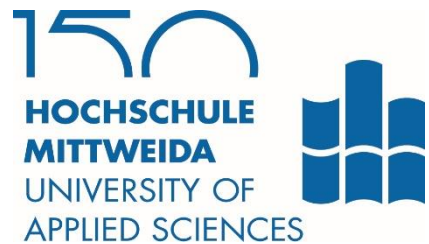
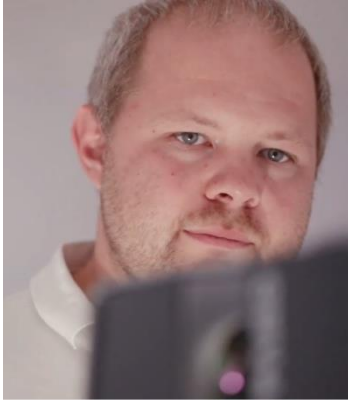

IT-SICHERHEIT – ES WAR EINMAL

 B.Sc., Martin Klöden



Fraunhofer Lernlabor Cybersicherheit an der Hochschule Mittweida



Martin Klöden

B.Sc. Medieninformatik und Interaktives Entertainment

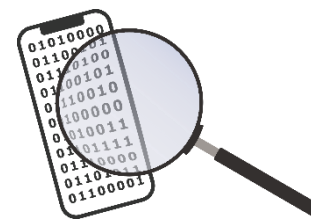
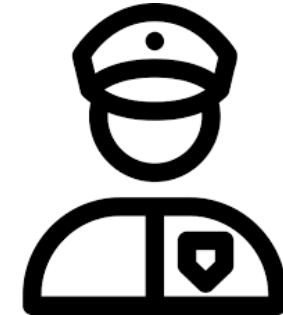
IT - Forensiker

BSI IT-Grundschutz Praktiker

Zertifizierter Business Continuity Manager

seit 01/2018 im Fraunhofer Lernlabor Cybersicherheit

E-Mail: kloeden@hs-mittweida.de



IT-Sicherheit – Es war einmal

ALDI informiert Internet: www.aldi.com

...ab Mittwoch 29. März 667 MHz

Multimedia-Internet-PC mit Intel® Pentium® III Processor incl. 56K PCI V.90 Daten-Fax-Modem

17" Professional Color Monitor
Flatscreen-Bildröhre
Strahlungs-arm nach TCO 99
379,-*
Garantie bis 30.4.2002

ohne Monitor 1.998,-*
Garantie bis 30.4.2002

Service-Beratungs-Hotline 365 Tage im Jahr auch Sonntags & Feiertags

SOFORT ONLINE mit umfangreicher Start-Software

6 Monate 20 Stunden*

Microsoft®-Software-Paket (CEM-Version)
= vorinstalliert = und auf CD-ROMs
WINDOWS 98 2nd Edition (CEM-Version)
incl. Internet-Explorer 5.0 und Internet Tools

Word 2000 (CEM-Version)
Works 2000 (CEM-Version)

ALDI

Medion 40,3 cm sichtbare Bildschirmdiagonale
0,27 mm Lochmaske
1280 x 1.024 max. Auflösung
Zeilenfrequenz: 30 - 72 kHz
Bildfrequenz: 50 - 120 Hz
Max. Fixelfrequenz: 110 MHz

Medion Micro ATX Gehäuse
Intel® Pentium® III Processor
667 MHz Taktfrequenz
Mit neuester 133 MHz Frontside Bus-Technologie
256 Kb Advanced Transfer Cache
3 PCI Steckplätze
Schnittstellen:
2 USB
- 1 parallel
- 2 seriell
2 PS/2

NVIDIA RIVA TNT2 pro AGP 4x Grafikkarte
128 Bit, 32 Mb Memory
Grafik aufrüstbar durch AGP 4x Steckplatz

Siemens 128 MB Arbeitsspeicher PC133-DRAM (1 Modul)
(aufrüstbar bis 1 GB)

Seagate 20 GB Festplatte
Ultra ATA66 Interface

Medion 56K V.90 PCI Daten-Fax-Modem
incl. Software Fax-Software (OEM-Version) und Telefon-Anschlusskabel

