Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

**Nationales Zentrum für Cybersicherheit NCSC**
Informatiksicherheit Bund

13. April 2022

# Bericht Informatiksicherheit Bund 2021

# Inhalt

# 1 Organisation der Informatiksicherheit in der Bundesverwaltung

Die Informatiksicherheit in der Bundesverwaltung umfasst alle Massnahmen um einen Cybervorfall zu vermeiden. Dabei geht es darum, ein unbeabsichtigtes oder von Unbefugten beabsichtigtes Ereignis, welches die Vertraulichkeit, Integrität, Verfügbarkeit oder Nachvollziehbarkeit von Daten beeinträchtigt oder zu Funktionsstörungen führt, zu verhindern[1].
Der Bundesrat erlässt dazu Verordnungen und Weisungen über den Schutz der Bundesverwaltung vor Cyberrisiken. Der Delegierte für Cybersicherheit erlässt dazu weitere Informatiksicherheitsvorgaben.
Zudem fungiert der Ausschuss Informatiksicherheit (A-IS) als Konsultativorgan für das Nationale Zentrum für Cybersicherheit (NCSC) betreffend Informatiksicherheitsfragen in der Bundesverwaltung.
Die Verwaltungseinheiten sind für den Schutz ihrer Informatiksysteme, Anwendungen und Daten (Schutzobjekte) verantwortlich. Dazu prüfen sie ihre Schutzobjekte regelmässig und ergreifen die notwendigen Sicherheitsmassnahmen. Zudem sind sie für die Einhaltung und die Umsetzung der Informatiksicherheitsvorgaben, der Sicherheitsverfahren und der Beschlüsse des Bundesrates, des NCSC und der Departemente beziehungsweise der Bundeskanzlei in ihrem Zuständigkeitsbereich verantwortlich.

# 2 Aktueller Stand der Informatiksicherheit in der Bundesverwaltung

Gestützt auf Artikel 11 Absatz 2 der Cyberrisikenverordnung (CyRV; SR 120.73) informiert der Delegierte für Cybersicherheit das EFD zuhanden des Bundesrates regelmässig über den Stand der Informatiksicherheit in den Departementen und der Bundeskanzlei. Dazu erstellt er jährlich den «Bericht Informatiksicherheit Bund».
Als Grundlage für den Bericht dienen die Berichte der Departemente, der Parlamentsdienste sowie der Bundeskanzlei (Artikel 13 Absatz 1 CyRV, Selbstdeklaration basierend auf einer strukturierten Umfrage), Erfahrungen und Feststellungen des NCSC sowie Sicherheitsmeldungen und -berichte der bundesinternen Leistungserbringer (LE).
Basierend auf den Angaben 2021 stellt das NCSC zusammenfassend fest, dass der aktuelle Sicherheitsstand der Informatik (IT) in der Bundesverwaltung insgesamt der aktuellen Bedrohungslage entspricht und bei Vorkommnissen umgehend die notwendigen Schritte eingeleitet werden.
Dabei ist jedoch zu beachten, dass trotz aufwendiger Sicherheitsvorkehrungen im Bereich der IT, jedes Unternehmen davon ausgehen muss Opfer einer Cyber-Attacke zu werden (Assume-Breach-Paradigma[2]). Diese Feststellung gilt auch für die Bundesverwaltung.
Damit die Implementierung der im IT-Grundschutz bzw. in den Sicherheitskonzepten geforderten Sicherheitsmassnahmen erfolgreich nachgewiesen werden kann, müssen die dazu notwendigen Sicherheitsdokumente aktuell (nicht älter als 5 Jahre) vorhanden sein. Im Bundesdurchschnitt sind bei 90% (Wert wie Vorjahr) aller Schutzobjekte die entsprechenden Sicherheitsdokumente vorliegend. Dies stellt grundsätzlich einen guten Wert dar.
Die Gültigkeit der vorhandenen Sicherheitsdokumente liegt im Bundesdurchschnitt bei 95% (Vorjahr 96%). Fehlende Sicherheitsdokumente werden laufend erarbeitet und wo nötig aktualisiert.

