzwerk verschafft und sich dort so lange wie möglich unentdeckt aufhält. Dies ist besonders gefährlich für Unternehmen, da Hacker fortlaufend Zugang zu sensiblen Unternehmensdaten haben. In der Regel wird jedoch kein Schaden an Firmennetzwerken oder lokalen Rechnern angerichtet. Das Ziel dieser Angriffe besteht darin, Daten zu stehlen.

Adware: Schadsoftware, die Werbebanner oder Pop-ups anzeigt, die Codes enthalten, mit denen das Online-Verhalten der Opfer nachverfolgt werden kann.

Anbieter digitaler Dienste: jeder, der eine oder mehrere dieser drei Arten von digitalen Dienstleistungen anbietet: Online-Marktplatz, Online-Suchmaschinen, Cloud-Computing-Dienste.

Betreiber wesentlicher Dienste: öffentliche oder private Einrichtung, die einen Dienst bereitstellt, der für die Aufrechterhaltung kritischer gesellschaftlicher und wirtschaftlicher Tätigkeiten wesentlich ist.

Biometrische Daten (biometrische Identifikatoren): physische (wie Fingerabdrücke und Augen) oder verhaltensbasierte Berechnungen, die sich auf menschliche Merkmale beziehen. Die Authentifizierung wird in der Informatik als eine Form der Identifikation und Zugriffskontrolle verwendet.

Bitcoin: im Jahr 2009 geschaffene digitale bzw. virtuelle Währung (Kryptowährung), bei der die Peer-to-Peer-Technologie (Netz gleichberechtigter Rechner) genutzt wird, um sofortige Zahlungen zu ermöglichen.

Cloud-Computing: bedarfsbezogene Bereitstellung von IT-Ressourcen – wie Speicherplatz, Rechenleistung oder Kapazitäten für die gemeinsame Datennutzung – über das Internet durch Speicherung auf standortfernen Servern.

Cyberabwehr: Teilbereich der Cybersicherheit mit dem Ziel, den Cyberraum mit militärischen und anderen geeigneten Mitteln zu verteidigen, um militärstrategische Ziele zu erreichen.

Cyberangriff: Versuch, die Vertraulichkeit, Integrität und Verfügbarkeit von Daten oder eines Computersystems im Cyberraum zu untergraben oder zu zerstören.

Cyberbedrohung: böswillige Handlung, mit der darauf abgezielt wird, Daten zu beschädigen, Daten zu stehlen oder das digitale Leben im Allgemeinen zu stören.

Cyberdiplomatie: Einsatz diplomatischer Ressourcen und Ausübung diplomatischer Funktionen zum Schutz nationaler Interessen in Bezug auf den Cyberraum. Sie wird ganz oder teilweise von Diplomaten betrieben, die auf bilateraler Ebene (z. B. im Rahmen des Dialogs zwischen den Vereinigten Staaten und China) oder in multilateralen Foren (wie den Vereinten Nationen) zusammenkommen. Über den traditionellen Aufgabenbereich der Diplomatie hinaus interagieren die Diplomaten auch mit verschiedenen nichtstaatlichen Akteuren, wie z. B. den Leitern von Internetunternehmen (wie Facebook oder Google), Technologieunternehmern oder Organisationen der Zivilgesellschaft. Diplomatie kann auch beinhalten, dass unterdrückten Stimmen in anderen Ländern durch Technologie Gehör verschafft wird.

Cyberkriminalität: unterschiedliche kriminelle Aktivitäten, bei denen Computer und IT-Systeme entweder Hauptinstrument oder Hauptziel sind. Diese Aktivitäten umfassen herkömmliche Straftaten (z. B. Betrug, Fälschung und Identitätsdiebstahl), inhaltsbezogene Straftaten (z. B. Verbreitung von kinderpornografischen Inhalten im Internet, Aufwiegelung zum Rassismus) und Straftaten, die nur über Computer und Informationssysteme möglich sind (z. B. Angriffe auf Informationssysteme, Überlastungsangriffe, Schadprogramme oder Ransomware).

Cyberökosystem: komplexes System aus interagierenden Geräten, Daten, Netzen, Menschen, Prozessen und Organisationen sowie das Prozess- und Technologieumfeld, das diese Interaktion beeinflusst und unterstützt.