Creative Soundblaster Audio PCI 128

Liteon 48 max CD-RW Laufwerk

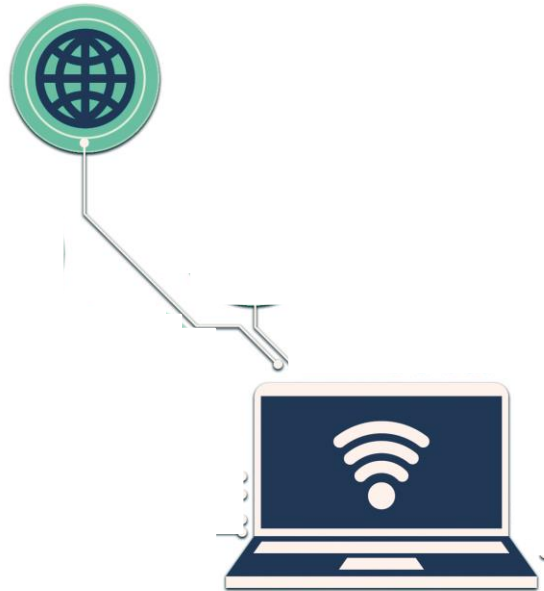
Sony 3,5" Diskettenlaufwerk

PS/2 Maus incl. Pad

PS/2 Tastatur mit Euro-Symbol



IT-Sicherheit – Es war einmal



IT-Sicherheit – Es war einmal



IT-Sicherheit – Es war einmal



144 MIO. **+ 22%**
neue Schadprogramm-Varianten gegenüber 2020:
117,4 MIO.

DURCHSCHNITTLICH

394.000

2020: 322.000

neue

Schadprogramm-
Varianten pro Tag

IM HÖCHSTWERT

553.000

2020: 470.000



13 Tage

lang konnte ein Universitätsklinikum
nach einem *Ransomware*-Angriff keine
Notfall-Patienten aufnehmen.



