IT-SICHERHEIT – ES WAR EINMAL

B.Sc., Martin Klöden

Fraunhofer FKIE

axilaris
safe data. smart software.

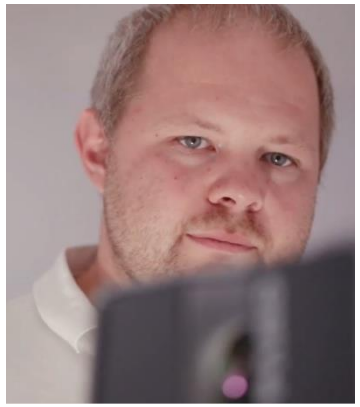
Fraunhofer ACADEMY

HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

Lernlabor Cybersicherheit

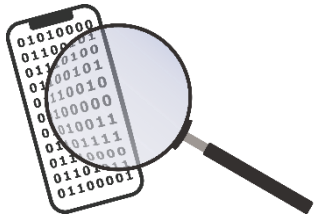
© Fraunhofer

Fraunhofer Lernlabor Cybersicherheit an der Hochschule Mittweida



Fraunhofer FKIE

HOCHSCHULE MITTWEIDA UNIVERSITY OF APPLIED SCIENCES



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

© Fraunhofer

offen

Fraunhofer ACADEMY

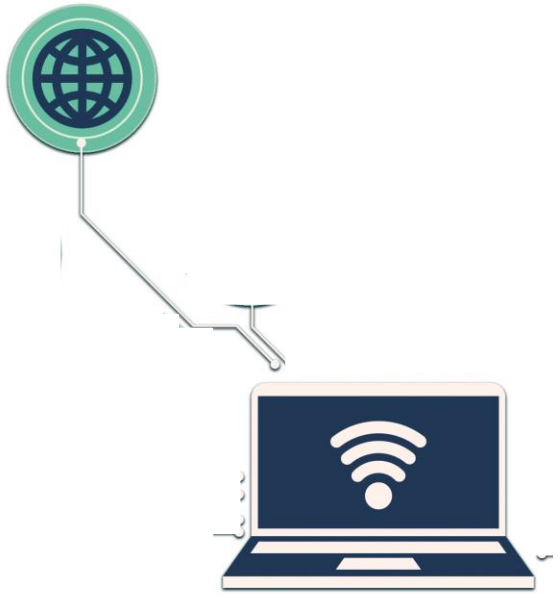
IT-Sicherheit – Es war einmal

© Fraunhofer

offen

Fraunhofer ACADEMY

IT-Sicherheit – Es war einmal



© Fraunhofer

IT-Sicherheit – Es war einmal

© Fraunhofer

Fraunhofer ACADEMY

IT-Sicherheit – Es war einmal

144 MIO. neue Schadprogramm-Varianten

+22 % gegenüber 2020: **117,4 MIO.**

DURCHSCHNITTLICH **394.000** neue **Schadprogramm-Varianten** pro Tag (2020: 322.000)

IM HÖCHSTWERT **553.000** (2020: 470.000)

