

Crashkurs IT-Sicherheit

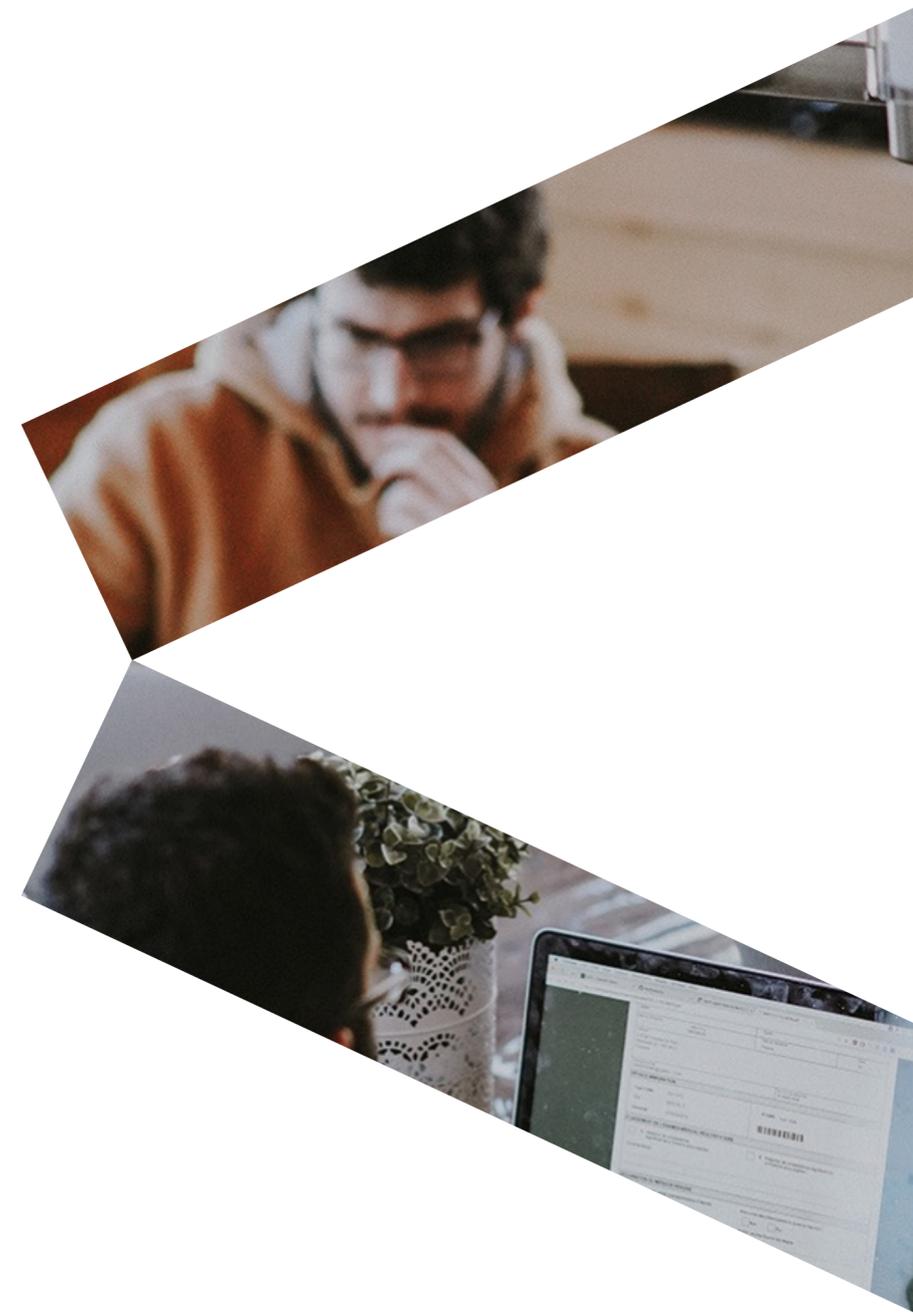
Datenleck braucht einen Check

Moritz Pietzschke,
Philipp Escher,
Dennis Krafczyk

24.03.2022



Willkommen bei Westcode. 🖐️
Begeistert von **digitalen Technologien** 🚀,
sind wir davon überzeugt, dass erfolgreiches
Geschäft durch **innovative Ideen** 💡 entsteht
und verstehen uns als Partner 💪 mit **exzellentem**
IT-Knowhow 🧑💻 und **Ende-zu-Ende-**
Verantwortung. 🤝