[1] Verordnung vom 27. Mai 2020 über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, CyRV) SR **120.73**

[2] In der Bezeichnung 'Assume-Breach-Paradigma' stecken die englischen Vokabeln 'assume' (=vermuten, annehmen) und 'breach' (=Lücke, Schwachstelle) (Quelle: www.digitalacademy.de)

Die Umsetzung der Sicherheitsmassnahmen sowie deren Kontrolle (Grundschutzmassnahmen sowie Massnahmen aus den ISDS-Konzepten) war 2021 bei 70% aller Schutzobjekte sichergestellt (Vorjahr 57%). Diese Verbesserung ist auf die Anstrengungen der Departemente, die Sicherheitsdokumentationen zu aktualisieren bzw. fehlende Dokumente zu erstellen sowie der Kontrolle der Umsetzung der Massnahmen, zurückzuführen.
Die Steuerung der Umsetzung der Informatiksicherheitsmassnahmen liegt im Auftrag der Leitenden der Verwaltungseinheiten bei den Informatiksicherheitsverantwortlichen der Stufe Departement (ISBD) und Verwaltungseinheit (ISBO).
Alle Stellen der ISBD und ISBO sind besetzt. In den Departementen EDI, WBF und UVEK sind jedoch nur 0,6 Stellen der ISBD besetzt. Gefordert sind jeweils 0,8 Stellen auf Stufe Departement.
Im Zusammenhang mit dem Arbeiten aus dem Homeoffice als Folge der Corona-Massnahmen, traten im Januar 2021 vermehrt Probleme mit der Verfügbarkeit auf (Bandbreite des Internetanschlusses des Bundes). Durch die Homeoffice-Tätigkeiten der Benutzer wurde der Internetanschluss mehr belastet, teilweise gab es Performanceprobleme zum Beispiel mit Skype-Anrufen insbesondere auch mit Videokonferenzen.
Das Bundesamt für Informatik und Telekommunikation (BIT) hat - in Abstimmung mit dem Bereich Digitale Transformation und IKT-Lenkung (DTI) der Bundeskanzlei - einerseits die Bandbreite erhöht und andererseits gewisse Streaming-Dienste gesperrt. Auf der einen Seite wurde das Netzwerk dadurch entlastet und Video-Konferenzen konnten wieder besser durchgeführt werden. Auf der anderen Seite konnten aber Videos im Internet nicht mehr betrachtet werden. Durch weitere Massnahmen konnte jedoch auch dieses Problem gelöst werden.
Es darf festgehalten werden, dass das Arbeiten aus dem Homeoffice grundsätzlich gut funktioniert und bisher keine Sicherheitsvorfälle auf den Homeoffice-Betrieb zurückzuführen sind.

# 3 Sicherstellung der Informatiksicherheit - Faktor Mensch

Die Mitarbeitenden aller Stufen tragen eine wichtige Rolle im Bereich der Informatiksicherheit. Dementsprechend werden die Mitarbeitenden der Bundesverwaltung regelmässig im Umgang mit der Informatiksicherheit sensibilisiert und geschult.
Unter der Leitung der ISBD und ISBO wurden rund 95% der neueintretenden Mitarbeitenden in die Belange der Informatiksicherheit eingeführt (Vorjahr 87%). Diese Verbesserung wurde durch die vermehrte Digitalisierung der Ausbildung während der Corona-Zeit erreicht.
Im Rahmen eines bundesweiten Eintrittspakets für neue Mitarbeitende, erstellt das NCSC zurzeit ein Modul, welches die Belange der Informatiksicherheit abdeckt. Das Modul soll Mitte 2022 der gesamten Bundesverwaltung zur Verfügung stehen.
Verschiedene Departemente und Verwaltungseinheiten führten individuelle Sensibilisierungsmassnahmen z. B. im Bereich Phishing-Mails durch.
Gut besucht wurden die vom NCSC durchgeführten Schulungen im Bereich der Informatiksicherheit. Diese Schulungen wurden im Rahmen des Ausbildungszentrums der Bundesverwaltung (AZB) angeboten. Sie wurden im Jahr 2021 grösstenteils online durchgeführt und durch die Teilnehmenden durchwegs positiv beurteilt.
Zusätzlich wurden neu «Expertenwissenskurse» durch das NCSC angeboten. Diese Kurse haben zum Ziel, den Auf- und Ausbau von Expertenwissen im Cybersicherheitsbereich bei den Mitarbeitenden des NCSC, den ISBD und ISBO sowie anderen interessierten Personen der Bundesverwaltung, die sich mit Fragen der Cybersicherheit befassen, sicherzustellen.
Es darf auch festgehalten werden, dass zahlreiche Mitarbeitende richtig auf Spam- und Phishing-E-Mails reagieren und diese umgehend löschen oder mit dem «Spam-Button», welcher im E-Mail-Programm Outlook zur Verfügung steht, dem LE zur Analyse melden.