Digitalisierung

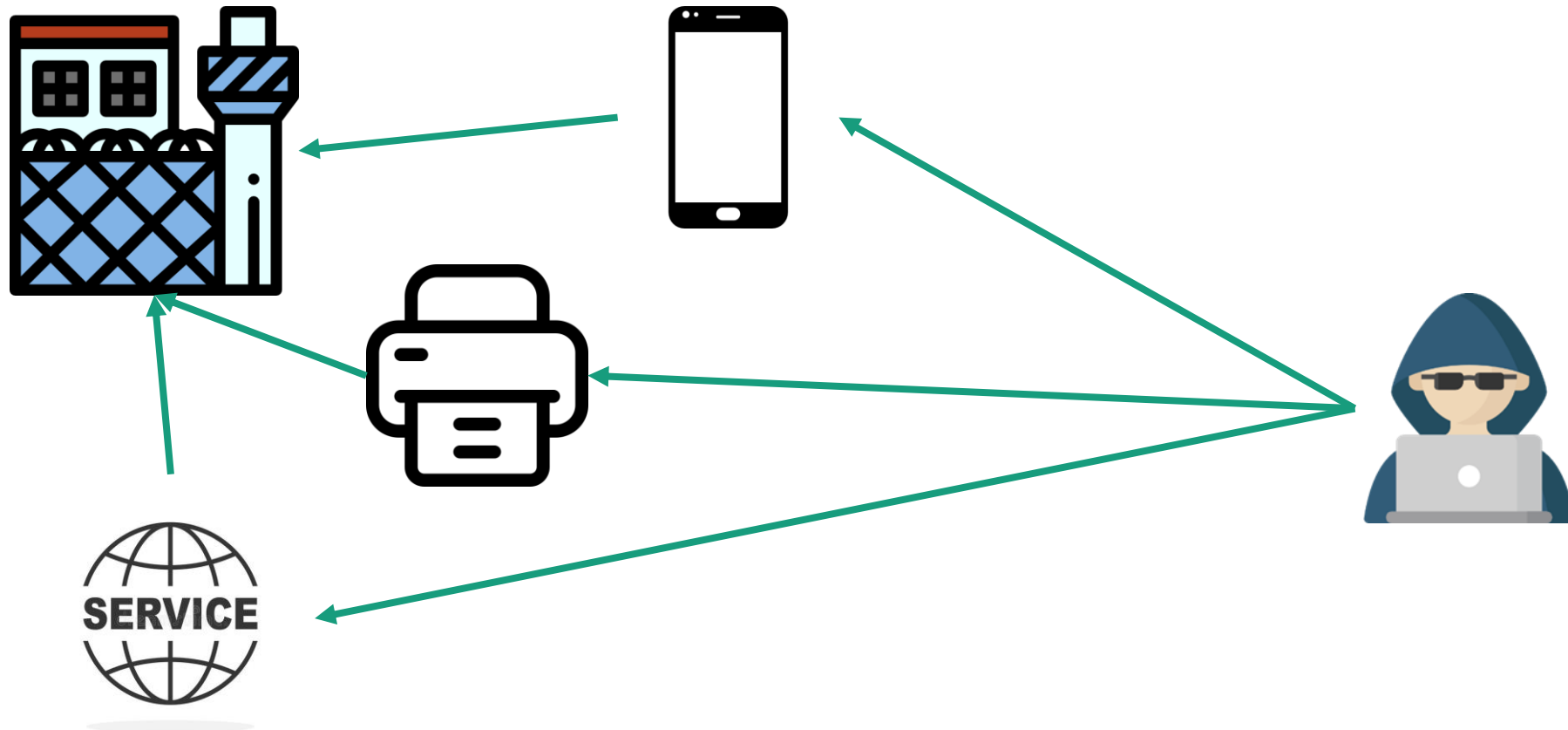


CYBERSICHERHEIT

43 Milliarden Euro
Schaden durch
Hackerangriffe

■ Die Unterwelt macht sich die Digitalisierung ebenso zunutze wie die legale Wirtschaft.

IT-Sicherheit – Es war einmal



IT-Sicherheit – Es war einmal

Address	Name			Vulnerabilities ▾	Risk
223	002	0	3	42	22,064
214	OG	0	3	42	22,064
220		0	3	42	22,064
205					
204					
221	G				
206	OG				
217	001_r048dpk1_r048				

CRITICAL ESXi 6.5 / 6.7 XSS (VMSA-2020-0008)

Description

The remote VMware ESXi host is version 6.5 or 6.7 and is affected by a cross-site scripting (XSS) vulnerability in virtual machine attributes due to improper validation of user-supplied input before returning it to users. An authenticated, remote attacker with access to modify the system properties of a virtual machine from inside the guest OS can exploit this, by inserting script-related HTML in the system properties and having a user view the system properties from the ESXi Host Client, to execute arbitrary script code in a user's ESXi Host Client session.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Apply the appropriate patch as referenced in the vendor advisory.

See Also

<https://www.vmware.com/security/advisories/VMSA-2020-0008.html>

Output

```
ESXi version      : 6.5
Installed build   : 7388607
Fixed build      : 15256549
```

Port	Hosts

Aktuelle Angriffe



Overview
Employee Self-Service > Overview

Edit Personal Data

✖ Cancel

Title

Name

Form of Address:

Last Name:

First Name:

Middle Name:

Initials:

Known as:

Birth Data

Marital Status

Marital Status / Since:

Number of Children:

Other Personal Data

Nationality:

Comm:

IT-Sicherheit – Es war einmal

a.klam@tenno.com: [REDACTED]

sander@kmi-service.de: [REDACTED]

elisa.finke@stadtwerke-goerlitz.de: [REDACTED]

heinz.schnettler@plato-technology.de: [REDACTED]

j.laetsch@landskron.de: [REDACTED]

sdi@nordisk.eu: [REDACTED]



Identity Leak Checker

- 700 Leaks ausgewertet
- 20.000.000 neue Identitäten jeden Monat
- <https://sec.hpi.de/ilc/searchoder>

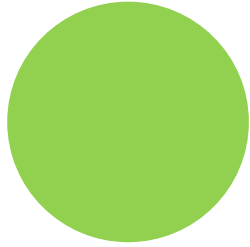
Ergebnis Ihrer Anfrage bei HPI Identity Leak Checker

Achtung: Ihre E-Mail-Adresse [REDACTED] taucht in mindestens einer gestohlenen und unrechtmäßig veröffentlichten Identitätsdatenbank (so genannter Identity Leak) auf.