Allgegenwärtig

Persönlich verantwortlich

Konkret gefährdet



Schutzziele

Vertraulichkeit

Integrität

Verfügbarkeit

Authentizität

Verbindlichkeit

Anonymisierung
und
Pseudonymisierung

Physische Sicherheit

- Zutrittskontrolle
- Schutz vor Elementarschäden
- Klimatisierung
- USV

→ Schutz am Endpunkt: Zero Trust



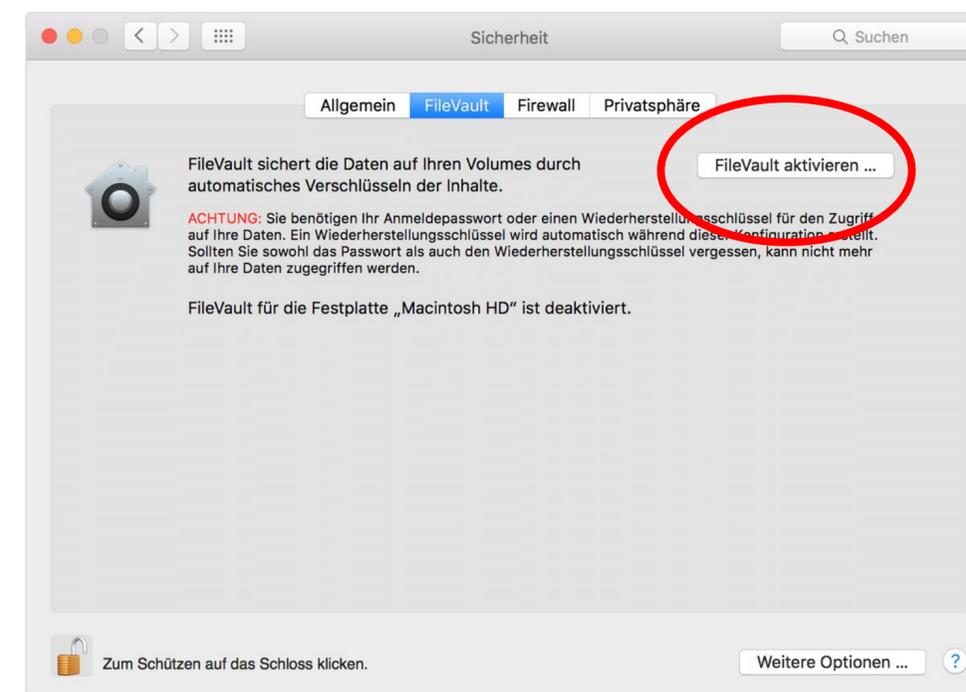
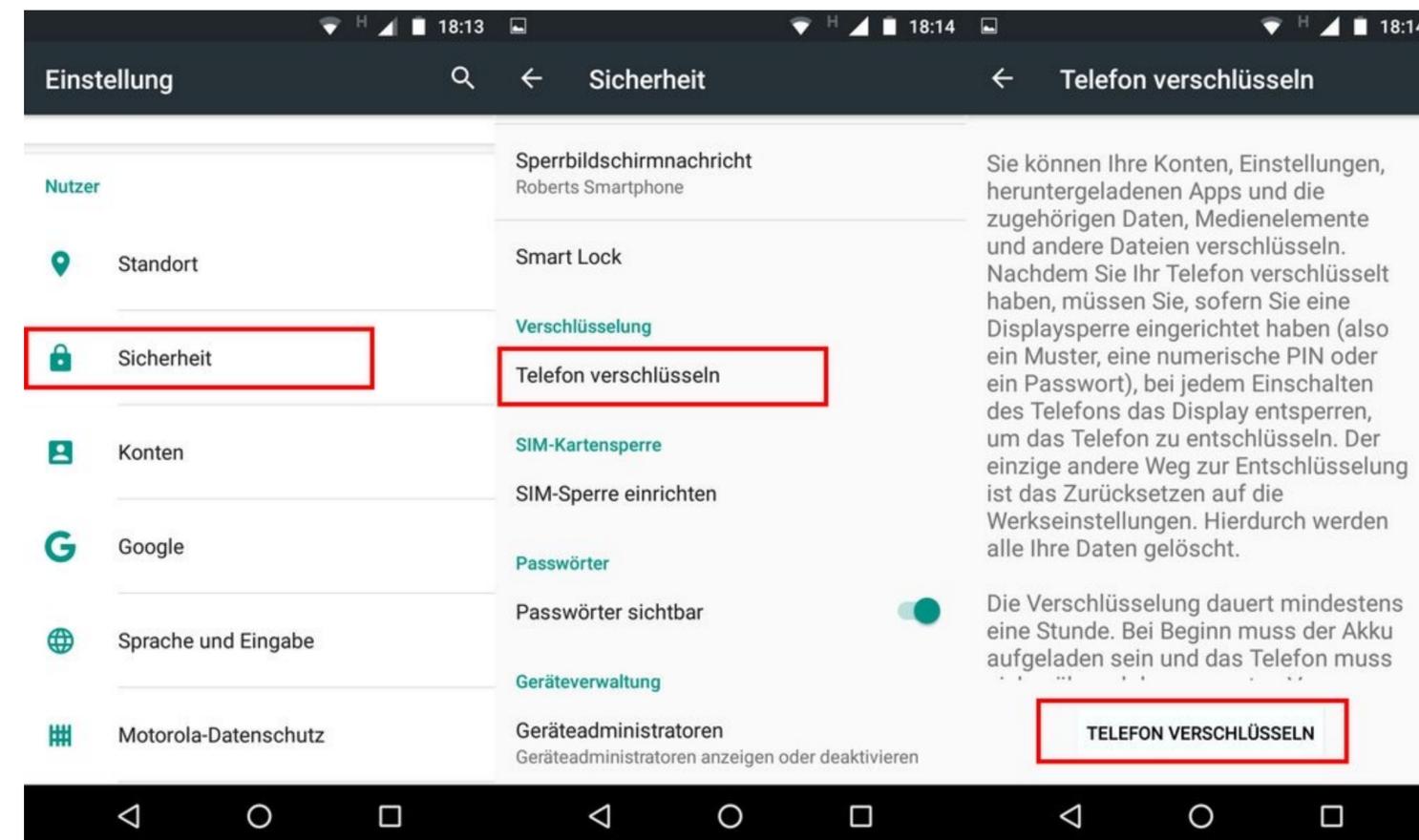
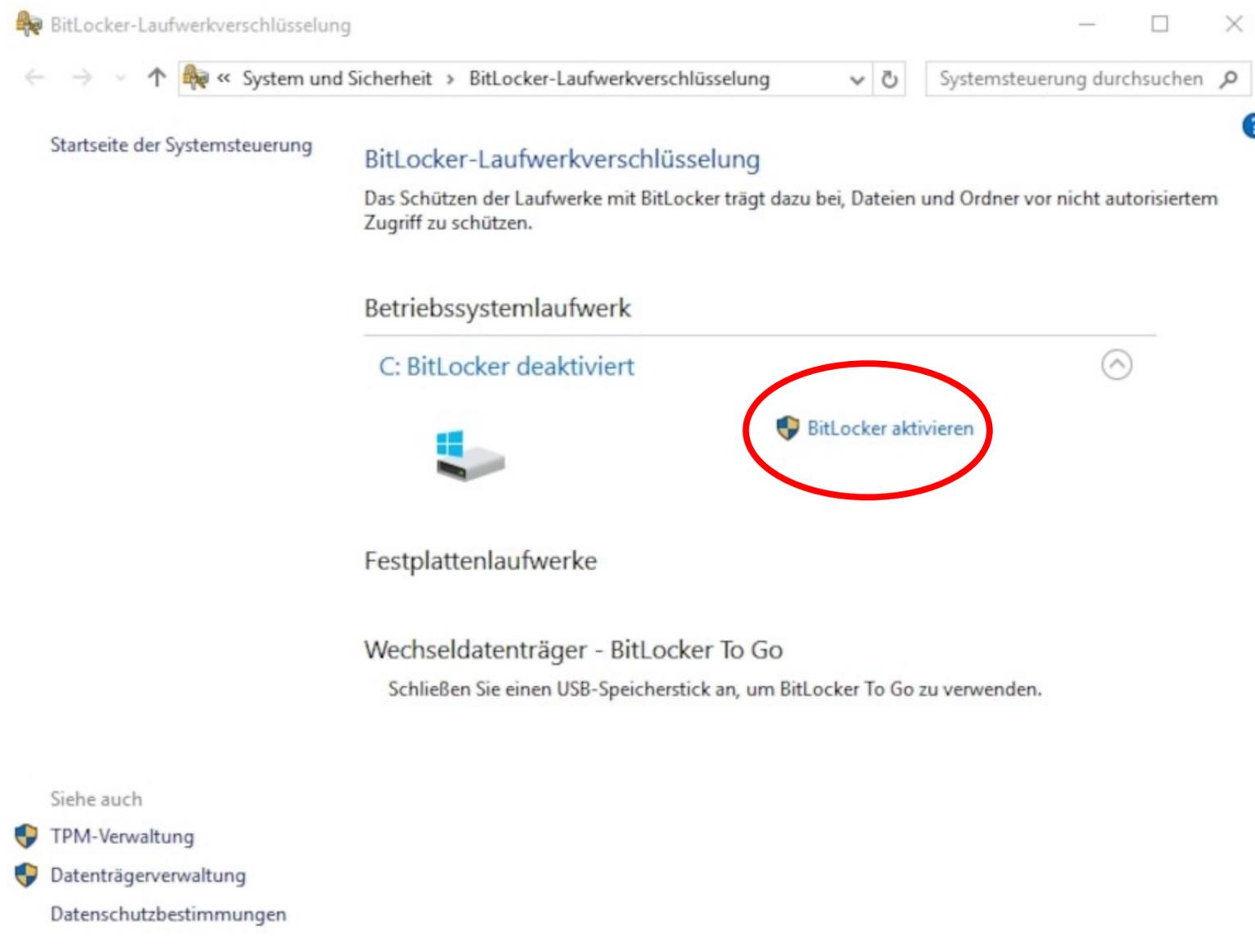
Zero Trust *„Never trust always verify“*