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

© Fraunhofer

offen

Fraunhofer ACADEMY

Digitalisierung

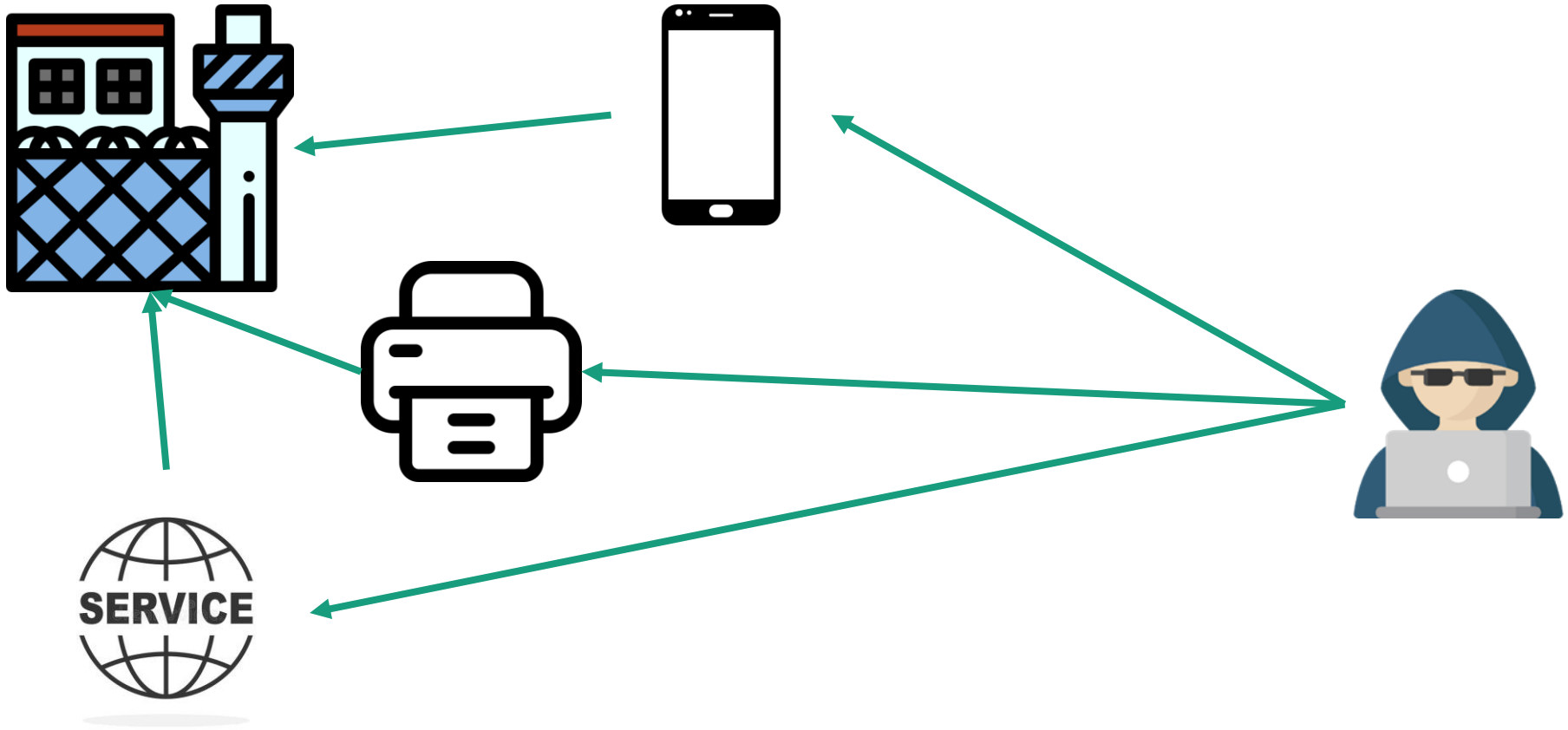
CYBERSICHERHEIT

43 Milliarden Euro Schaden durch Hackerangriffe

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

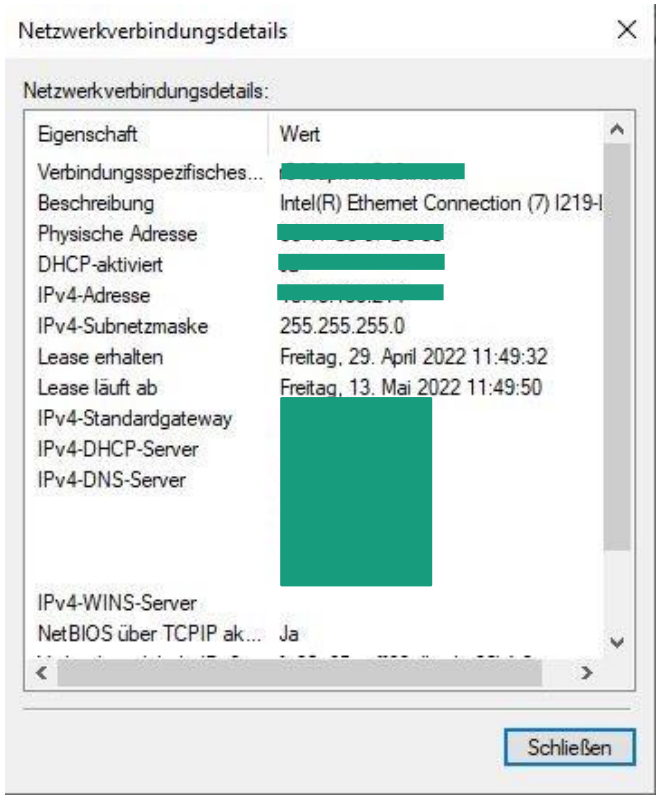
© Fraunhofer

IT-Sicherheit – Es war einmal



© Fraunhofer

IT-Sicherheit – Es war einmal




```
18.[redacted]  00-[redacted]  dynamisch
18.[redacted]  6c-[redacted]  dynamisch
18.[redacted]  7c-[redacted]  dynamisch
18.[redacted]  7c-[redacted]  dynamisch
18.[redacted]  6c-[redacted]  dynamisch
18.[redacted]  6c-[redacted]  dynamisch
18.[redacted]  6c-[redacted]  dynamisch
18.[redacted]  6c-[redacted]  dynamisch
18.[redacted]  6c-[redacted]  dynamisch
18.[redacted]  6c-[redacted]  dynamisch
18.[redacted]  6c-[redacted]  dynamisch
18.[redacted]  7c-[redacted]  dynamisch
18.[redacted]  6c-[redacted]  dynamisch
18.[redacted]  6c-[redacted]  dynamisch
18.[redacted]  6c-[redacted]  dynamisch
18.[redacted]  6c-[redacted]  dynamisch
18.[redacted]  6c-[redacted]  dynamisch
18.[redacted]  6c-[redacted]  dynamisch
18.[redacted]  00-[redacted]  dynamisch
18.[redacted]  00-[redacted]  dynamisch
18.[redacted]  00
```

IT-Sicherheit – Es war einmal

Address	Name			Vulnerabilities	Risk
[redacted]223	[redacted]G02	0	3	42	22,064
[redacted]214	[redacted]OG	0	3	42	22,064
[redacted]220		0	3	42	22,064
[redacted]205					
[redacted]204					
[redacted]221	[redacted]G				
[redacted]206	[redacted]OG				
[redacted]217	[redacted]01.r048dpk1.r048.i				