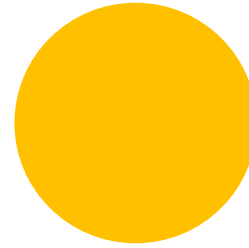
Folgende sensible Informationen wurden im Zusammenhang mit Ihrer E-Mail-Adresse frei im Internet gefunden:

Betroffener Dienst	Datum	Verifiziert	Betroffene Nutzer	Passwort	Vor- und Zuname	Geburtsdatum	Anschrift	Telefonnummer	Kreditkarte	Bankkontodaten	Sozialversicherungsnr.	IP-Adresse
Combolist	Jul. 2016		19.351.766	Betroffen	–	–	–	–	–	–	–	–
dropbox.com	Sep. 2012	✓	68.658.165	Betroffen	–	–	–	–	–	–	–	–
linkedin.com	Jun. 2012	✓	160.144.040	Betroffen	–	–	–	–	–	–	–	–

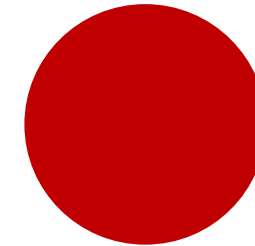
Sicherheitsvorkehrungen



Technisch



Organisatorisch



Personell

BSI Grundschutz Katalog
Datenlöschkonzepte
Informationssicherheitsmanagement
Rollen- und Rechtekonzepte
Datensicherung
Zugangskontrollen
Passwortsicherheit
Auditierungen, Zertifizierungen
ISO 27001
Peripheriegerätemanagement

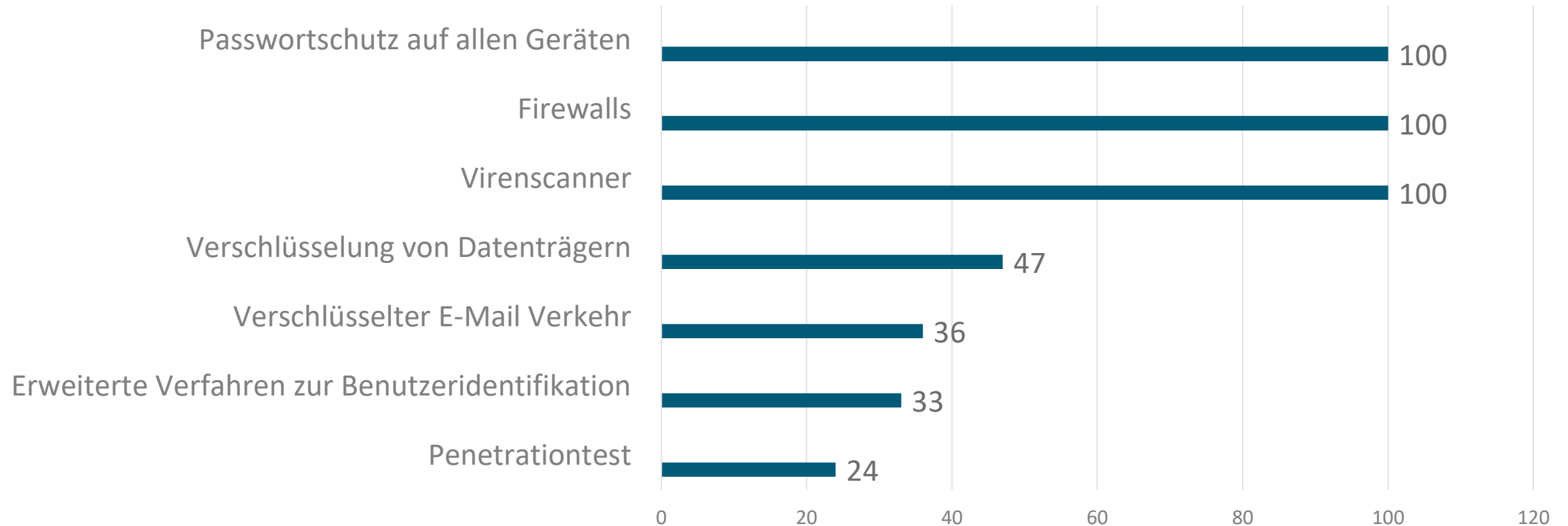
Passwortmanagement
Informationssicherheitsmanagement
Berechtigungskonzepte
Datensicherung
Funktionsbewertungen
Zugangskontrollen
Penetrationstests
Internes Schwachstellenmanagement
Datensicherung
Notbetrieb und Wiederanlaufszzenarien
Dokumentation / Nachweis der Maßnahmen