Für gezielte Phishing-Angriffe (und auch andere Betrugsversuche) werden oft gehackte E-Mails von externen Stellen (z. B. Lieferanten) missbraucht. Für die Empfänger sind diese oftmals nur schwer als solche erkennbar. In mehreren Fällen waren die Angreifer zunächst auch erfolgreich, weshalb weiterhin Bedarf für Sensibilisierungskampagnen besteht.

# 4 Sicherheitsvorfälle und Schwachstellen

## 4.1 Zusammenfassungen der internen Leistungserbringer

Im Jahr 2021 hat der grösste Leistungserbringer des Bundes, das Bundesamt für Informatik und Telekommunikation (BIT), insgesamt 434 (Vorjahr 834) Sicherheitsvorfälle[3] bearbeitet. Dabei ist festzuhalten, dass nicht jeder Sicherheitsvorfall direkten Schaden für die Bundesverwaltung bedeutet: im Rahmen der Bearbeitung von Sicherheitsvorfällen werden zum Beispiel auch kritische Schwachstellen präventiv untersucht.
Als Leistungserbringer für den IKT-Standarddienst Datenkommunikation ist das BIT, mit dem Computer Security Incident Response Team (CSIRT), für die Netzüberwachung - ausser bei sehr wenigen speziellen Netzwerken[4] - zuständig. Damit können die Vorfälle in den Berichten des CSIRT-BIT als repräsentativ für die ganze zivile Bundesverwaltung bezeichnet werden.
Zusätzlich hat das Cyber Fusion Center (CFC) des LE VBS im Berichtsjahr über 400 interne Meldungen bearbeitet. Das Gros der Meldungen wurde als nicht kritisch eingestuft.
Keine besonderen Vorkommnisse melden die weiteren LE.

## 4.2 Sicherheitsvorfälle

Die Bundesverwaltung wird laufend angegriffen: Das können sehr breit gestreute Angriffe über E-Mails oder gezielte Angriffe auf die IT-Infrastruktur des Bundes oder gegen einzelne Mitarbeitende sein. Dabei reicht das Spektrum der Angreifer von Massen-Spam-Verteiler über die organisierte Kriminalität oder Hacktivisten bis hin zu vermuteten staatlichen Akteuren.

**Eingehende E-Mails**
Das BIT analysiert alle eingehenden E-Mails und sorgt dafür, dass unsicher erscheinende E-Mails gar nicht erst den Empfängern zugestellt werden.
Im Jahr 2021 wurden 34.5% (Vorjahr 48%) der eingehenden E-Mails **gelöscht** noch bevor sie dem Empfänger zugestellt wurden:

| | |
|---|---|
| Eingegangene E-Mails in die Bundesverwaltung | 138'872'079 (Vorjahr rund 160 Mio Mails) |
| Davon zentral gelöscht[5] | 47'955’038 |
| An die Empfänger weitergeleitete E-Mails | 90'917’041 |

[3] Als Sicherheitsvorfall werden alle eingehenden Sicherheitsmeldungen erfasst. Dazu gehören auch Verdachtsfälle, die sich nach der Analyse als harmlos bzw. als falscher Alarm herausstellen oder Phishing-Fälle, welche nicht direkt die Bundesverwaltung betreffen.

[4] Ausgenommen davon ist u.a. die Datenkommunikation, die über die Kernnetze der Armee sichergestellt wird (namentlich über Netze zugunsten der Gruppe Verteidigung) und die aufgrund der Verfügbarkeits- und Degradationsanforderungen auf bundeseigener Infrastruktur und intern durch die Führungsunterstützungsbasis (FUB) erbracht werden müssen. (Marktmodell IKT-Standarddienst Datenkommunikation vom 19. Juni 2020)

[5] Zentral gelöscht - und damit unschädlich gemacht - werden E-Mails von bekannten Spam- und Malware-Versendern sowie E-Mails, in welchen direkt Viren und Malware erkannt werden.