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

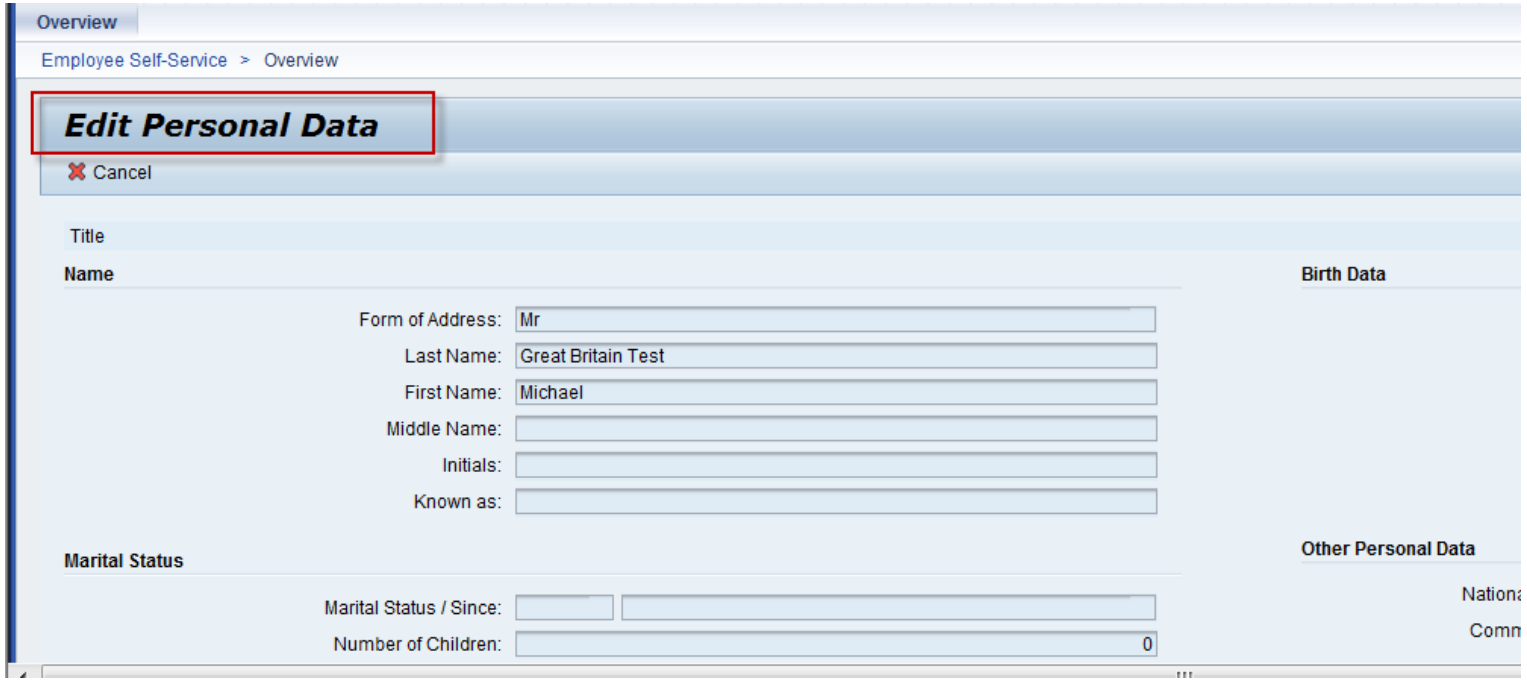
Output

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

Port	Hosts
[redacted]	

© Fraunhofer

Aktuelle Angriffe



© Fraunhofer
offen

Fraunhofer ACADEMY

IT-Sicherheit – Es war einmal

[redacted]
a.klam@tenno.com:[redacted]

[redacted]
sander@kmi-service.de[redacted]

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

[redacted]
heinz.schnettler@plato-technology.de[redacted]

[redacted]
j.laetsch@landskron.de:[redacted]

[redacted]
sdi@nordisk.eu:[redacted]

© Fraunhofer
offen

Fraunhofer ACADEMY

Identity Leak Checker

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

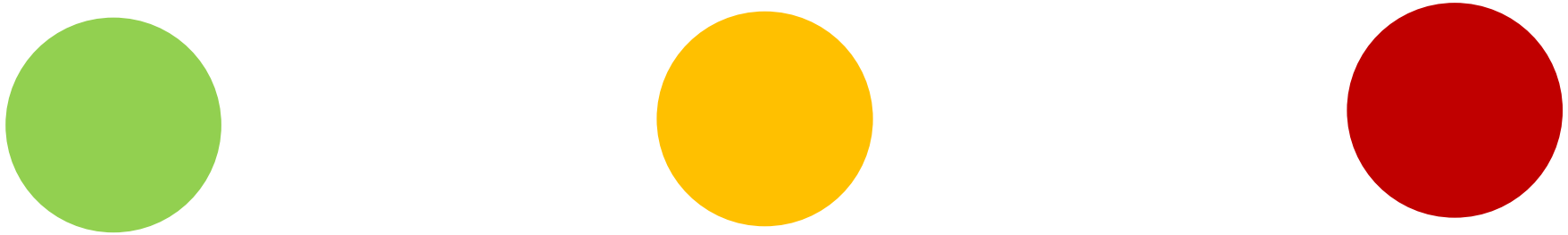
Ergebnis Ihrer Anfrage bei HPI Identity Leak Checker

