Rechnungshof Österreich
Unabhängig und objektiv für Sie.

# IT–Sicherheit des Bundes

*Rechnungshof.Mehr.Wert*

IMPRESSUM

Herausgeber: Rechnungshof
Dampfschiffstraße 2, 1030 Wien
www.rechnungshof.gv.at
Redaktion und Grafik:
Rechnungshof Österreich
Herausgegeben: Wien, im September 2024

AUSKÜNFTE

Rechnungshof Österreich
Telefon: +43 (0) 1 711 71 – 8946
E–Mail: info@rechnungshof.gv.at
facebook/RechnungshofAT
Twitter: @RHSprecher
instagram: rechnungshofat

# IT–Sicherheit des Bundes

*Rechnungshof.Mehr.Wert*


## INHALTSVERZEICHNIS

# VORWORT

Der Rechnungshof legt das Themenpapier „**IT–Sicherheit des Bundes**|***Rechnungshof.Mehr.Wert***“ auf Basis seiner veröffentlichten Berichte vor. In diesem Sinne möchte er seine Beratungsfunktion verstärkt wahrnehmen. Unsere Berichte ergeben ein aussagekräftiges Bild über die Schlüsse, die der Rechnungshof aus seiner Prüftätigkeit zieht. Sie sind als „Lessons Learned“ für die laufenden und für künftige Krisenbewältigungen zu verstehen.

Die öffentliche Verwaltung war in der Vergangenheit von Cyber–Angriffen betroffen. In den vergangenen Jahren war ein stetiger Anstieg schwerwiegender Vorfälle zu verzeichnen. Ein Sicherheitsvorfall betraf z.B. das Land Kärnten, einer das Außenministerium.

Es traten auch Sicherheitsvorfälle in Form von Attacken auf IT–Services, von Verbindungsproblemen aufgrund von Leitungsausfällen, von Sicherheits–Zertifikatproblemen, Fehlkonfigurationen von Netzwerkkomponenten, Datenverschlüsselung oder auch Datenschutzverletzungen auf.

Ein hohes Maß an IT-Sicherheit zu gewährleisten, stellt daher für alle öffentlichen Institutionen – einschließlich des RH – eine zentrale Aufgabe dar. Dies insbesondere, um die öffentliche Leistungserbringung sicherstellen zu können.

Auch für den RH selbst gehört die IT-Sicherheit zu den wichtigsten Herausforderungen unserer Zeit, um die wir uns tagtäglich bestmöglich bemühen.

*Margit Kraker*
Präsidentin des Rechnungshofes

*Rechnungshof.Mehr.Wert*

# Rechnungshof

## Vier Gebarungsüberprüfungen zum Thema IT–Sicherheit


(Stand Juni 2024)

- ✓ Management der IT–Sicherheit in der Verwaltung ausgewählter Bundesministerien
- ✓ Umstellung von der Bürgerkarte/ Handysignatur auf den elektronischen Identitätsnachweis (E–ID)
- ✓ Dienstrechtliche und technische Umsetzung von Telearbeit in ausgewählten Bundesministerien
- ✓ Management der IT–Sicherheit im Finanzministerium, Klimaschutzministerium und Landwirtschaftsministerium

Die Informationstechnologie (IT) stellt die Basis einer funktionierenden effektiven staatlichen Verwaltung dar. Der RH hat daher seit 2020 einen seiner Schwerpunkte auf Gebarungsüberprüfungen der IT–Sicherheit gelegt.

Da noch keine einheitlichen Sicherheitsstandards für die IT der Bundesverwaltung vorlagen, zog der RH ausgewählte Aspekte des „Österreichischen Informationssicherheitshandbuchs“ (Stand Februar 2023) als Maßstab für die in den Bundesministerien eingesetzten Maßnahmen des Managements der IT–Sicherheit heran.

Das Management der IT–Sicherheit umfasst die von jedem Ressort selbst zu treffenden IT–Sicherheitsvorkehrungen. Beispielhaft beinhalten diese nachfolgende Aufgabenbereiche:

## IT–Konsolidierung

Bündelung der IT–Serviceleistungen im Bund, Standardisierung von IT–Arbeitsplätzen

## IT–Sicherheitsorganisation

IT–Strategie und IT–Sicherheitsstrategie, IT–Sicherheitsstandards, Funktionen der IT–Sicherheitsorganisation

## IT–Arbeitsplatz (einschließlich Telearbeit)

Maßnahmen für die Funktion und Sicherheit der Daten des IT–Arbeitsplatzes

## IT–Sicherheit Personal

Maßnahmen zu Gewährleistung der personellen IT–Sicherheit für internes und externes Personal

## IT–Sicherheit zentraler IT–Systeme

Maßnahmen für die Sicherheit der zentralen IT–Infrastruktur

Der RH fasst die bei seinen Gebarungsüberprüfungen in einzelnen Bundesministerien festgestellten Ergebnisse nachfolgend im Sinne genereller Aussagen zusammen und wiederholt dazu wichtige Empfehlungen in den Kernaussagen

# Handlungsempfehlungen IT–Sicherheit

Die Konsolidierung der IT wäre umzusetzen, um die Kosten der Beschaffung und der Lizenzgebühren zu reduzieren, die Heterogenität zu verringern und die Betreuung zu bündeln; dies würde auch zur IT–Sicherheit beitragen.

Die Bundesministerien sollten den Bedarf an IT–Sicherheits–Audits basierend auf einer umfassenden Risikoanalyse erheben, die notwendigen IT–Sicherheits–Audits priorisieren und diese Überprüfungen zeitnah durchführen.

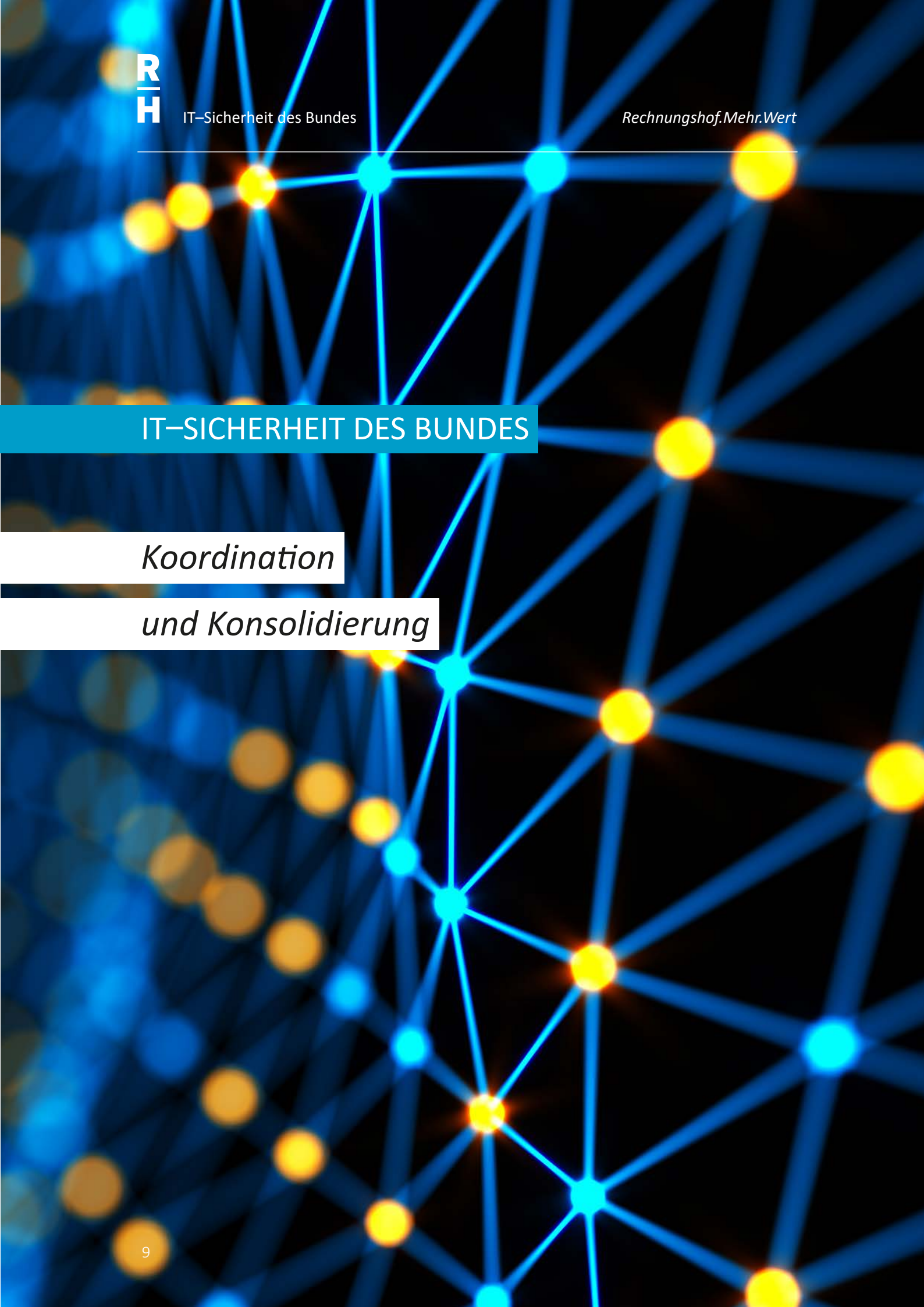
Die Bundesministerien sollten die IT–Sicherheitsmaßnahmen für den IT–Arbeitsplatz einer Risikoanalyse unterziehen, den Bedarf an weiteren technischen Sicherheitsmaßnahmen prüfen und erforderlichenfalls Maßnahmen setzen.