- Sicheres Arbeiten in ungesicherten Umgebungen
- Endpunkte müssen sicher sein
- Keiner Komponente wird vertraut
- Das Netzwerk wird als kompromittiert angesehen



Bildquelle: Cloudflare

Festplatten- / Dateiverschlüsselung



Transportverschlüsselung

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [westcode.de](#) > 3.126.143.160

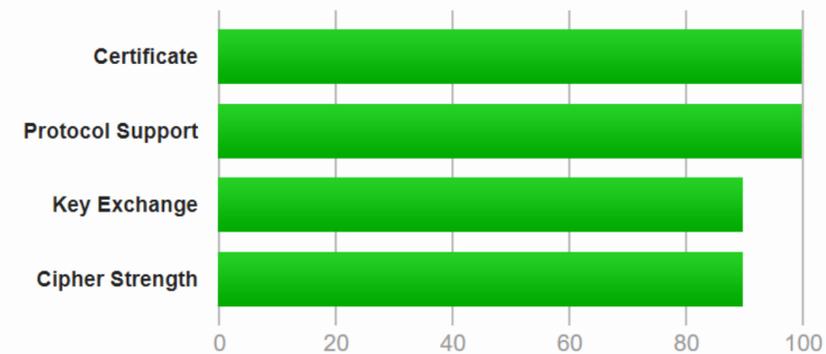
SSL Report: [westcode.de](#) (3.126.143.160)