Cyberraum: virtuelles globales Umfeld, in dem Menschen mithilfe von Computernetzen und technischen Geräten über Software mit Diensten online kommunizieren.

Cybersicherheit (Cyberschutz): alle Vorkehrungen und Maßnahmen zum Schutz von IT-Systemen und ihren Daten vor unbefugten Zugriffen, vor Angriffen und vor Schaden, um ihre Verfügbarkeit, Vertraulichkeit und Integrität zu gewährleisten.

Cyberspionage: Handlung oder Praxis, Geheimnisse und Informationen ohne die Erlaubnis oder das Wissen des Inhabers der Informationen von Privatpersonen, Wettbewerbern, Konkurrenten, Gruppen, Regierungen und Feinden zum persönlichen, wirtschaftlichen, politischen oder militärischen Vorteil unter Verwendung des Internets, von Netzwerken oder von einzelnen Computern zu erlangen.

Cybervorfall: Ereignis, das die Resilienz und Sicherheit eines IT-Systems und der mit diesem System verarbeiteten, gespeicherten oder übermittelten Daten direkt oder indirekt schädigt oder bedroht.

Datenschutzverletzung: absichtliche oder unabsichtliche Freigabe von geschützten oder persönlichen/vertraulichen Informationen an eine nicht vertrauenswürdige Umgebung.

Datenverarbeitung: Ausführung von Operationen an Daten, insbesondere durch einen Computer, um Informationen abzurufen, umzuwandeln oder zu klassifizieren.

Desinformation: nachweislich falsche oder irreführende Informationen, die mit dem Ziel des wirtschaftlichen Gewinns oder der vorsätzlichen Täuschung der Öffentlichkeit konzipiert, vorgelegt und verbreitet werden und öffentlichen Schaden anrichten können.

Digitale Inhalte: alle in einem digitalen Format gespeicherten Daten (zum Beispiel Text-, Ton-, Bild- oder Videomaterial).

Digitale Plattform: Umgebung für Interaktionen zwischen mindestens zwei verschiedenen Gruppen, von denen die eine typischerweise aus Anbietern und die andere aus Verbrauchern/Nutzern besteht. Dabei kann es sich um die Hardware oder das Betriebssystem handeln, sogar um einen Webbrowser und zugehörige Anwendungsprogrammierschnittstellen oder andere zugrunde liegende Software, solange der Programmcode damit ausgeführt wird.

Digitale Vermögenswerte: alles, was in digitaler Form vorliegt, einer Person oder einem Unternehmen gehört und mit einem Nutzungsrecht verbunden ist (z. B. Bilder, Fotos, Videos, Textdateien usw.).

Digitalisierung: Prozess der Umwandlung von Informationen in ein digitales Format, bei dem die Informationen in Bits organisiert sind. Das Ergebnis ist die Darstellung eines Objekts, Bildes, Tons, Dokuments oder Signals durch Generieren einer Reihe von Zahlen, die eine diskrete Menge seiner Punkte oder Abtastwerte beschreiben.

Distributed Denial of Service (DDoS): Cyberangriff, der rechtmäßige Nutzer am Zugang zu Online-Diensten oder -Ressourcen hindert, indem diese mit Anfragen überlastet werden.

Ethische Hacker: Personen (Computersicherheitsexperten), die in ein Computernetzwerk eindringen, um dessen Sicherheit zu testen oder zu bewerten, ohne eine böswillige oder kriminelle Absicht zu verfolgen.

Hacker: Personen, die Computer-, Netzwerk- oder andere Fähigkeiten nutzen, um sich unbefugten Zugriff auf Daten, Computersysteme oder Netzwerke zu verschaffen.

Hochleistungsrechnen: Fähigkeit, mit hoher Geschwindigkeit Daten zu verarbeiten und komplexe Berechnungen durchzuführen.

Hybride Bedrohung: Bekundung feindlicher Absichten durch Gegner, die eine Mischung aus konventioneller und nicht konventioneller Kriegsführung (d. h. militärische, politische, wirtschaftliche und technologische Mittel) einsetzen, um ihre Ziele gewaltsam durchzusetzen.