Die Gründe für diesen erfreulichen Rückgang an gelöschten E-Mails liegt vor allem in der Zerschlagung der Emotet[6]-Infrastruktur (Details s unten im Kapitel «Sperrung von URL und Domains) ».
Mit der Analyse und Bereinigung der eingehenden E-Mails trägt das BIT einen wesentlichen Teil zur Sicherheit der ganzen Bundesverwaltung bei.

**Phishing**
Mittels Phishing wird versucht, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten einer Benutzerin oder eines Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen oder es kann – mit angehängten Dokumenten - Schadsoftware auf das System geladen werden.
Mitarbeitende der Bundesverwaltung bleiben davor nicht verschont: 2021 wurden 11 erfolgreiche Phishing-Angriffe bearbeitet (Vorjahr 34).
Wie die grosse Anzahl an Spam-Meldungen zeigen, ist diese Methode bei Cyber-Kriminellen immer noch hoch im Kurs.
In der ganzen Bundesverwaltung werden die Mitarbeitenden weiterhin auf Phishing-Angriffe sensibilisiert. Dabei wird auch aufgezeigt, wie subtil die inzwischen verwendeten Methoden sind.

**Malware**
Als sehr erfreulich darf erwähnt werden, dass 2021 nur **ein** Vorfall mit Malware **ein** Bundesgerät verseucht hat (Vorjahr 15). Trotz des gezielten Angriffes, konnte durch die umgehende Intervention des zuständigen LE grösserer Schaden verhindert werden.
Trotz dem einzigen Vorfall im Jahr 2021 darf nicht auf weitere Verbesserungen beim Malwareschutz verzichtet werden.

**Skype for Business**
Im Oktober 2021 wurden Angriffsversuche gegen Skype for Business eines Departements detektiert. Die Angreifenden versuchten sich mittels Durchprobieren von Kennwörtern auf zahlreichen Konten in Skype anzumelden. Sie waren damit in 3 Fällen erfolgreich. Mit den betroffenen Mitarbeitenden wurde umgehend Kontakt aufgenommen und ein Passwortwechsel durchgeführt. Zusätzlich wurden weitere Sofortmassnahmen eingeleitet

**Learning Management System (LMS) der Schweizer Armee**
Bei den Corona-bedingten Starts der Rekrutenschulen im Homeoffice traten Mängel bei der Verfügbarkeit des LMS der Armee auf. Auch wurde eine Datenschutz-Schwachstelle durch eine externe Stelle aufgedeckt. Beide Probleme konnten zeitnah behoben werden.

**Sperrung von URL und Domains (externe Webseiten)**
Mit 11 Aufträgen wurden 90 Domains[7] gesperrt (Vorjahr 217 Domains). Obwohl die Sperrungen zur Hauptsache nach wie vor wegen Malware erfolgten, erklärt sich die tiefe Anzahl auch wegen der Zerschlagung der Emotet-Infrastruktur durch Europol und weiterer Strafverfolger, die Ende Januar bekannt wurde. Bis im März wurden deutlich weniger Angriffsversuche mittels in Spam enthaltener Malware registriert. Dann erfolgten neue Angriffe mit der Malware IcedID, die den Platz von Emotet einnahm. Trotz dieser Angriffswellen wurde nur ein einzelner Client verseucht (s. oben «Malware»).

[6] Emotet ist eine Schadsoftware, die vor allem über Spam-E-Mail versendet wird. Zu Beginn war Emotet ein reiner Bankentrojaner. Das Ziel der Angreifer war es, in das IT-System der Opfer zu gelangen, um die Zugangsdaten der Bankverbindungen zu erhalten. Danach funktionierte Emotet wie ein «Dropper». Dropper werden oft dazu verwendet weitere Module nachzuladen.

[7] Die Domain ist der weltweit eindeutige Name einer Website.