Im Rahmen des (Konsolidierungs–) Projekts Security Framework Bund wären einheitliche verbindliche Sicherheitsstandards für die IKT der öffentlichen Verwaltung zu erarbeiten.

Die IT–Sicherheit durch die Anwenderinnen und Anwender wäre durch entsprechende Regelungen, verpflichtende Schulungen und regelmäßige Weiterbildungsmaßnahmen sicherzustellen.

Die Funktionen Chief Information Security Officer (CISO), Chief Information Officer (CIO) und Chief Digital Officer (CDO) wären zu besetzen und voneinander unabhängig einzurichten.

Die Bundesministerien sollten ihre technischen Maßnahmen zur Erhöhung der IT–Sicherheit der zentralen IT–Infrastruktur dahingehend regelmäßig prüfen, ob diese umfassend sind und dem aktuellen Stand der Technik entsprechen.



# IT–SICHERHEIT DES BUNDES

## *Koordination und Konsolidierung*

# KOORDINATION UND KONSOLIDIERUNG

**Die IT–Konsolidierung soll die Heterogenität der im Bund eingesetzten IT–Arbeitsplätze verringern und IT–Serviceleistungen bündeln. Das trägt zu Kosteneinsparungen und zur Vereinheitlichung der Servicequalität bei.**

## KOORDINATION DER IT–SICHERHEIT

Die IT–Ausstattung der Arbeitsplätze in den Bundesministerien bestand u.a. aus dem mobilen Gerät oder Standgerät mit Betriebssystem, Bürosoftware, E–Mail–programm und Browser (zur Darstellung von Websites). Gemäß dem Bericht IT–Konsolidierung der Österreichischen Bundesregierung (November 2019) lag in den Bundesministerien keine einheitliche IT–Ausstattung der Arbeitsplätze vor.

Darüber hinaus setzten die Bundesministerien spezifische IT–Fachanwendungen und spezifische Systeme für die zentrale Infrastruktur ein, z.B. Datenserver, Applikationsserver, Netz, zentrale Speicher. Die IT–Abteilungen spezialisierten sich in der Folge in hohem Maße auf die in ihrem Bundesministerium konkret vorliegenden IT–Arbeitsplätze sowie zentralen Systeme und IT–Fachanwendungen. Die Betreuung erfolgte – in jedem Bundesministerium individuell organisiert – durch die eigene IT–Abteilung, durch die BRZ GmbH oder durch externe Dienstleister.

Die IT–Sicherheit in den Bundesministerien war grundsätzlich durch organisatorische Maßnahmen, den Einsatz technischer Systeme seitens der eigenen IT–Abteilung bzw. unter Zuhilfenahme externer Dienstleister zu gewährleisten. Die individuelle Gestaltung der IT führte auch zu einer individuellen Gestaltung der technischen Sicherheitsmaßnahmen und der dafür verwendeten spezifischen Produkte. Eine Kompetenz zur ressortübergreifenden Koordination der IT–Sicherheit war im Bundesministeriengesetz nicht normiert.

**Handlungsfelder**

- Die Ministerverantwortlichkeit ermöglicht es jedem Bundesministerium, eigene ressortspezifische IT–Lösungen für Infrastruktur und Software einzusetzen. Auch die IT–Sicherheitsmaßnahmen und das Management der IT–Sicherheit sind daher ressortspezifisch individuell gestaltet.

- Mangels Kompetenz für eine ressortübergreifende Koordination der IT–Sicherheit liegen in den Ministerien unterschiedliche Sicherheitsmaßnahmen vor. Das hat auch ein unterschiedliches Maß an IT–Sicherheit zur Folge.

## ÜBERNAHME VON IT–AGENDEN

Bundesministeriengesetz–Novellen führten z.B. zwischen 2018 und 2024 mehrmals zu umfassenden Verschiebungen von Zuständigkeiten zwischen den Bundesministerien. Die Zuständigkeit für Digitalisierung etwa wanderte vom Bundeskanzleramt zum Wirtschaftsministerium, vom Wirtschaftsministerium zum Finanzministerium und vom Finanzministerium wieder ins Bundeskanzleramt:

Zuständigkeit Digitalisierung in den Ministerien

| | |
|---|---|
| bis 7. Jänner 2018 | Bundeskanzleramt |
| ab 8. Jänner 2018 | Bundesministerium für Digitalisierung und Wirtschaftsstandort |
| ab 29. Jänner 2020 | Bundesministerium für Digitalisierung und Wirtschaftsstandort |
| ab 18. Juli 2022 | Bundesministerium für Finanzen |
| ab 1. Mai 2024 | Bundeskanzleramt |

Die Verschiebung von Kompetenzen machte es erforderlich, die zuständigen Organisationseinheiten und ihre Bediensteten sowie die zugehörigen IT–Arbeitsplätze zu übertragen. Mit dieser Migration der IT–Arbeitsplätze waren Maßnahmen in der IT–Ausstattung, den Fachanwendungen, der IT–Betreuung und der IT–Sicherheit zwingend verbunden:

> die IT–Ausstattung der Arbeitsplätze der übernommenen Bediensteten mit jener des aufnehmenden Bundesministeriums zu vereinheitlichen

> die mit den übertragenen Zuständigkeiten verbundenen IT–Fachanwendungen im aufnehmenden Bundesministerium zu integrieren

> für die übertragenen IT–Fachanwendungen eine eigene IT–Betreuung sicherzustellen oder externe Dienstleister einzusetzen

> die eigene IT–Sicherheitsstrategie und die darauf aufbauenden technischen Methoden und Produkte auf die neue IT–Ausstattung der Arbeitsplätze, die IT–Fachanwendungen und ihre IT–Infrastruktur anzuwenden.

Der Migrationsprozess dauerte in den überprüften Bundesministerien bis zu einem Jahr. Während dieses Zeitraums übernahmen die IT–Abteilungen der abgebenden Bundesministerien weiterhin die Betreuung der IT–Arbeitsplätze und waren für die IT–Sicherheit verantwortlich. Das aufnehmende Ministerium hatte in dieser Phase der Migration für die neuen IT–Arbeitsplätze und Fachanwendungen die Risikoanalysen durchzuführen und die spezifischen technischen und organisatorischen Sicherheitsmaßnahmen umzusetzen.

**Handlungsfelder**

- Die Integration der – nach Verschiebung von Kompetenzen zwischen Bundesministerien – neu einzugliedernden Organisationseinheiten ist mit hohem Arbeitsaufwand verbunden und erfordert komplexe IT–technische Maßnahmen.

- Diese oft mehrmonatige Phase der Integration ist darüber hinaus kritisch in Bezug auf die durchgängige Gewährleistung der IT–Sicherheit.

## PROGRAMM IT–KONSOLIDIERUNG

Die im November 2019 im Ministerrat präsentierte „Machbarkeitsstudie“ stellte die Notwendigkeit einer IT–Konsolidierung für IT–Arbeitsplätze, Standard– und Fachanwendungen sowie die zentrale IT–Infrastruktur fest. Im November 2019 beschloss die Bundesregierung, die vorgeschlagenen Konsolidierungsmaßnahmen umzusetzen.

Im August 2020 erteilten die Generalsekretäre einen konkreten Auftrag für eine IT–Konsolidierung. Der Programmauftrag richtete sich an das damalige Digitalisierungsministerium und das Bundeskanzleramt unter Mitwirkung aller Ressorts. Zu den im Programmauftrag angeführten Zielen zählten Kosteneinsparungen, eine zuverlässige Sicherheitsarchitektur, eine verbesserte einheitliche Servicequalität einschließlich schnellerer Erbringung sowie gesteigerte Transparenz und zentrale Steuerung. Die Zuständigkeit für Digitalisierungsangelegenheiten verschob sich mit der Novelle des Bundesministeriengesetzes im Jahr 2022 in das Finanzministerium und mit Mai 2024 in das Bundeskanzleramt.

Das Programm zur IT–Konsolidierung umfasste im Mai 2023 insgesamt acht Projekte; zwei weitere waren in Vorbereitung (Bereitstellung Arbeitsplatz– und mobile Geräte, Rahmenplanung zur IT–Konsolidierung).

**Handlungsfelder**

- Vier Jahre nach dem Auftrag vom August 2020 war lediglich eines von acht Projekten zur IT–Konsolidierung umgesetzt: das einheitliche Videokonferenzsystem.

- Bei den Projekten „Standardarbeitsplatz und sichere Basisdienste“ sowie „Hotline/Service Desk“ waren die Analyse und Konzeption abgeschlossen. Der Lenkungsausschuss hatte aber die bundesweite Umsetzung eines derartig umfassenden Projekts als nicht erfolgversprechend eingeschätzt; die Erkenntnisse der Analyse und Konzeption sollen in nachfolgenden Projekten berücksichtigt werden.