Notfall Simulationen
Externes Schwachstellenmanagement
Antivirus Lösungen
Risikobewertungen
Backupkonzepte
2-Faktor-Authentifizierungen
Datenklassifizierung
Schulungen

Sensibilisierungen
Notfallpläne
Phishing Simulationen
Datensicherung
Update-Management
Active Security Monitoring
Incident Response

Sicherheitsvorkehrungen

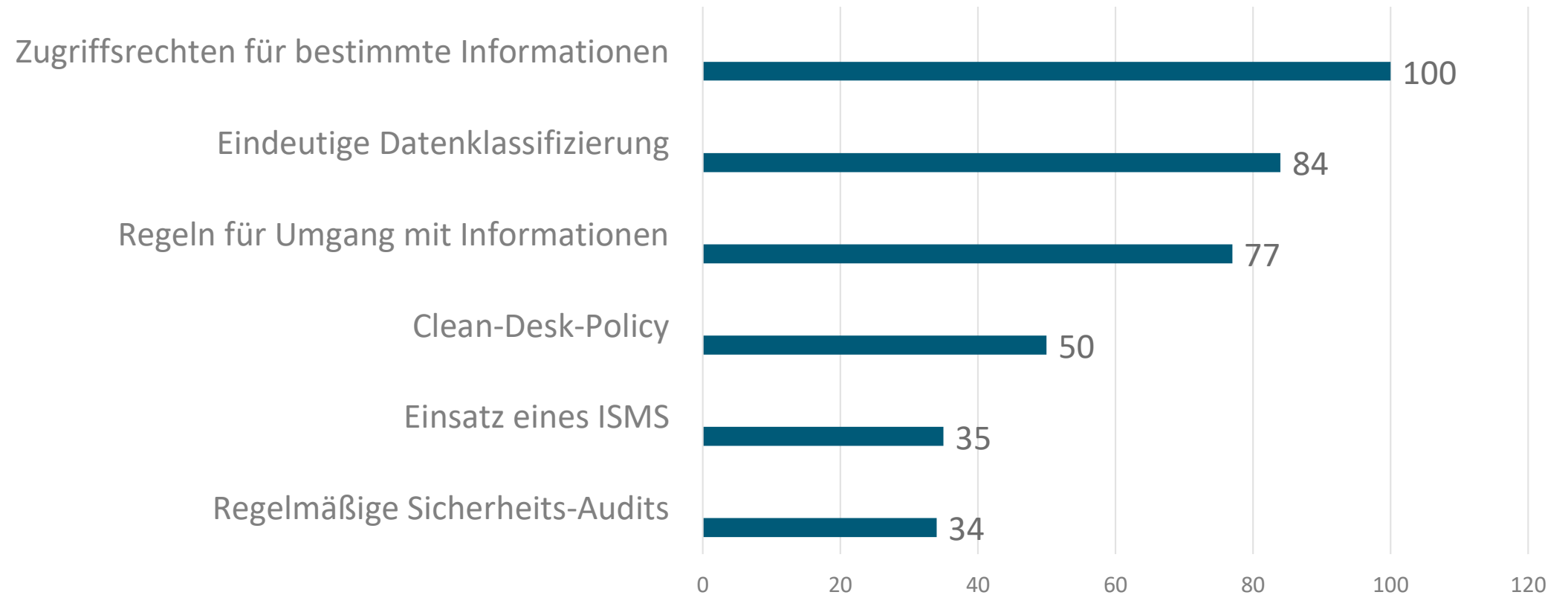
Eingesetzte technische Maßnahmen



Quelle: Bitkom – Wirtschaftsschutz 2018 - <https://www.bitkom.org/sites/default/files/file/import/181008-Bitkom-Studie-Wirtschaftsschutz-2018-NEU.pdf>