Assessed on: Mon, 21 Mar 2022 18:04:44 UTC | **HIDDEN** | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This site works only in browsers with SNI support.

This server supports TLS 1.3.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. [MORE INFO »](#)

DNS Certification Authority Authorization (CAA) Policy found for this domain. [MORE INFO »](#)

Transportverschlüsselung

The screenshot displays a Hardenize report for the domain westcode.de. The report is titled "Public Report | westcode.de" and includes a "TEST ANOTHER" button. The left sidebar lists various security categories with their status:

- Domain Name System**
 - ✓ DNS Zone
 - ✓ DNS Records
 - ✓ DNSSEC
 - ✓ CAA
- Email**
 - ✓ Mail servers
 - SECURE TRANSPORT (SMTP)
 - ✓ TLS
 - ✓ Certificates
 - AUTHENTICATION AND POLICY
 - ✓ SPF
- WWW**
 - PROTOCOLS
 - ✓ HTTP (80)
 - ✓ HTTPS (443)
 - SECURE TRANSPORT
 - ✓ TLS
 - ✓ Certificates
 - ✓ Cookies
 - ✓ Mixed Content
 - MODERN SECURITY FEATURES
 - ✓ Strict Transport Security
 - ✓ Content Security Policy
 - ✓ Subresource Integrity

The main content area is divided into two sections:

WEB SECURITY OVERVIEW

- HTTPS** (Very Important, Medium Effort): Web sites need to use encryption to help their visitors know they're in the right place, as well as provide confidentiality and content integrity. Sites that don't support HTTPS may expose sensitive data and have their pages modified and subverted.
- HTTPS Redirection** (Very Important, Low Effort): To deploy HTTPS properly, web sites must redirect all unsafe (plaintext) traffic to the encrypted variant. This approach ensures that no sensitive data is exposed and that further security technologies can be activated.
- HTTP Strict Transport Security** (Very Important, Medium Effort): HTTP Strict Transport Security (HSTS) is an HTTPS extension that instructs browsers to remember sites that use encryption and enforce strict security requirements. Without HSTS, active network attacks are easy to carry out.
- HSTS Preloaded** (Very Important, Medium Effort): HSTS Preloading is informing browsers in advance about a site's use of HSTS, which means that strict security can be enforced even on the first visit. This approach provides best HTTPS security available today.
- Content Security Policy** (Very Important, High Effort): Content Security Policy (CSP) is an additional security layer that enables web sites to control browser behavior, creating a safety net that can counter attacks such as cross-site scripting.

EMAIL SECURITY OVERVIEW

- STARTTLS** (Very Important, Low Effort): All hosts that receive email need encryption to ensure confidentiality of email messages. Email servers thus need to support STARTTLS, as well as provide decent TLS configuration and correct certificates.
- SPF** (Important, Low Effort): Sender Policy Framework (SPF) enables organizations to designate servers that are allowed to send email messages on their behalf. With SPF in place, spam is easier to identify.