- Fünf Projekte des Programms IT–Konsolidierung – „Software Asset Management“, „Standardisierte Rechenzentrumservices“, „Standard Services“, „Security Framework Bund“, „IT–Service Management Prozesse“ – befanden sich im Juni 2023 in der Analyse– und Konzeptionsphase. Für zwei dieser Projekte war keine Umsetzung vorgesehen, bei drei Projekten hatte der Lenkungsausschuss noch keine Entscheidung über eine nachfolgende Umsetzung getroffen.

**EMPFEHLUNGEN AUS RH–BERICHTEN:**

Im Bundesministeriengesetz wäre eine Kompetenz zur Koordination der IT–Sicherheit ausdrücklich festzulegen.

Die Konsolidierung der IT wäre in den Ressorts fortzuführen, um die Kosten der Beschaffung und der Lizenzgebühren zu reduzieren, die Heterogenität zu verringern und die Betreuung zu bündeln; dies würde auch zur IT–Sicherheit beitragen.

Die Konsolidierung der IT–Arbeitsplätze, der Standardanwendungen sowie der zentralen IT–Infrastruktur ist ein Beitrag für Kosteneinsparungen, für eine einheitliche Servicequalität und für eine verbesserte Sicherheitsarchitektur. Die im Konsolidierungsprogramm bereits erstellten Konzepte wären in einzelnen Bundesministerien auf ihre Umsetzbarkeit zu prüfen; die im Konsolidierungsprogramm erst eingeleiteten Projekte wären mit Nachdruck zu betreiben.

# IT–SICHERHEIT DES BUNDES

## *IT–Sicherheitsorganisation*

# IT–SICHERHEITSORGANISATION

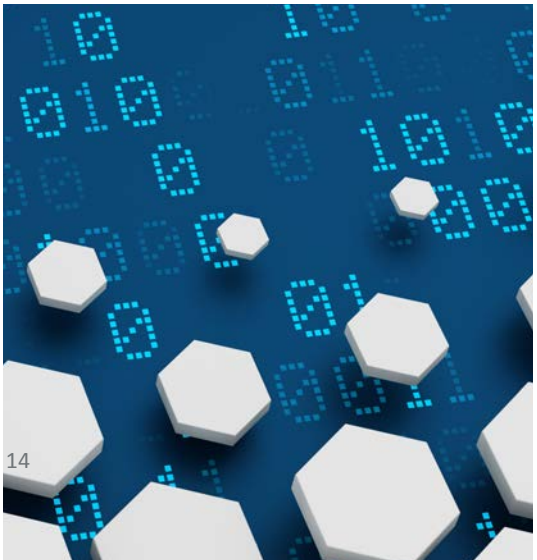
Um sich die Vorteile einer durchgängigen Digitalisierung nutzbar zu machen bei gleichzeitiger Bewältigung der Risiken muss eine IT–Sicherheitsorgansiation aufgebaut werden. Diese besteht aus folgenden Komponenten: einer IT–Strategie und im Speziellen der IT–Sicherheitsstrategie, aus den IT–Sicherheitsstandards und den Funktionen der IT–Sicherheitsorganisation.

## DIGITALISIERUNGSSTRATEGIE

Eine durchgängige Digitalisierung der Arbeits– und Geschäftsprozesse erfordert strategische Vorgaben in einer Digitalisierungsstrategie, um die für die Umsetzung dieser Ziele notwendigen technologie– und prozessbezogenen Entscheidungen abzusichern.

**Handlungsfelder**

- Einzelne Bundesministerien hatten keine Digitalisierungsstrategie oder ähnliche strategischen Festlegungen ausgearbeitet und in Kraft gesetzt. Damit fehlten strategische Festlegungen zur weiteren Digitalisierung des Bundesministeriums.



## IT–SICHERHEITSSTRATEGIE

Die IT–Sicherheitsstrategie ist die Grundlage des IT–Sicherheitsmanagements und definiert u.a. dessen Ziele, Verantwortlichkeiten und Methoden. Eine solche Strategie soll allgemeine Festlegungen treffen, um den Schutz der IT–Systeme innerhalb einer Organisation zu gewährleisten. Sie soll außerdem die Verantwortlichkeiten in der IT–Sicherheitsorganisation eines Bundesministeriums und der Bediensteten festlegen und sicherstellen, dass die Ressortleitung das IT–Sicherheitsmanagement ausreichend unterstützt („Management Commitment“). Die IT–Sicherheitsstrategie ist transparent in Kraft zu setzen, damit auch das Personal Kenntnis über ihre Inhalte erlangt.

**Handlungsfelder**

- Die überprüften Bundesministerien verfügten grundsätzlich über IT–Sicherheitsstrategien mit relevanten Zielen und nachvollziehbaren Maßnahmen.

- Die in einzelnen Bundesministerien festgestellten Mängel betrafen:

> Aktualität: Grundsatzdokumente zur IT–Sicherheitsstrategie waren in einzelnen Bundesministerien nicht aktuell, in Einzelfällen mehr als 20 Jahre alt.

> Geltungsbereich: Nach Verschiebung von Kompetenzen zwischen Bundesministerien war der Geltungsbereich der Strategie nicht an die neue Organisation angepasst worden.

> Unterstützung durch die oberste Führungsebene: Die Verantwortung der Ressortleitung war in den strategischen Dokumenten nicht festgelegt.

> Nachgeordneten Dienststellen: Diese waren vom Geltungsbereich der IT–Sicherheitsstrategien nicht oder nur teilweise umfasst.

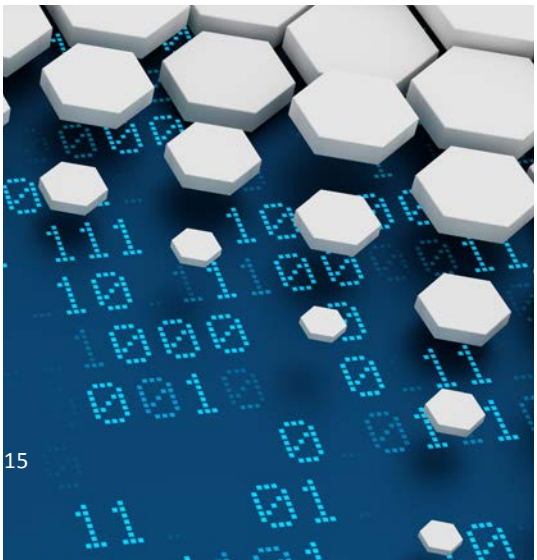
> Information der Bediensteten: Die IT– Sicherheitsstrategie wurde den Bediensteten nicht aktiv zur Kenntnis gebracht.

## SICHERHEITSSTANDARDS

Als technisch–organisatorische Grundlage für eine sichere IT im öffentlichen Sektor dienten die „Österreichische Strategie für Cybersicherheit 2021" und das „Österreichische Informationssicherheitshandbuch 2023". Sie enthielten Leitlinien und Empfehlungen zur sicheren Gestaltung der IT. Das Ziel, einheitliche und verbindliche Sicherheitsstandards für die IKT der öffentlichen Verwaltung zu schaffen, war im Regierungsprogramm 2020–2024 festgelegt. Auch der Beschluss des Nationalen Sicherheitsrates vom Februar 2020 empfahl einheitliche Sicherheitsstandards.

**Handlungsfelder**

- Einheitliche verbindliche Sicherheitsstandards für die IKT der öffentlichen Verwaltung fehlten.



## FUNKTIONEN DER IT–SICHERHEITSORGANISATION

Für die effiziente Wahrnehmung der operativen IT–Sicherheit ist es notwendig, Rollen und klare Verantwortlichkeiten festzulegen. Dafür haben sich gemäß dem Österreichischen Informationssicherheitshandbuch Standardfunktionen etabliert, denen entsprechende Aufgaben zugeordnet sind:

> Für alle Fragen der Informations– und IT–Sicherheit ist der **Chief Information Security Officer** (CISO) verantwortlich.

> Der Leiter der für die gesamte Infrastruktur und den Betrieb verantwortlichen IT–Abteilung wird auch als **Chief Information Officer** (CIO) bezeichnet.

> Der **Informationssicherheitsbeauftragte** (ISB) ist gemäß Informationssicherheitsgesetz in jedem Bundesministerium (verpflichtend) einzurichten und überwacht primär die Einhaltung dieses Bundesgesetzes.

> Der **Chief Digital Officer** (CDO) ist für die Digitalisierungsstrategie und Digitalisierungsmaßnahmen eines Bundesministeriums zuständig.

**Handlungsfelder**

- Die überprüften Bundesministerien verfügten grundsätzlich über eine IT–Sicherheitsorganisation auf Grundlage des Österreichischen Informationssicherheitshandbuchs.

- Einzelne Sicherheitsorganisationen wichen vom Standard ab:

> Ein Chief Information Security Officer (CISO) war nicht direkt eingerichtet. Damit fehlte die für die Informations– und IT–Sicherheit zuständige Funktion.