Sicherheitsvorkehrungen

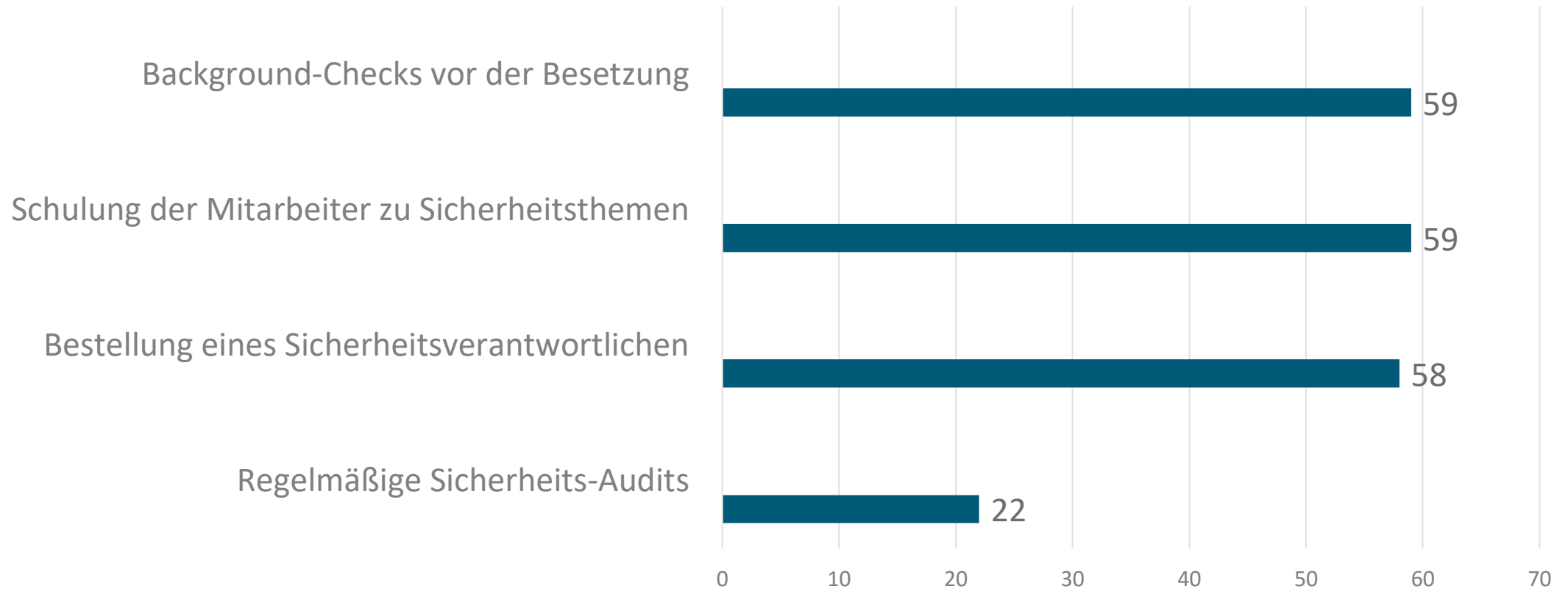
Organisatorische Maßnahmen



Quelle: Bitkom – Wirtschaftsschutz 2018 - <https://www.bitkom.org/sites/default/files/file/import/181008-Bitkom-Studie-Wirtschaftsschutz-2018-NEU.pdf>

Sicherheitsvorkehrungen

Personelle Maßnahmen



Quelle: Bitkom – Wirtschaftsschutz 2018 - <https://www.bitkom.org/sites/default/files/file/import/181008-Bitkom-Studie-Wirtschaftsschutz-2018-NEU.pdf>

Cyber Security geht nur gemeinsam

- Cyber Security ist Chefsache!
- Security-Assessment: Identifizieren Sie Schwachstellen!
- Prüfen Sie E-Mails / URLs
- Daten klassifizieren
- Cyber Security auch beim Kunden und Geschäftspartner
- Notfallplan schmieden
- Sicherheit testen



Entscheider haften mit
Ihrem privaten Vermögen

Die Rechtslage ist eindeutig:
Ist ein Unternehmen nicht
hinreichend abgesichert,
haften Führungsorgane bei
Hackerangriffen mit ihrem
Privatvermögen!

§ 93 Abs. 1 Satz 1 AktG, bzw. §§ 116 Satz 1 i.V.m.

§ 93 AktG bei GmbHs § 43 Abs. 2 GmbHG