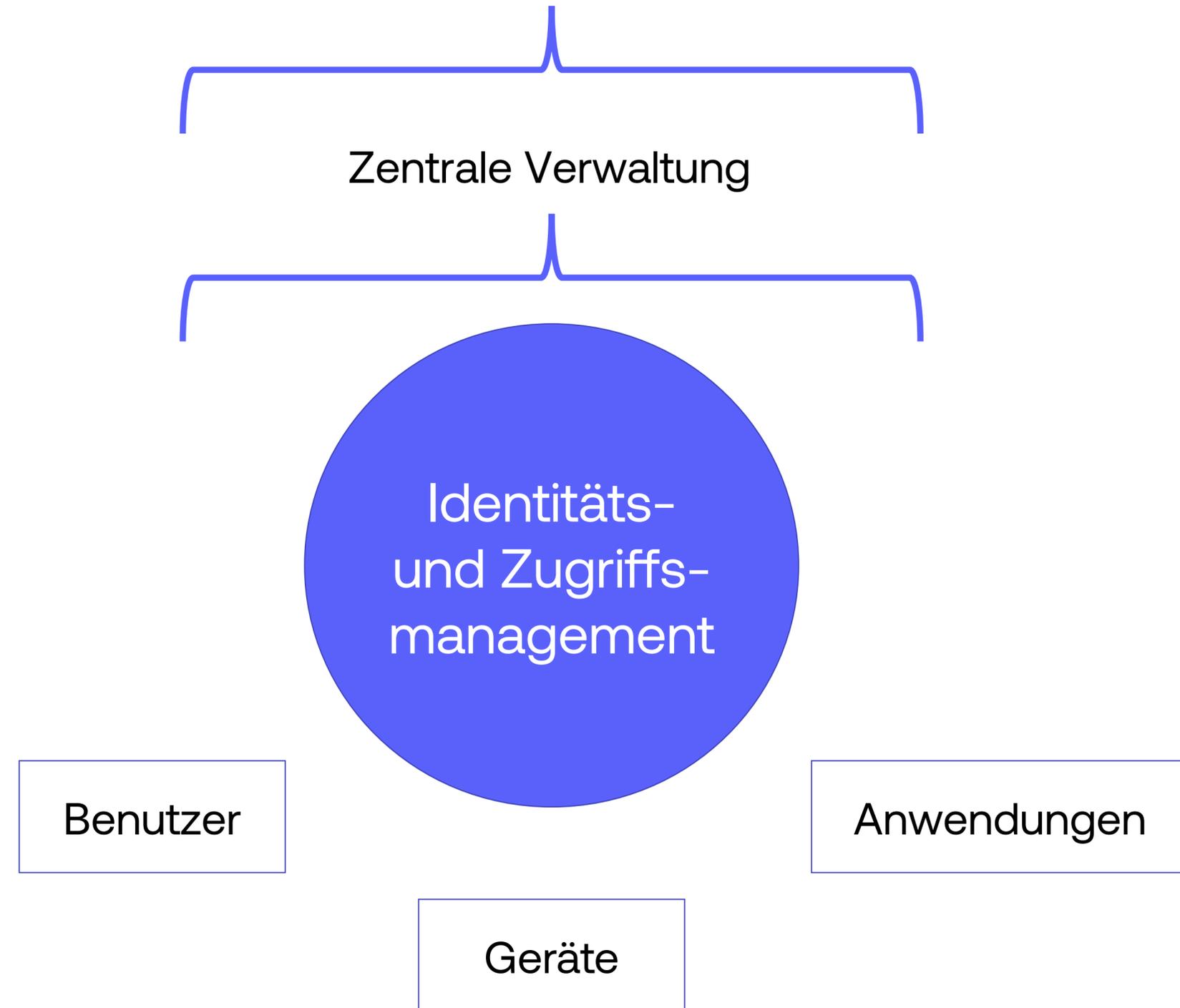
IT-Governance

Unterstützung regulatorischer Vorgaben

Mitarbeiter Lifecycle

- 👉 Onboarding
- 👉 Probezeit
- 👉 Arbeitsverhältnis
- 👉 Abteilungswechsel
- 👉 Offboarding

Einheitliche Richtlinien und Standards



IT-Awareness

Home Office / Mobiles Arbeiten

Awareness-Schulungen

Datenschutz



Aussies Doing Things @aussiesdointhgs · 1. Apr.