> Der Leiter der IT–Abteilung (Chief Information Officer) war zugleich Chief Information Security Officer (CISO). Damit war diese Sicherheitsfunktion nicht unabhängig von der operativen Umsetzung.

> Ein Chief Digital Officer war nicht eingerichtet. Damit fehlte die für die Digitalisierungsstrategie und Digitalisierungsmaßnahmen zuständige Funktion.

**EMPFEHLUNGEN AUS RH–BERICHTEN:**

In jedem Bundesministerium wären eine Digitalisierungsstrategie oder ähnliche strategische Festlegungen zu erarbeiten. Darin wäre insbesondere auf die Herausforderungen im Zusammenhang mit der Digitalisierung der Arbeits– und Geschäftsprozesse und der Telearbeit Bezug zu nehmen.

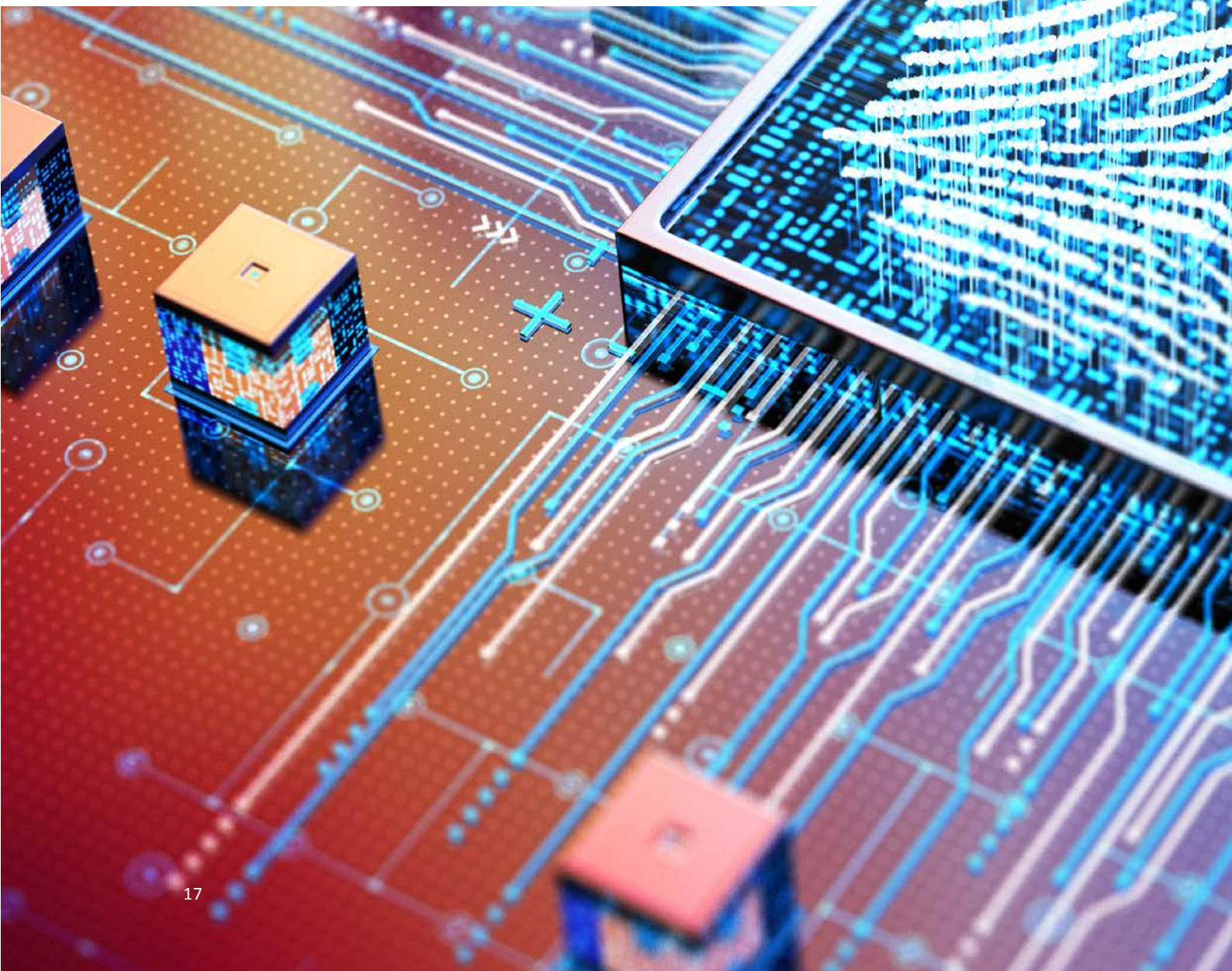
Die IT–Sicherheitsstrategie wäre auf Ressortebene als Grundlage des IT–Sicherheitsmanagements zu erstellen und für alle Bediensteten transparent in Kraft zu setzen. Sie sollte klare Ziele, Verantwortlichkeiten, einschließlich der Unterstützung durch die Ressortleitung („Management Commitment"), und nachvollziehbare Methoden des IT–Sicherheitsmanagements festlegen. Sie wäre bedarfsgerecht zu aktualisieren.

Im Rahmen des Projekts Security Framework Bund wären einheitliche verbindliche Sicherheitsstandards für die IKT der öffentlichen Verwaltung zu erarbeiten.

Die Funktionen Chief Information Security Officer (CISO), Chief Information Officer (CIO) und Chief Digital Officer (CDO) wären zu besetzen und voneinander unabhängig einzurichten.

# IT–SICHERHEIT DES BUNDES

## *IT–Arbeitsplätze und Telearbeit*



# IT–ARBEITSPLÄTZE UND TELEARBEIT

**Der IT–Arbeitsplatz ist zunehmend ortsungebunden. Um dennoch alle Funktionen und die umfassende Sicherheit der Daten des IT–Arbeitsplatzes zu gewährleisten, sind technische und organisatorische Maßnahmen zu implementieren.**

## EINSATZ PRIVATER UND DIENSTLICHER AUSSTATTUNG

Ab 2005 konnten Bedienstete in den Bundesministerien ihren Dienst in Form von Telearbeit zu Hause (Homeoffice) regelmäßig tageweise verrichten, sofern sie und ihr Arbeitsplatz die Voraussetzungen erfüllten. Die dafür erforderliche IT–Ausstattung war vom Dienstgeber bereitzustellen. Im Februar 2020 lag der Anteil der Bediensteten, denen Telearbeit (im Ausmaß von ein bis zwei Tagen pro Woche) gewährt wurde, in den überprüften Bundesministerien zwischen 6 % und 22 %.

Während der COVID–19–Pandemie arbeitete ein Großteil der Bundesbediensteten in der Verwaltung der Zentralstellen phasenweise im Homeoffice. Dies wurde durch Ministerratsbeschlüsse ab 16. März 2020 ermöglicht. Die Bediensteten mussten zur Dienstverrichtung teilweise private IT–Ausstattung verwenden. Diese wurde in der Regel über einen gesicherten IT–Zugang mit den zentralen Systemen vernetzt – dabei werden die IT–Anwendungen nur zentral ausgeführt. Durch diese Maßnahmen konnte der Dienstbetrieb unter Berücksichtigung des Gesundheitsschutzes aufrechterhalten werden.

Die überprüften Bundesministerien ersetzten in der Folge ihre stationären IT–Arbeitsplätze schrittweise durch mobile. Im Dezember 2023 wies nur noch eines der überprüften Bundesministerien keine Vollausstattung an mobilen dienstlichen Geräten auf. Die Vollausstattung sollte bis Mitte 2024 erreicht werden.

Die Bundesministerien hatten nicht festgelegt, welche konkreten dienstlichen Aufgaben aus Sicherheitsgründen nur an der Dienststelle zu verrichten sind und welche aus Sicherheitsgründen für Telearbeit nicht geeignet sind.

**Handlungsfelder**

- Der Einsatz privater IT–Ausstattung für den Dienstbetrieb im Homeoffice birgt Sicherheitsrisiken. Diese Risiken sind beispielsweise folgende:

> Dienstliche Daten bleiben auf privaten Geräten gespeichert.

> Die für dienstliche Aufgaben verwendete private IT–Ausstattung wird auch von anderen Personen genutzt.

> Die private IT–Ausstattung, die die IT–Anwendungen des Ressorts im Homeoffice nutzt, weist im Vergleich mit den dienstlichen Geräten geringere Sicherheitsvorkehrungen auf.

- Auch bei Verwendung eines dienstlichen mobilen IT–Arbeitsplatzes für Homeoffice besteht das Risiko, dass im Homeoffice nicht befugte (aber z.B. haushaltszugehörige) Personen Zugang zu sicherheitsrelevanten bzw. sicherheitsklassifizierten Informationen bekommen.