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	Sozial-versicherungsnr.	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	–	–	–	–	–	–	–	–

© Fraunhofer

Sicherheitsvorkehrungen

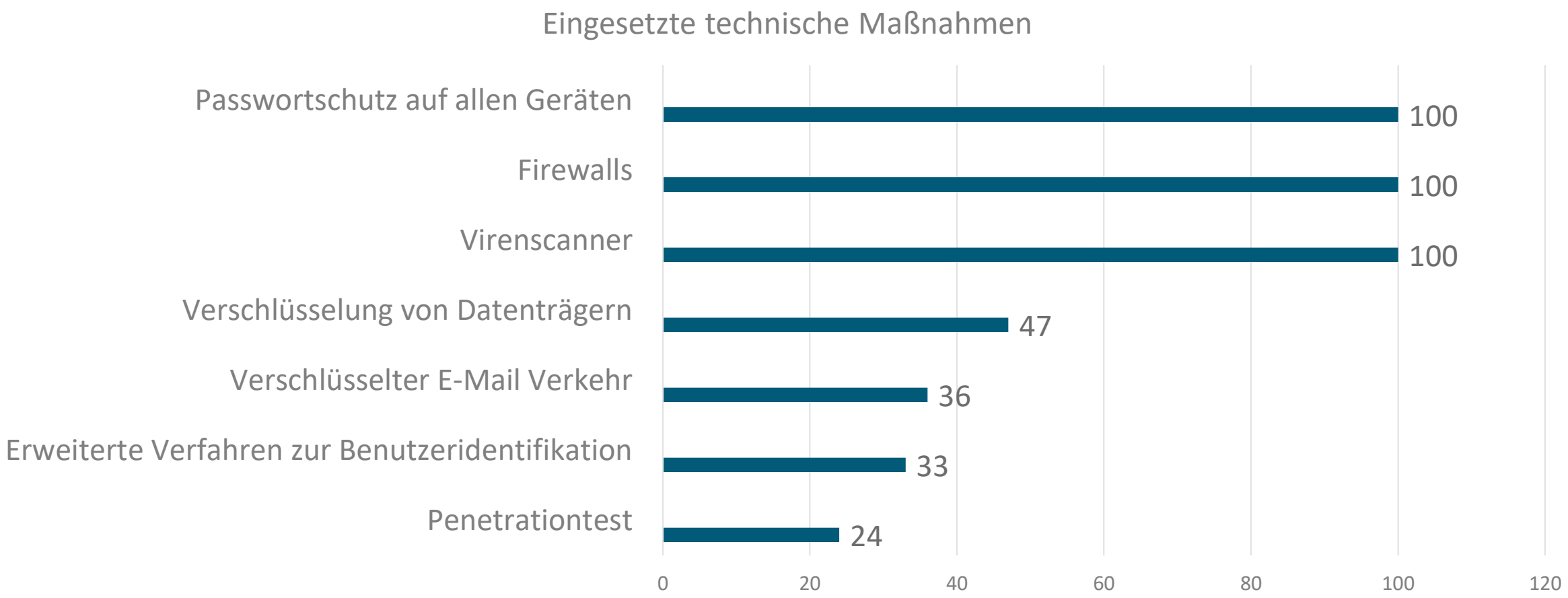


Notfall Simulationen
Sensibilisierungen
Notfallpläne
BSI Grundschutz Katalog
Externes Schwachstellenmanagement
Passwortmanagement
Antivirus Lösungen
Datenlöschkonzepte
Phishing Simulationen
Informationssicherheitsmanagement
Risikobewertungen
Datensicherung
Update-Management
Rollen- und Rechtekonzepte
Berechtigungskonzepte
Backupkonzepte
2-Faktor-Authentifizierungen
Datensicherung
Funktionsbewertungen
Zugangskontrollen
Penetrationstests
Datenklassifizierung
Active Secuirty Monitoring
Passwortsicherheit
Internes Schwachstellenmanagement
Schulungen
Incident Response
Auditierungen, Zertifizierungen
Datensicherung
Notbetrieb und Wiederanlaufszenarien
ISO 27001
Peripheriegerätemanagement
Endpoint Security
Dokumentation / Nachweis der Maßnahmen