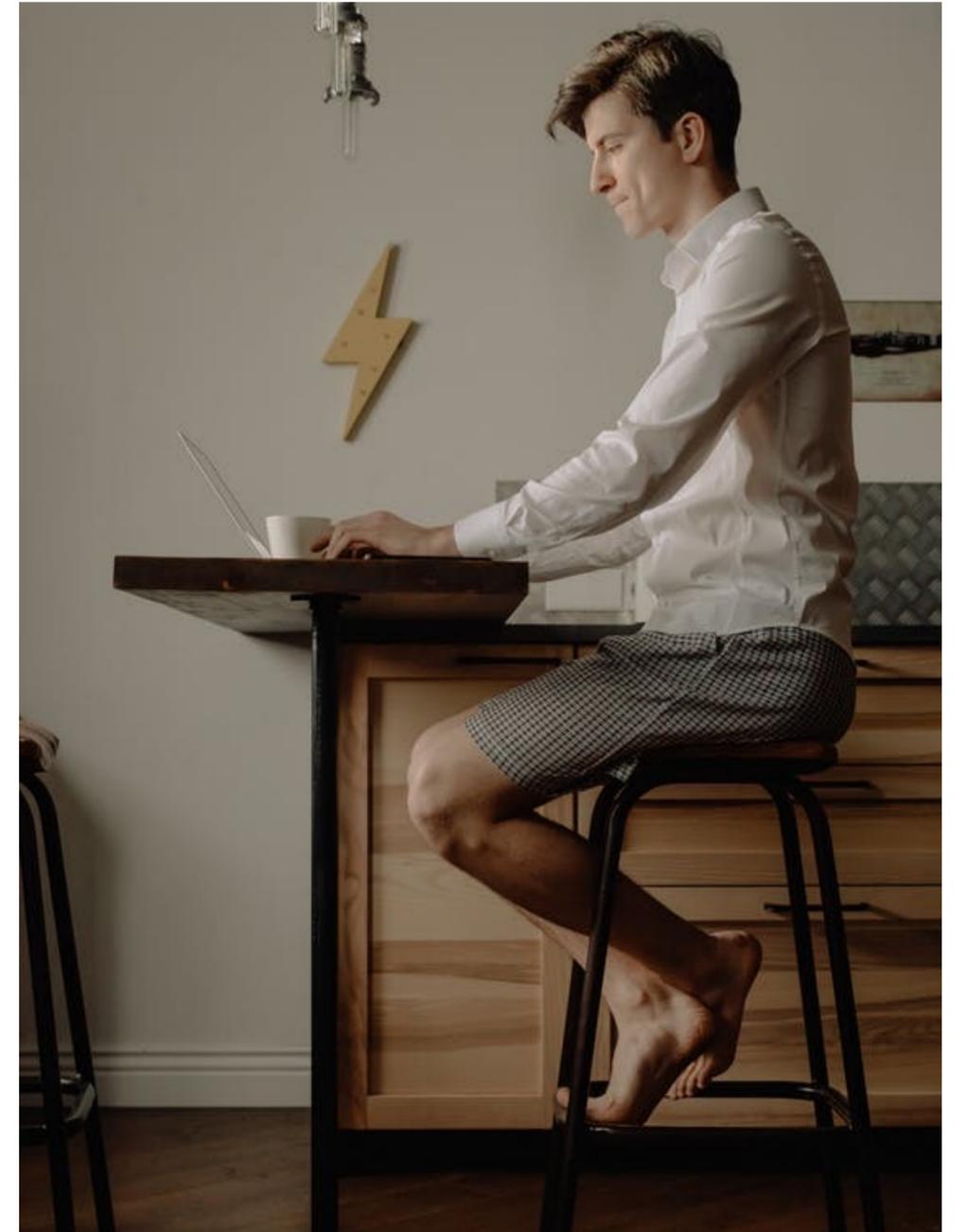


This is Wilson. He is now working from home. 🖥️



Home Office / Mobiles Arbeiten

- Technische als auch menschliche Komponenten fehlen
- Richtlinien für mobiles Arbeiten
- Regelmäßige Prüfung
- Distanz zur Arbeit behalten