## VIDEOKONFERENZSYSTEME

Aufgrund des in der COVID–19–Pandemie angeordneten Homeoffice war es ab März 2020 für die Bundesministerien wichtig, rasch Videokonferenzsoftware für die IT–Arbeitsplätze zu beschaffen. Dies sollte die Zusammenarbeit innerhalb eines Ressorts und zwischen den Ressorts im Wege elektronischer Kommunikation unterstützen. In den überprüften Bundesministerien – drei im Jahr 2020, sechs im Jahr 2021 und drei im Jahr 2022 – kamen zahlreiche unterschiedliche Systeme zum Einsatz. Dabei waren auch innerhalb eines Ressorts bis zu vier unterschiedliche Videokonferenzsysteme in Verwendung.

Das im Jänner 2021 im Rahmen des IT–Konsolidierungsprogramms gestartete Projekt „Videokonferenzsystem Bund" sollte bis Ende 2021 eine einheitliche Videokonferenzlösung für den Bund bereitstellen. Die Bestrebungen des Bundes zum Einsatz eines einheitlichen Videokonferenzsystems waren zweckmäßig. Das Projekt war laut Stellungnahme des Finanzministeriums mit 31. Oktober 2023 abgeschlossen.

**Handlungsfelder**

- Der Einsatz unterschiedlicher Videokonferenzsysteme erschwert die elektronische Kommunikation innerhalb eines Ressorts und zwischen den Ressorts. Er erhöht außerdem den Beschaffungs– und Betreuungsaufwand.

## TECHNISCHE SICHERHEITSMASSNAHMEN FÜR DEN IT–ARBEITSPLATZ

Die IT–Sicherheitsrisiken am IT–Arbeitsplatz können durch technische und organisatorische Maßnahmen reduziert werden. Beispiele dafür sind:

> Verschlüsselung der Daten auf den Festplatten der mobilen Arbeitsplätze
Die Verschlüsselung reduziert das Risiko, dass bei einem Verlust des Arbeitsplatzrechners bzw. bei einem unerlaubten Zugang zum Arbeitsplatzrechner die auf diesem Computer gespeicherten Daten missbräuchlich verwendet oder manipuliert werden.

> Verhinderung des Startens eines externen Betriebssystems (Booten) von externen Datenträgern auf den mobilen IT–Arbeitsplätzen
Dadurch reduziert sich das Risiko eines missbräuchlichen Zugangs zu den auf diesem IT–Arbeitsplatzrechner gespeicherten Daten bzw. das Risiko, dass diese Daten verändert werden.

> USB–Port–Deaktivierung bzw. USB–Port–Kontrolle
Sie reduziert das Risiko, Schadsoftware zu laden, oder den missbräuchlichen Zugang mit Hardwaretools am USB–Port.

> Applikations–Whitelisting
Das Whitelisting gewährleistet, dass nur explizit erlaubte Anwendungen auf den IT–Arbeitsplätzen gestartet werden können.

> Verschlüsselter Datenaustausch (Virtual Private Network) zwischen mobilem Arbeitsplatz und zentraler IT–Infrastruktur
Die Verschlüsselung reduziert das Risiko, dass Unbefugte die übertragenen Daten ausspähen können.

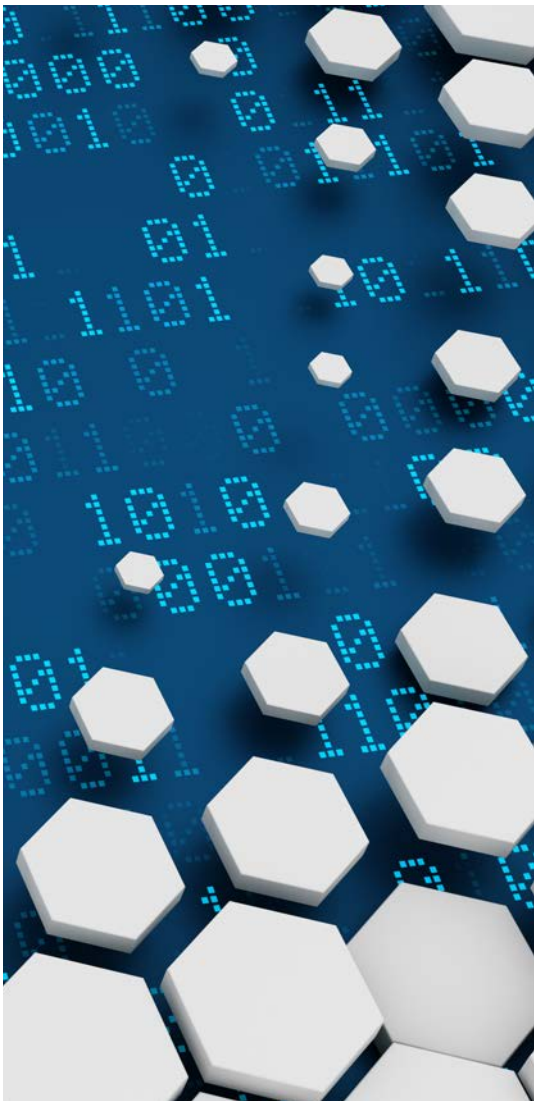
> Virenschutz bzw. Schutz vor Schadsoftware
Er schützt IT–Arbeitsplätze vor Viren, Trojanern, Ransomware, Spyware etc.

> Endpoint–Protection–System
Dadurch soll ein aktiver Schutz für alle Endgeräte gewährleistet werden. Cyber–Bedrohungen sollen direkt am Endgerät – dort, wo sensible Daten gespeichert werden bzw. gespeichert werden können – effektiv identifiziert, eingedämmt und eliminiert werden.

> Auto–Virtual–Private–Network–Funktion
Sie baut – sobald eine Netzwerkverbindung besteht – automatisch eine generierte verschlüsselte Verbindung vom IT–Arbeitsplatz zu den zentralen IT–Systemen des Bundesministeriums auf. Dadurch ist gewährleistet, dass alle Verbindungen ins Internet über die zentralen IT–Systeme geführt und dass deren Sicherheitsmechanismen genutzt werden.

> (Automatisierte) Software–Updates des IT–Arbeitsplatzes
Die Updates stellen grundsätzlich sicher, dass die installierten Softwarekomponenten aktuell sind und dem neuesten Stand an Sicherheitsvorkehrungen entsprechen.

> Zwei–Faktor–Authentifizierung
Sie dient dem erweiterten Schutz gegen unbefugte Verwendung beim Starten des IT–Arbeitsplatzes.



# Maßnahmen zur Erhöhung der IT–Sicherheit zentraler IT–Systeme


**Verschlüsselung der Daten auf den Festplatten**
reduziert das Risiko, die gespeicherten Daten missbräuchlich zu verwenden oder zu manipulieren

**Verhinderung des Startens eines externen Betriebssystems**
reduziert das Risiko eines missbräuchlichen Zugangs auf diesem IT–Arbeitsplatz

**USB–Port–Deaktivierung**
reduziert das Risiko, Schadsoftware zu laden

**Applikations–Whitelisting**
nur explizit erlaubte Anwendungen können gestartet werden

**verschlüsselter Datenaustausch**
zwischen mobilem Arbeitsplatz und zentraler IT–Infrastruktur

**Schutz vor Schadsoftware**
schützt IT–Arbeitsplätze vor Viren, Trojanern, Ransomware, Spyware

**Endpoint–Protection–System**
dient dazu, Cyber–Bedrohungen direkt am Endgerät effektiv zu identifizieren, einzudämmen und zu eliminieren

**Auto–Virtual Private Network–Funktion**
automatisch generierte verschlüsselte Verbindung vom IT–Arbeitsplatz zu den zentralen IT–Systemen

**(automatisierte) Software–Updates**
stellen sicher, dass installierte Softwarekomponenten aktuell sind

**Zwei–Faktor–Authentifizierung**
Schutz gegen unbefugte Verwendung beim Starten des IT–Arbeitsplatzes

Quelle: RH; Darstellung: RH

**Handlungsfelder**

- Die überprüften Bundesministerien setzten wichtige technische Sicherheitsvorkehrungen am IT–Arbeitsplatz um.