**Externe Sicherheitsvorfälle mit direkter Auswirkung auf die Bundesverwaltung**
Vier kritische Sicherheitslücken in Microsoft Exchange[8] erlaubten Angriffe aus der Ferne mit anschliessender Codeausführung. Die Exchange Systeme wurden durch einen Emergency Change durch die LE innerhalb weniger Tage gepatcht. Zusätzlich hat Microsoft mit Print-Nightmare eine kritische Schwachstelle veröffentlicht: Benutzer ohne hohe Privilegien, welche einen Druckertreiber installieren dürfen, könnten das ganze System gefährden. Allgemein stellt das Installieren von Software durch die Benutzer ein grosses Risiko dar. Dies ist auf den Bundesclients unterbunden, was dieses Risiko stark minimiert.
Am 10. Dezember 2021 wurde eine sehr kritische Log4j[9] Schwachstelle publiziert. Die Apache Software Foundation hat Log4j die maximale Kritikalitätsstufe 10 zugewiesen. Angreifer können unter Ausnützung dieser Schwachstelle Schadcode aus der Ferne auf dem betroffenen Rechner ausführen und unter Umständen das System komplett übernehmen. Ein Log4j Update - um die Sicherheitslücke zu schliessen - war einige Tage vor der Bekanntgabe der Schwachstellte publiziert worden. Es folgten weitere Log4j Updates im Zusammenhang mit dieser Sicherheitslücke, weil die vorherigen Updates die Schwachstelle nicht komplett geschlossen hatten, d.h. in manchen nicht Standardkonfigurationen wäre sie eventuell noch ausnutzbar. Log4j ist in vielen Softwarelösungen integriert. In manchen Fällen muss auf das Update des Softwareherstellers gewartet werden, weil man selber keine Aktualisierung durchführen kann. Die Versuche von Angreifern, diese Schwachstelle in der Bundesverwaltung auszunützen, konnten erfolgreich abgewehrt werden, da die LE die verfügbaren Updates unmittelbar installierten und auch die Auswirkungen von Log4j intensiv überwachten. Durch die unmittelbare Reaktion der LE - unter Koordination des NCSC - führten die geschilderten Sicherheitsvorfälle zu keinen negativen Auswirkungen innerhalb der Bundesverwaltung.

**Schwachstellen in den Departementen**
Die Departemente melden, dass erkannte Schwachstellen grundsätzlich nur kleine oder mittlere Auswirkungen[10] zur Folgen hatten.
Grosse Auswirkungen zeigten sich einzig beim Ausfall von Querschnittdienstleistungen: die Verfügbarkeit von wichtigen Aufgaben war beeinträchtigt und konnten zeitweise nicht mehr erfüllt werden.

## 4.3 Veraltete Systeme / Netzwerkprotokolle

Ausser den Parlamentsdiensten und dem UVEK melden die Departemente, dass noch veraltete Systeme und Netzwerkprotokolle im Einsatz stehen.

Die Verantwortung für den Einsatz veralteter Systeme und Protokolle liegt bei den Anwendungsverantwortlichen der Leistungsbezüger in den Ämtern und Departementen. Diese wiederum haben aufgrund fehlender Finanzen oder mangelnder personeller Ressourcen nur beschränkte Möglichkeiten, die Protokolle abzulösen und müssen zwangsläufig das Risiko in Kauf nehmen, dass weiterhin z.T. erhebliche Sicherheitslücken bestehen.

[8] Microsoft Exchange ist eine Groupware- und E-Mail-Transport-Software des Unternehmens Microsoft. Sie dient der zentralen Ablage und Verwaltung von E-Mails, Terminen, Kontakten, Aufgaben und weiteren Elementen für mehrere Benutzer und ermöglicht so die Zusammenarbeit in einer Arbeitsgruppe oder in einem Unternehmen.

[9] Auch unter dem Namen Log4Shell gekannt.