Informationssicherheit: Reihe von Prozessen und Instrumenten zum Schutz von physischen und digitalen Daten vor Zugriff, Verwendung, Preisgabe, Störung, Änderung, Erfassung oder Zerstörung durch Unbefugte.

Integrität: Schutz vor unzulässiger Änderung oder Zerstörung von Informationen und Sicherstellung ihrer Unversehrtheit.

Internet der Dinge: Netz alltäglicher Gegenstände, die mit Elektronik, Software und Sensoren ausgestattet sind und so über das Internet kommunizieren und Daten austauschen können.

Kritische Infrastruktur: physische Ressourcen, Dienste und Anlagen, deren Störung oder Zerstörung gravierende Auswirkungen auf das Funktionieren von Wirtschaft und Gesellschaft hätte.

Kritisches Informationssystem: bestehendes oder geplantes Informationssystem, das für den effizienten und wirksamen Betrieb einer Organisation als wesentlich angesehen wird.

Kryptowährung: digitaler Vermögenswert, der – unabhängig von Zentralbanken – mithilfe von Verschlüsselungstechniken ausgegeben und getauscht wird. Kryptowährungen werden von den Mitgliedern einer virtuellen Gemeinschaft als Zahlungsmittel anerkannt.

Künstliche Intelligenz: Simulation menschlicher Intelligenz durch Maschinen, die so programmiert sind, dass sie wie Menschen denken und deren Handlungen nachahmen; jede Maschine, die Merkmale eines menschlichen Geistes, wie Lernen und Problemlösungskompetenzen, aufweist.

Malware: Schadsoftware. Computerprogramm, das Computer, Server oder Netze beschädigen soll.

Netzsicherheit: Teilbereich der Cybersicherheit, der den Schutz von Daten betrifft, die über Geräte im gleichen Netz verschickt werden, damit diese Daten nicht abgegriffen oder geändert werden können.

Öffentliche Versorgungssysteme: Masten, Türme, ober- oder unterirdische Leitungen, sonstige tragende oder stützende Strukturen sowie Gräben jeweils mit allem Zubehör, die für die Bereitstellung (Versorgung oder Verteilung) von Strom-, Telefon-, Telegrafen-, Kabel- oder Signaldiensten oder anderen ähnlichen Diensten genutzt werden können.

Patching: Einspielung einer Reihe von Änderungen an einer Software, um sie zu aktualisieren, zu reparieren oder zu verbessern, einschließlich der Beseitigung von Sicherheitslücken.

Personenbezogene Daten: Informationen über eine identifizierbare natürliche Person.

Phishing: Senden von E-Mails aus einer scheinbar vertrauenswürdigen Quelle, um die Empfänger dazu zu verleiten, auf schädliche Links zu klicken oder personenbezogene Daten preiszugeben.

Ransomware: Schadsoftware, die den Opfern den Zugriff auf ein Computersystem verwehrt oder Dateien – in der Regel durch Verschlüsselung – unlesbar macht. Die Angreifer erpressen in der Regel anschließend das Opfer, indem sie sich weigern, den Zugang vor Zahlung eines Lösegeldes wieder freizugeben.

Remote Desktop Protocol: (von Microsoft herausgegebener) technischer Standard, für den Fernzugriff auf Computer. Remote-Desktop-Nutzer können auf ihren Desktop zugreifen, Dateien öffnen und bearbeiten und Anwendungen nutzen, als ob sie tatsächlich an ihrem Desktop-Computer sitzen würden.

Sabotage: Handlung zur absichtlichen Zerstörung, Beschädigung oder Behinderung, insbesondere zur Erlangung politischer oder militärischer Vorteile.

Social Engineering: im Bereich der Informationssicherheit die psychologische Manipulation von Menschen, um sie zur Durchführung einer Aktion oder Preisgabe vertraulicher Informationen zu verleiten.

Spyware: Schadsoftware, die darauf abzielt, Informationen über eine Person oder Organisation zu sammeln und diese Informationen auf eine Weise an Dritte zu senden, die dem Nutzer schadet, z. B. durch Verletzung der Privatsphäre oder durch Gefährdung der Sicherheit des Geräts.

Textvektorisierung: Umwandlung von Wörtern, Sätzen oder ganzen Dokumenten in numerische Vektoren, damit sie von Algorithmen für das maschinelle Lernen genutzt werden können.