- In Einzelfällen fehlten folgende Sicherheitsmaßnahmen:

> das Unterbinden des Startens von externen Datenträgern

> die USB–Port–Deaktivierung bzw. USB–Port–Kontrolle

> das Applikation–Whitelisting für die IT–Arbeitsplätze

> das Endpoint–Protection–System

> die AutoVirtual–Private–Network–Funktionalität

> die Zwei–Faktor–Authentifizierung

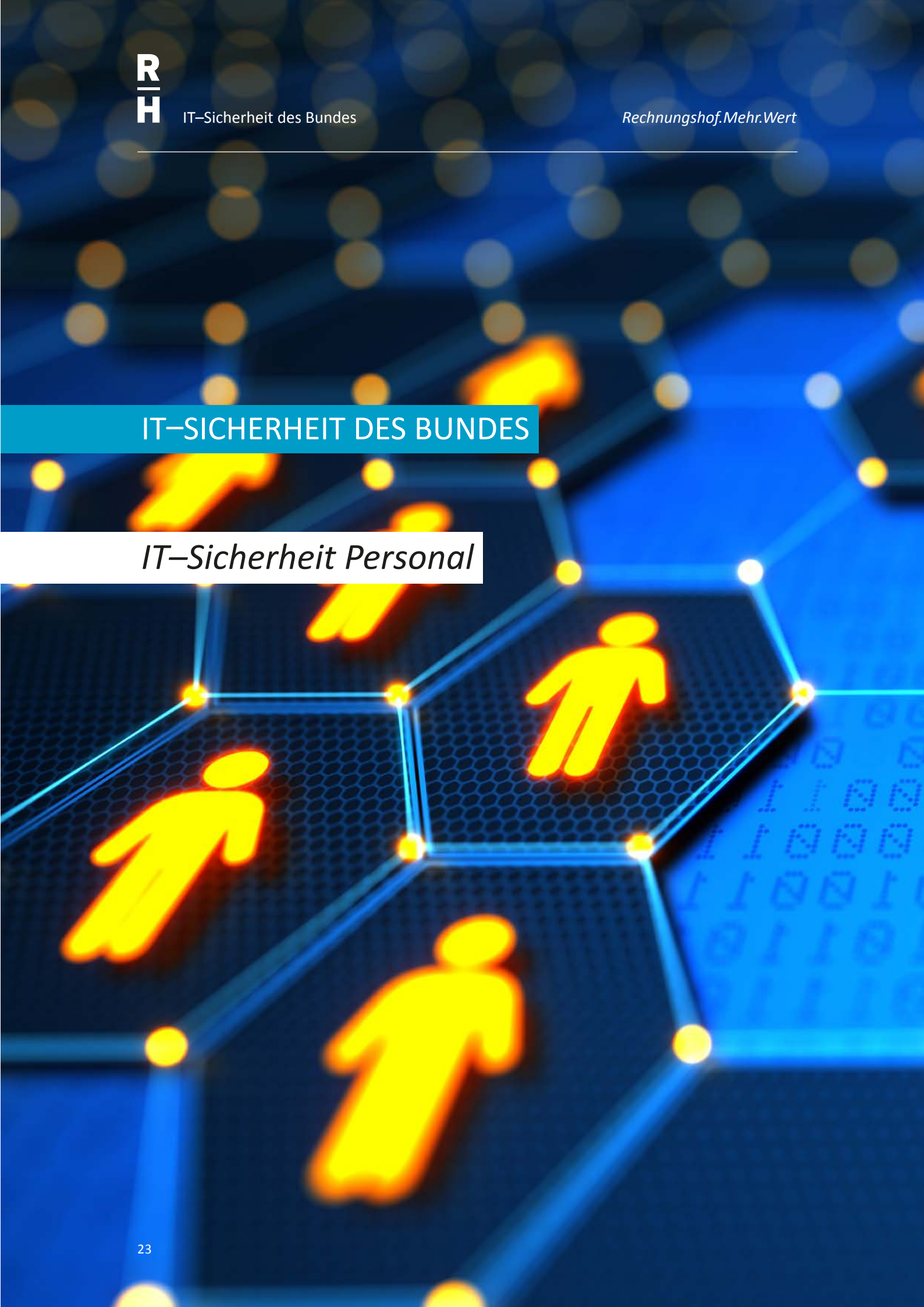
**EMPFEHLUNGEN AUS RH–BERICHTEN:**

Im regulären Dienstbetrieb sollte der Einsatz privater IT–Ausstattung für Telearbeit aufgrund von Sicherheitsrisiken nicht vorgesehen werden.

Es wäre konkret festzulegen, ob bestimmte dienstliche Aufgaben jedenfalls aus Sicherheitsgründen an der Dienststelle und nicht in Telearbeit zu verrichten sind.

Die Anzahl der innerhalb eines Ressorts eingesetzten Videokonferenzsysteme wäre auf das erforderliche Maß zu verringern.

Die Ressorts sollten ihre jeweiligen technischen IT–Sicherheitsmaßnahmen für den IT–Arbeitsplatz einer Risikoanalyse unterziehen, den Bedarf an technischen Sicherheitsmaßnahmen prüfen und erforderlichenfalls weitere technische Maßnahmen setzen.



# IT–SICHERHEIT DES BUNDES

## *IT–Sicherheit Personal*

# IT–SICHERHEIT PERSONAL

Vom analogen Schlüssel, der den Bediensteten zu Dienstbeginn gegen Unterschrift ausgehändigt wurde, bis zur Zwei–Faktor–Authentifizierung mit Token und Passwort: Durch die Digitalisierung des Arbeitsplatzes haben sich auch die personellen IT–Sicherheitsvorkehrungen geändert. Die personelle IT–Sicherheit ist durch entsprechende organisatorische Regelungen für internes und externes Personal sicherzustellen.

## REGELUNGEN UND SICHERHEITS-MASSNAHMEN FÜR INTERNES PERSONAL

Neben den technischen Maßnahmen zur Erhöhung der IT–Sicherheit sind auch organisatorische Maßnahmen insbesondere für das Personal erforderlich. Die nachfolgend gemäß Österreichischem Informationssicherheitshandbuch beispielhaft angeführten generellen Regelungen sowie Maßnahmen zur Gewährleistung der IT–Sicherheit des ressortinternen Personals waren in den überprüften Bundesministerien grundsätzlich vorgesehen und in Prozessabläufen geeignet festgelegt:

| Maßnahmen zur personellen IT–Sicherheit |
|---|
| **Regelungen betreffend personelle IT–Sicherheit** |
| Richtlinie zur Nutzung der IKT |
| Passwort–Richtlinie |
| Richtlinie zu mobilen Endgeräten |
| Erläuterungen zum Datenschutz |
| Regelungen zur Telearbeit |
| Regelungen zur elektronischen Kommunikation |
| Regelungen zur Privatnutzung |
| Umgang mit klassifizierten Informationen |
| **Maßnahmen vor Beginn des Dienstverhältnisses** |
| Überprüfung der Qualifikation der Bediensteten im Aufnahmeverfahren |
| Arbeitsplatzbeschreibungen mit IT–sicherheitsrelevanten Aufgaben (z.B. Mitglieder des IT–Sicherheitsmanagement–Teams) |
| Überprüfung der Vertrauenswürdigkeit (z.B. Strafregisterauszug, Sicherheitsüberprüfung nach Informationssicherheitsgesetz) |
| Verpflichtungserklärung hinsichtlich Geheimhaltung |
| Verpflichtungserklärung hinsichtlich IKT–Nutzung |
| **Maßnahmen während des Dienstverhältnisses** |
| laufende Awareness–Schulungen |
| Weiterbildung IT–Personal |
| Informationen zu Support, Anforderungs– und Meldewegen |
| Informationen zu aktuellen Nutzungsregelungen |
| Vertretungsregelungen IT–Personal |
| Informationen über Sicherheitsvorfälle (Sicherheitsempfehlungen und Meldestruktur) |
| **Maßnahmen nach Ende des Dienstverhältnisses** |
| strukturierter Personalprozess bei Beendigung des Dienstverhältnisses mit vorgegebenem Prozessablauf |
| Sicherstellung von Daten und Ausstattung |
| Entzug von Zugangs– und Zugriffsberechtigungen |

**Handlungsfelder**

- Regelungen zur IT–Sicherheit des Personals waren vorgesehen und Prozessabläufe eingerichtet.

- In Einzelfällen wichen die Bundesministerien in ihren organisatorischen Maßnahmen zur personellen IT–Sicherheit von den Vorgaben ab:

> Die Richtlinien zur Nutzung mobiler Endgeräte waren erst in Ausarbeitung.

> Die Regelungen zur Telearbeit waren noch nicht in einer Richtlinie zusammengefasst.

> Der Umgang mit klassifizierten Informationen war in ressortspezifischen Dokumenten nicht festgelegt.

> Die Awareness–Schulungen zur IT–Sicherheit waren nicht verpflichtend.

> Ein Teil der Vertretungsregelungen von IT–Schlüsselpersonal wurde nur anlassbezogen festgelegt.

## REGELUNGEN UND SICHERHEITSMASSNAHMEN FÜR EXTERNES PERSONAL

Alle überprüften Bundesministerien setzten externe IT–Dienstleister ein. Die regelmäßigen Dienstleistungen betrafen – in jedem Ressort in unterschiedlichem Ausmaß – beispielhaft

- die Anwenderbetreuung,
- den Second Level Support,
- die Betriebsführung und Wartung der zentralen Infrastruktur oder
- den Betrieb von IT–Sicherheitsmaßnahmen.

First Level Support ist der Erstkontakt zur Lösung technischer Probleme der Anwender. Second Level Support ist die zweite Ebene zur Lösung technischer Probleme mit vertieften inhaltlichen Kenntnissen und erhöhtem technischem Handlungsspielraum.