[10] Grosse Auswirkungen = Datenabfluss, schützenswerte Informationen/Daten können durch Unberechtigte eingesehen werden, Einhaltung gesetzlicher Vorgaben stark gefährdet oder verunmöglicht, Dienstleistungen verunmöglicht, ganzes Departement und/oder externe Stellen betroffen

Mittlere Auswirkungen = Einhaltung gesetzlicher Vorgaben gefährdet oder beeinträchtigt, Dienstleistungen eingeschränkt, vertretbare Auswirkungen für externe Stellen

Kleine Auswirkungen = Einhaltung gesetzlicher Vorgaben nicht gefährdet oder beeinträchtigt, Dienstleistungen VE-intern eingeschränkt, keine Auswirkungen für externe Stellen

Diese Lücken werden zwar in den Sicherheitsberichten ausgewiesen und von den Geschäftsleitungen getragen – faktisch dürfte es aber aufgrund der technischen Komplexität den wenigsten Verantwortungsträgerinnen und -trägern bewusst sein, welche Informationssicherheitsrisiken sie tatsächlich akzeptieren. Diese Situation kann zu einer Kumulierung der Sicherheitsrisiken führen. Im Sinne seiner koordinierenden Führungsverantwortung im Bereich Cybersicherheit wird das NCSC diese Problematik verfolgen.
Für den Grossteil der Systeme und Protokolle ist eine Ablösung bzw. eine Aktualisierung geplant (z.T. bis Ende 2024).
Einige veraltete Systeme – vor allem in Labor-Umgebungen – sind bereits in isolierten Netzwerken untergebracht und generieren keinen Netzwerkverkehr mit dem Bundesnetz.

# 5 Stärkung der Informatiksicherheit

## 5.1 Massnahmen 2021

Zur Stärkung der Informatiksicherheit haben alle Departemente, die Parlamentsdienste und die Bundeskanzlei Massnahmen umgesetzt bzw. entsprechende Aktionen durchgeführt.

So wurden unter anderem
- Regelmässig Sensibilisierungsaktionen (z. T. überdepartemental) durchgeführt;
- Zugriffsberechtigungen regelmässig überprüft;
- Mobiltelefone auf die Schad- bzw. Spionagesoftware «Pegasus» überprüft;
- «Direktionsgespräche» u. a. zum Thema Informatiksicherheit durchgeführt;
- Schulungen, wie z.B. die «Security Academy VBS» (Ausbildungswoche des VBS), durchgeführt;
- Personellen Ressourcen für die Informatiksicherheit ausgebaut;
- Bug Bounty-Programme[11] und Public Security Tests durchgeführt;
- Informationssicherheits-Management-Systeme (ISMS) weiter ausgebaut;
- Spezielle Technikzonen v. a. für Domotik-Systeme (Gebäudetechnik) geschaffen;
- Audits durchgeführt;
- Permanente VPN-Verbindungen (Always-On VPN) der Arbeitsstationen durchgesetzt;
- Projekte wie bspw. Makro Signierung initialisiert.

## 5.2 Kurz- und mittelfristig geplante Massnahmen

Zur kurz- und mittelfristigen Stärkung der Informatiksicherheit haben die Departemente, die Parlamentsdienste und die Bundeskanzlei u. a. folgende Massnahmen geplant:

- Einführung einer Digitalisierungsstrategie;
- Sensibilisierungskampagnen;
- Schulung im Umgang mit klassifizierten Informationen;
- Aufbau eines departementalen ISMS;
- Stärkung der personellen Ressourcen;
- Durchführung von technischen Audits;
- Aktualisierung der internen Informationssicherheitsweisungen;

[11] Im Rahmen von Bug Bounty-Programmen werden «ethische Hacker» – Hacker, welche in einem definierten Rahmen legal nach Schwachstellen suchen – dazu aufgerufen, Schwachstellen in den IT-Systemen einer Organisation aufzuspüren. Für jede gefundene und bestätigte Schwachstelle (Bug) erhält der erfolgreiche Hacker eine Belohnung (Bounty), abgestuft nach Schweregrad der gefundenen Schwachstelle.

- Weiterführung und Abschluss des Programms zur Abschwächung des Diebstahls von Zugangsdaten «Mitigation Credential Theft – MTC», der Makro Signierung und Ablösung der bundeseigenen Verschlüsselungssoftware «SecureCenter».

Auf Stufe NCSC werden, nebst der Sicherstellung der Unterstützung der ISBD und ISBO in allen Bereichen der Informatiksicherheit, schwergewichtig die Sicherheitsvorgaben weiterentwickelt, das Schwachstellen-Management gestärkt, Massnahmen für die weitere Ausbildung der Bundesmitarbeitenden geschaffen sowie die Umsetzung des Informationssicherheitsgesetztes (ISG) bearbeitet.