Trojaner: Schadcode bzw. -software, der/die legitim aussieht, aber die Kontrolle über einen Computer übernehmen kann. Trojaner sind darauf ausgelegt, Daten oder Netzwerke zu beschädigen, zu stören, zu stehlen oder ganz allgemein einen anderen schädlichen Vorgang auszuführen.

Verfügbarkeit: Gewährleistung, dass der Zugriff auf und die Nutzung von Informationen zeitnah und zuverlässig möglich sind.

Verschlüsselung: Umwandlung von Klartext in codierten Text, um ihn zu schützen. Um den Text lesen zu können, muss der Nutzer einen geheimen Schlüssel oder ein Passwort haben.

Vertraulichkeit: Schutz von Informationen, Daten oder Vermögenswerten vor unbefugtem Zugriff oder vor Verrat.

Wahlinfrastruktur: Dazu gehören für Wahlkampagnen eingesetzte IT-Systeme und Datenbanken, vertrauliche Informationen über Kandidaten sowie Systeme zur Wählerregistrierung und -verwaltung.

Webbasierte Angriffe: Definierte Nutzer vertrauen darauf, dass die sensiblen personenbezogenen Daten, die sie auf einer Website preisgeben, vertraulich behandelt werden und sicher sind. Wird (durch einen Angriff) in die Website eingedrungen, können Kreditkartendaten, Sozialversicherungsdaten oder medizinische Daten öffentlich zugänglich werden, was möglicherweise schwerwiegende Folgen hat.

Widerstandsfähigkeit gegenüber Cyberangriffen (Cyber-Resilienz): Fähigkeit, Cyberangriffe und -vorfälle zu verhindern, sich darauf vorzubereiten, ihnen standzuhalten und einen Betrieb oder einen Prozess aufrecht zu erhalten.

Würmer: Computerwürmer sind eigenständige Schadprogramme, die sich selbst vervielfältigen, um sich auf andere Computer auszubreiten. Häufig verbreiten sie sich mithilfe eines Computernetzwerks, wobei sie Sicherheitslücken auf dem Zielcomputer ausnutzen, um darauf zuzugreifen.

Zugangsdaten: Informationen über die Login- und Logout-Aktivitäten eines Nutzers beim Zugang zu einem Dienst, wie Uhrzeit, Datum und IP-Adresse.

Die EU kontaktieren

Besuch
In der Europäischen Union gibt es Hunderte von „Europe-Direct"-Informationsbüros. Über diesen Link finden Sie ein Informationsbüro in Ihrer Nähe: https://europa.eu/european-union/contact_de

Telefon oder E-Mail
Der Europe-Direct-Dienst beantwortet Ihre Fragen zur Europäischen Union. Kontaktieren Sie Europe Direct
— über die gebührenfreie Rufnummer: 00 800 6 7 8 9 10 11 (manche Telefondienstanbieter berechnen allerdings Gebühren),
— über die Standardrufnummer: +32 22999696 oder
— per E-Mail über: https://europa.eu/european-union/contact_de

Informationen über die EU

Im Internet
Auf dem Europa-Portal finden Sie Informationen über die Europäische Union in allen Amtssprachen: https://europa.eu/european-union/index_de

EU-Veröffentlichungen
Sie können – zum Teil kostenlos – EU-Veröffentlichungen herunterladen oder bestellen unter https://publications.europa.eu/de/publications.
Wünschen Sie mehrere Exemplare einer kostenlosen Veröffentlichung, wenden Sie sich an Europe Direct oder das Informationsbüro in Ihrer Nähe (siehe https://europa.eu/european-union/contact_de).

Informationen zum EU-Recht
Informationen zum EU-Recht, darunter alle EU-Rechtsvorschriften seit 1952 in sämtlichen Amtssprachen, finden Sie in EUR-Lex https://eur-lex.europa.eu

Offene Daten der EU
Über ihr Offenes Datenportal (http://data.europa.eu/euodp/de) stellt die EU Datensätze zur Verfügung. Die Daten können zu gewerblichen und nichtgewerblichen Zwecken kostenfrei heruntergeladen werden.

Contact Committee

Kontaktausschuss

der Obersten Rechnungskontrollbehörden der EU