Folgende Maßnahmen sind beim Einsatz externen Personals zur Gewährleistung der IT–Sicherheit erforderlich:

Maßnahmen zur personellen IT–Sicherheit bei Einsatz von externem Personal

| Maßnahmen externes Personal |
|---|
| IT–Sicherheitsanforderungen als Vertragsbestandteil |
| vertragliche Festlegung der Qualifikationen des externen Personals |
| vertragliche Festlegung der Geheimhaltungspflichten |
| vertragliche Festlegung der Pflichten hinsichtlich Datenschutz |
| Überprüfung der Vertrauenswürdigkeit durch Sicherheitsüberprüfung nach § 55 Sicherheitspolizeigesetz |
| Einhaltung der IT–Sicherheitsvorgaben des Ressorts durch Überbindung der wesentlichen Regelungen |
| Informationssicherheitsmanagementsystem beim Auftragnehmer |

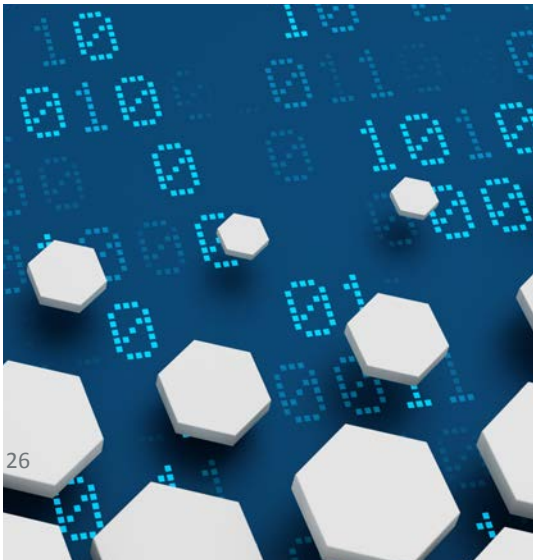
**Handlungsfelder**

- Maßnahmen zur Gewährleistung der IT–Sicherheit beim Einsatz von externem Personal setzten die überprüften Bundesministerien grundsätzlich um.

- In Einzelfällen waren Risiken noch nicht angemessen bewältigt:

> Das Personal eines externen Dienstleisters mit dem Aufgabenbereich des Second Level Supports hatte seinen Arbeitsort im EU–Ausland. Es waren zwar hierzu vertragliche Regelungen festgelegt, u.a. zu Geheimhaltung, Datenschutz und Einhaltung der Sicherheitsvorgaben. Die in diesem Aufgabenbereich erforderlichen Sicherheitsüberprüfungen erfolgten allerdings mithilfe der örtlich zuständigen ausländischen Behörden. Eine unmittelbare Aufsicht und Kontrolle des externen Personals durch den Auftraggeber und Auftragnehmer war durch den Arbeitsort im EU–Ausland erschwert.

> Ein externer Dienstleister hatte einen permanenten Fernwartungszugriff für zentrale Systeme. Dieser war teilweise mit Administratorrechten privilegiert.



**EMPFEHLUNGEN AUS RH–BERICHTEN:**

Die Gewährleistung der IT–Sicherheit durch die Anwender ist durch entsprechende Regelungen, verpflichtende Schulungen und regelmäßige Weiterbildungsmaßnahmen sicherzustellen.

Beim Einsatz von externem IT–Personal mit Zugriff auf sicherheitskritische Bereiche wären die Risiken hinsichtlich der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der im Ressort verarbeiteten Daten derart zu berücksichtigen, dass der Dienstleister und der Auftraggeber unmittelbar Kontrolle und Überprüfungsmöglichkeiten über das externe IT–Personal haben. Dies kann bei einem Dienstort Österreich möglicherweise effektiver sichergestellt werden als bei einem Arbeitsort im EU–Ausland.

Fernwartungszugriffe auf zentrale Systeme wären für externe Dienstleister nur anlassbezogen und zeitlich begrenzt zu gewähren.

# IT–SICHERHEIT DES BUNDES

## *IT–Sicherheit der zentralen IT–Systeme*

# IT–SICHERHEIT DER ZENTRALEN IT–INFRASTRUKTUR

Waren die Papierakten durch Eisenschränke oder Ähnliches vor Zerstörung durch Feuer zu schützen, sind in der digitalen Arbeitswelt Firewalls Teil der Sicherheitsstruktur. Die Funktion und die Sicherheit der Daten der zentralen IT–Infrastruktur sind durch umfassende technische und organisatorische Maßnahmen zu gewährleisten.

## TECHNISCHE MASSNAHMEN ZUR ERHÖHUNG DER SICHERHEIT DER ZENTRALEN IT–SYSTEME

Ziel von technischen Maßnahmen ist es, die IT–Sicherheit der zentralen IT–Komponenten und in der Folge die der zentralen IT–Anwendungen zu erhöhen. Dabei sollen Maßnahmen eingesetzt werden, die unter Berücksichtigung von Kosten–Nutzen–Erwägungen die Erreichung eines hohen Sicherheitsniveaus erwarten lassen.

Im Einzelnen sind beispielhaft folgende technische Maßnahmen geeignet, die IT–Sicherheitsrisiken für die zentrale IT–Infrastruktur zu reduzieren:

> ein (netzwerkbasiertes) Intrusion Detection System (IDS) bzw. Intrusion Prevention System (IPS) zur Erkennung und Verhinderung von Angriffen

> Firewalls, um die unerwünschte Netzwerkverbindungen vom Internet in das lokale Netz zu unterbinden und umgekehrt vom lokalen Netz ins Internet

> Spamfilter zur Unterdrückung unerwünschter E–Mails

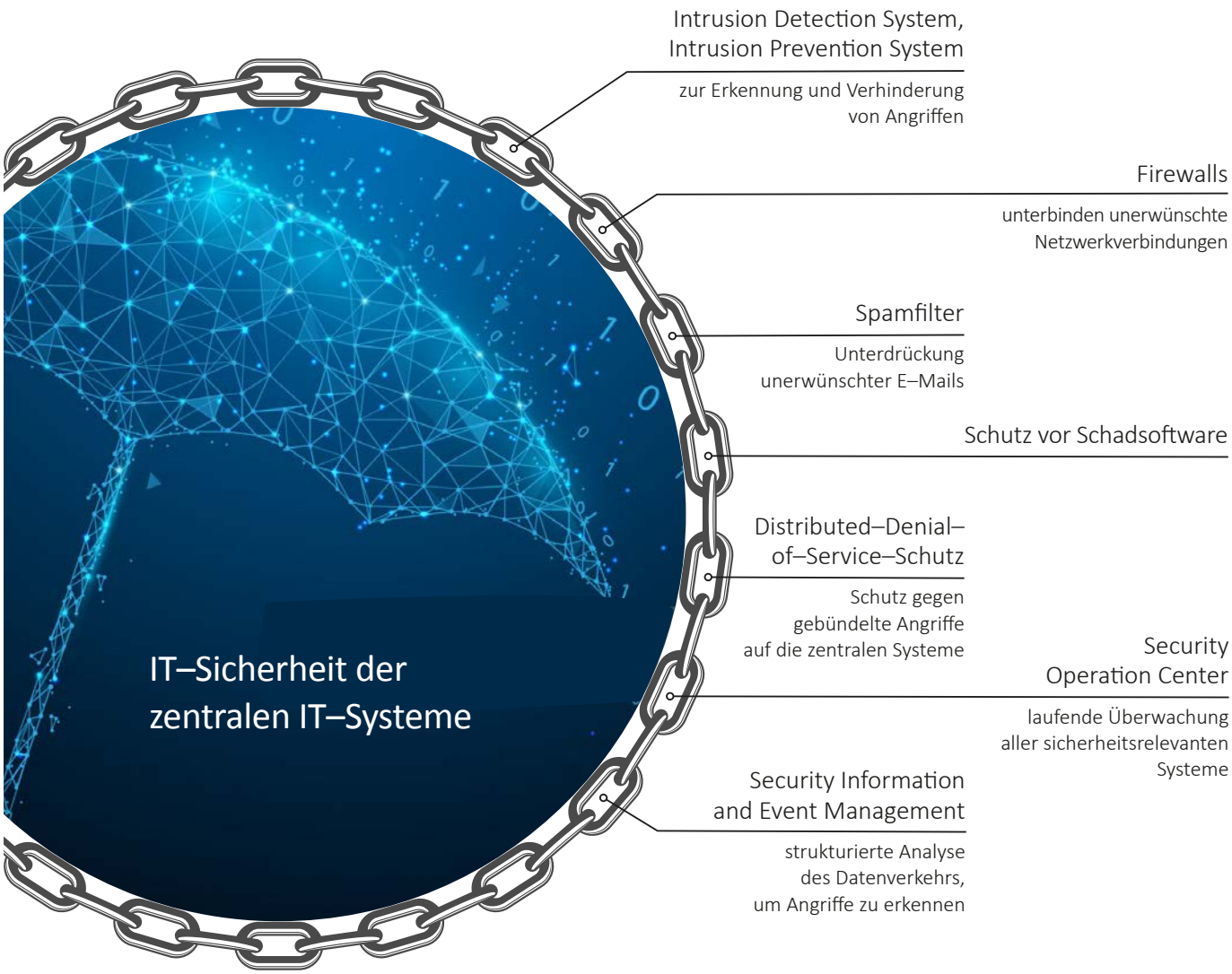
> Schutz vor Schadsoftware für die zentralen Systeme, etwa Viren, Trojaner, Ransomware, Spyware etc.