© Fraunhofer

Fraunhofer ACADEMY

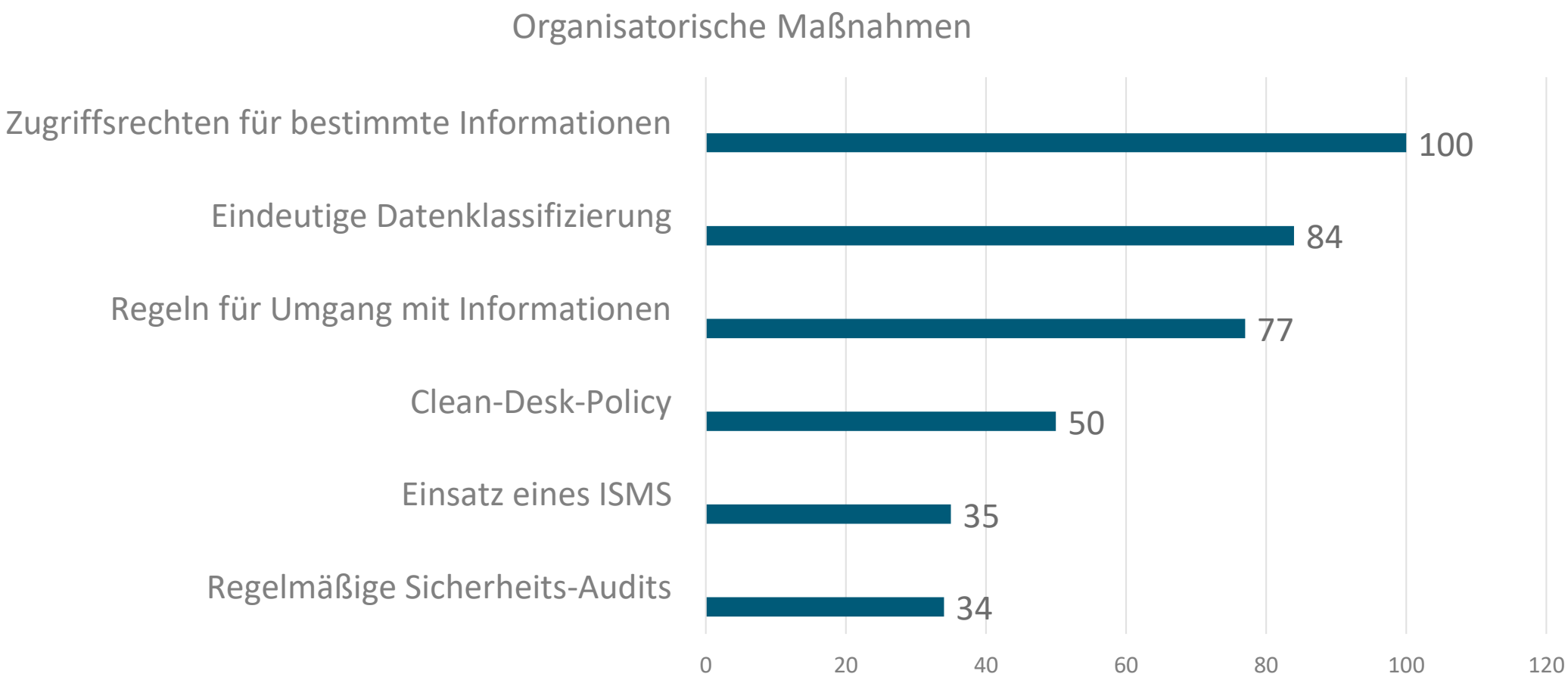
Sicherheitsvorkehrungen



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

© Fraunhofer

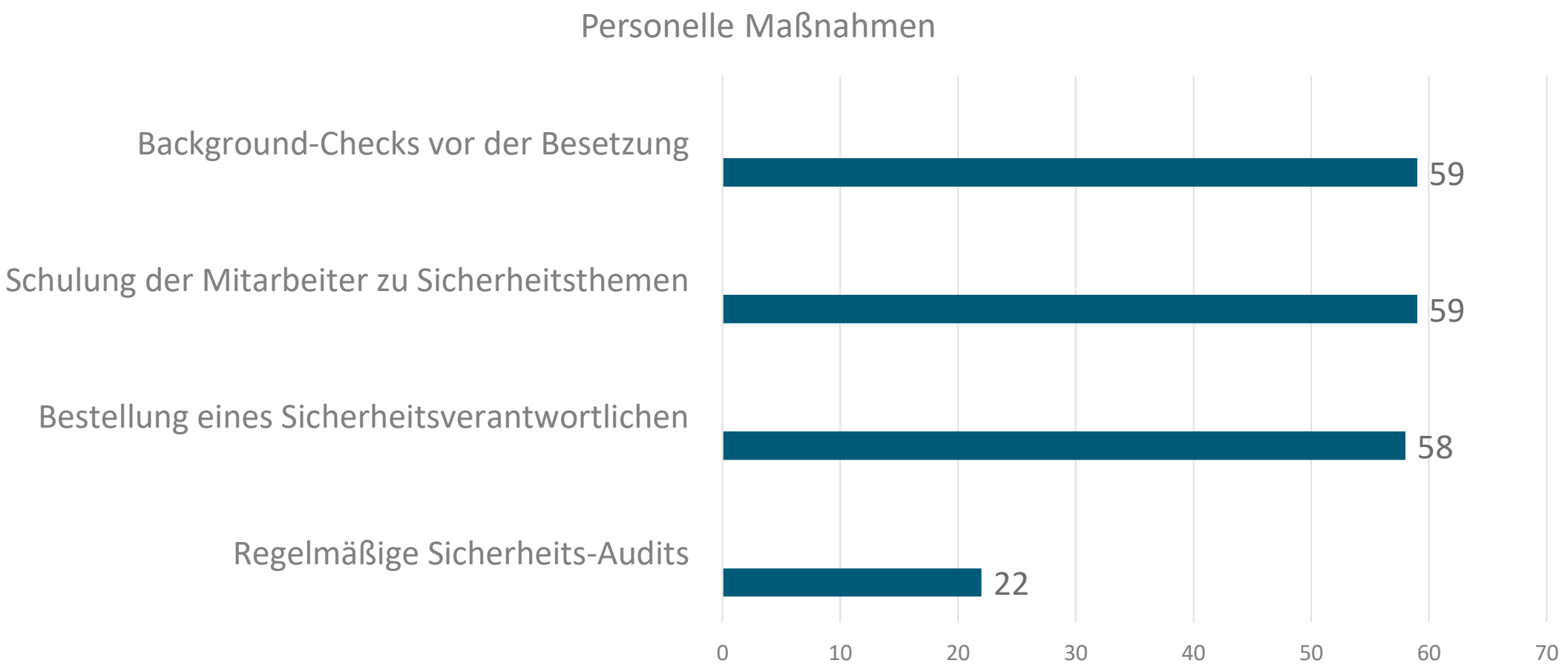
Sicherheitsvorkehrungen



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

© Fraunhofer

Sicherheitsvorkehrungen



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

© Fraunhofer

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

© Fraunhofer