> DDoS–Schutz (Distributed–Denial–of–Service–Schutz) gegen gebündelte Angriffe auf die zentralen Systeme; Ziel solcher gebündelter Angriffe ist es, das System mithilfe einer Vielzahl von Anfragen zu blockieren oder funktionsunfähig zu machen; ein DDoS–Schutz erfordert im Allgemeinen Unterstützung durch den Internetdienstanbieter, damit IP–Adressen blockiert werden

> ein Security Information and Event Management (SIEM) zur strukturierten Analyse des Datenverkehrs; damit sollen Angriffe bzw. ungewöhnliches Verhalten im Netz erkannt werden und gegebenenfalls Gegenmaßnahmen ergriffen werden; diese Systeme klassifizieren und protokollieren teilweise automatisiert sicherheitskritische Vorfälle

> ein Security Operation Center (SOC), das in der Regel auf Grundlage der Ergebnisse des Security Information and Event Managements (SIEM) alle sicherheitsrelevanten Systeme (Netzwerke, Server, Clients, Webservices etc.) überwacht und analysiert.

# Maßnahmen zur Erhöhung der IT–Sicherheit zentraler IT–Systeme




Quelle: RH; Darstellung: RH

**Handlungsfelder**

- Die überprüften Bundesministerien setzten wichtige technische Sicherheitsvorkehrungen für die zentrale IT–Infrastruktur um.

- Einzelne Sicherheitsmaßnahmen fehlten:

> das System zur Erkennung bzw. Verhinderung von Angriffen – Intrusion Detection System (IDS) bzw. Intrusion Prevention System (IPS),

> ein Security Information and Event Management (SIEM) zur strukturierten Analyse des Datenverkehrs und

> ein Security Operation Center (SOC) zur Überwachung der sicherheitsrelevanten Systeme.

## IT–SICHERHEITS–AUDITS

Ziel von IT–Sicherheits–Audits ist es, die Wirksamkeit der getroffenen technischen und organisatorischen IT–Sicherheitsmaßnahmen zu überprüfen. Diese Überprüfungen sollten auf einer umfangreichen Risikoanalyse beruhen. Sie können – bei vorhandener Expertise – durch die jeweilige Organisation selbst oder von externen Spezialistinnen und Spezialisten durchgeführt werden, zum Teil auch automatisiert, z.B. Penetration–Tests, Port–Scans, Schwachstellen–Scans. Einem Best–Practice–Ansatz entsprechen u.a. folgende spezifischen IT–Sicherheits–Audits:

> Prozess–Audits zur Beurteilung einzelner Prozesse

> System–Audits zur Betrachtung des IT–Managementsystems

> Netzwerk–Audits zur Analyse von Netzwerken, IT und Infrastruktur

> Social Engineering Audits zur Überprüfung von Verhaltensregeln von Mitarbeiterinnen und Mitarbeitern

> Datenschutz–Audits, z.B. zur Überprüfung, ob die Anforderungen der Datenschutz–Grundverordnung erfüllt werden

> Vulnerability Scannings zur Analyse und Identifizierung von Schwachstellen

> Penetration Testing zur Überprüfung von Systemen aus der Sicht eines Angreifers,

> Compliance Audits zur Überprüfung, ob gesetzliche Vorschriften und Richtlinien im IT–Bereich eingehalten werden

> technische Audits zur Beurteilung technischer Systeme

> Produkt–Audits zur Beurteilung eines Produkts anhand der Kundenerwartungen

> Projekt–Audits zur Beurteilung der Einhaltung der Projektvorgaben

**Handlungsfelder**

- Nur zwei der genannten IT–Sicherheits–Audits wurden in allen überprüften Bundesministerien eingesetzt: die Vulnerability Scannings und das Penetration Testing.
- Die anderen Sicherheits–Audits wendeten die Ressorts nicht an oder sie waren erst in Planung. Damit waren die IT–Sicherheitsmaßnahmen in diesen Ressorts nicht nachweislich auf ihre Funktion und Effektivität überprüft.

## NOTFALLMANAGEMENT

Die nachfolgende Tabelle gibt einen Überblick, über die für ein Notfallmanagement erforderlichen Maßnahmen:

| Erforderliche Maßnahmen für das Notfallmanagement |
|---|
| **Notfallkonzepte und –szenarien** |
| IT–Notfallhandbuch bzw. Notfallkonzepte |
| IT–Notfallszenarien bzw. IT–Notfallpläne |
| Definition der Kriterien für den Eintritt eines IT–Notfalls |
| Definition einer IT–Notfallorganisation (Festlegung zuständiger Organisationseinheiten) |
| Analyse der sicherheitskritischen IT–Systeme, –Dienste und –Anwendungen |
| **Festlegung der sicherheitskritischen IT–Systeme, IT–Dienste und IT–Anwendungen** |
| Definition der IT–Notfallprozesse |
| Wiederherstellungsverfahren |
| Systeme zur laufenden Überwachung sowie Dokumentation durch Berichtswesen |
| **Überprüfung des Notfallmanagements** |
| eigene Testung der Notfallszenarien |
| externe Überprüfung des Notfallmanagements |

**Handlungsfelder**

- Die überprüften Bundesministerien setzten wichtige Vorkehrungen für ein Notfallmanagement ihrer IT–Infrastruktur um.

- In Einzelfällen lagen Mängel vor:

> Ein Notfallhandbuch sowie Notfallkonzepte fehlten bzw. waren nicht mehr aktuell.

> Notfallszenarien waren nicht definiert und Notfallpläne nicht festgelegt.

> Die Kriterien für den Eintritt eines Notfalls waren nicht oder nicht klar beschrieben.

> Eine Notfallorganisation war nicht oder nur für Teilbereiche vorhanden.

- Alle Ressorts hatten sicherheitskritische Bereiche und Wiederherstellungsverfahren festgelegt, in Einzelfällen fehlten die Notfallprozesse für einzelne Verfahren.

- Die Überprüfung des Notfallmanagements erfolgte in den meisten Bundesministerien durch regelmäßige Testung der Notfallszenarien. Externe Überprüfungen ließen die meisten Bundesministerien nicht durchführen.

**EMPFEHLUNGEN AUS RH–BERICHTEN:**

Die Bundesministerien sollten ihre technischen Maßnahmen zur Erhöhung der IT–Sicherheit der zentralen IT–Infrastruktur dahingehend regelmäßig prüfen, ob diese umfassend sind und dem aktuellen Stand der Technik entsprechen. Dabei wäre auch zu evaluieren, ob die Maßnahmen einen effektiven Beitrag zur Verbesserung der IT–Sicherheit mit sich bringen würden. Erforderlichenfalls wären diese anzuwenden.

Die Bundesministerien sollten den Bedarf an IT–Sicherheits–Audits basierend auf einer umfassenden Risikoanalyse erheben. Die notwendigen IT–Sicherheits–Audits wären zu priorisieren und zeitnah unter Berücksichtigung der verfügbaren Ressourcen und bedarfsgerecht unter Einbindung von externem Fachwissen durchzuführen.

Für die Sicherstellung der Kontinuität des IT–Betriebs ist ein umfassendes Notfallmanagement mit Notfallhandbuch und Notfallkonzepten erforderlich. Dafür sind die Risiken der wichtigen IT–Systeme, IT–Dienste und IT–Verfahren anhand definierter Notfallszenarien zu bewerten. Die Risikobewertung sollte Grundlage für die IT–Notfallprozesse und –Maßnahmen sowie für Wiederherstellungsverfahren sein. Das Notfallmanagement wäre regelmäßig intern und extern zu überprüfen.

## RH–PRÜFUNGEN ZUR IT–SICHERHEIT DES BUNDES

| Berichtstitel | Vorlage | Reihe Bund |
|---|---|---|
| Management der IT–Sicherheit in der Verwaltung ausgewählter Bundesministerien | 10.09.21 | 2021/31 |
| Dienstrechtliche und technische Umsetzung von Telearbeit in ausgewählten Bundesministerien | 09.09.22 | 2022/27 |
| Umstellung von der Bürgerkarte/Handysignatur (E–ID) auf den elektronischen Identitätsnachweis | 03.03.23 | 2023/7 |
| Management der IT–Sicherheit im Finanzministerium, Klimaschutzministerium und Landwirtschaftsministerium | 24.05.24 | 2024/16 |

Rechnungshof Österreich

Wien, im September 2024
Die Präsidentin:

Dr. Margit Kraker

## FOTOS

| | |
|---|---|
| Umschlag: | iStock@JuSun |
| S. 4: | iStock@JuSun (5x); iStock@BlackJack3D |
| S. 5: | Rechnungshof@Achim Bieniek (2x) |
| S. 6: | Rechnungshof@Manuel Brenner |
| S. 9: | iStock@JuSun |
| S.13: | iStock@JuSun |
| S. 14 und 15: | iStock@JuSun |
| S. 17: | iStock@BlackJack3D |
| S. 20: | iStock@JuSun |
| S. 21: | iStock.com/Who_I_am; iStock@art-sonik |
| S. 23: | iStock@JuSun |
| S. 26: | iStock@JuSun |
| S. 27: | iStock@JuSun |
| S. 29: | iStock.com/Who_I_am; iStock@art-sonik |


R
H