Awareness-Schulungen

- Motivation für IT-Sicherheit im eigenen Unternehmen herleiten
- Awareness-Schulungen (mit interaktiven Komponenten)
- Schaffung einer Sicherheitskultur durch begleitete Integration



Datenschutz

- Personenbezogene Daten erfordern besondere Sensibilität
- Schatten-IT vermeiden:
Anforderungen der Mitarbeiter erfüllen
- Bewusster Umgang mit Daten:
Screensharing, Social Media, Fotos verschicken, Sichtbarkeitsschutz
(Shoulder Surfing 🏄)





chrome web store

[Startseite](#) > [Erweiterungen](#) > Lightshot (Screenshot Tool)



Lightshot (Screenshot Tool)

Angeboten von: <https://app.prntscr.com>

★★★★★ 7.235

[Soziale Netze & Kommunikation](#)

 2.000.000+ Nutzer

- Account recovery



- noreply** <noreply@bitcointox.web.app>

To: sergein777@yahoo.com

Hello **Sergein777**,

We confirmed the validity of documents you provided for your account recovery.
Your new password is: [REDACTED]

If you didn't request this account recovery, [contact us](#) immediately.

IT-Notfallvorsorge

Wenn es passiert, dann bitte geordnet.

IT-Notfallvorsorge

Brand

Einbruch

Infektion

Gefahr für Leib und Leben

IT-Notfallvorsorge

~~Brand~~
Ausfall

~~Einbruch~~
Datendiebstahl

~~Infektion~~
Malware

Gefahr für Ruf und Geschäft

IT-Notfallvorsorge

Ausfall

Datendiebstahl

Malware-Infektion

Datenschutzvorfälle

Was ist in einem Notfall wichtig?

IT-Notfallvorsorge



IT-Notfallvorsorge

- Schnelle Reaktion durch Erkennung und Meldung
- Ereignisse protokollieren und festhalten
- Verantwortliche Personen informieren
- Weiteren Schaden verhindern

VERHALTEN BEI IT-NOTFÄLLEN

 **Ruhe bewahren & IT-Notfall melden**
Lieber einmal mehr als einmal zu wenig anrufen!

 IT-Notfallrufnummer:

 Wer meldet?

 Welches IT-System ist betroffen?

 Wie haben Sie mit dem IT-System gearbeitet?
Was haben Sie beobachtet?

 Wann ist das Ereignis eingetreten?

 Wo befindet sich das betroffene IT-System?
(Gebäude, Raum, Arbeitsplatz)

Verhaltenshinweise

Weitere Arbeit am IT-System einstellen	Beobachtungen dokumentieren	Maßnahmen nur nach Anweisung einleiten
--	--------------------------------	--

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik

IT-Notfallvorsorge

Der IT-Notfallprozess muss...

- ✓ bekannt und umsetzbar sein.
- ✓ anhand der maximal tolerierbaren Ausfallzeit geplant sein.
- ✓ Abhängigkeiten beachten. (technisch, organisatorisch, vertraglich)



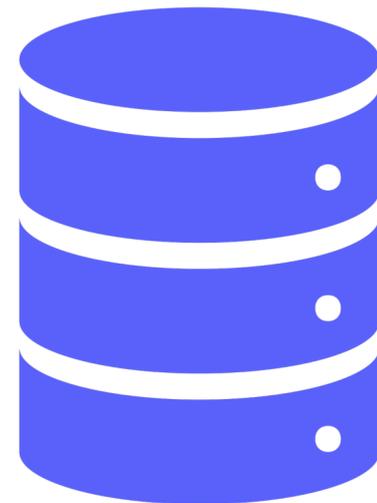
BSI-Standard 100-4: Notfallmanagement;
BSI-Standard 200-4: Business Continuity Management

IT-Notfallvorsorge

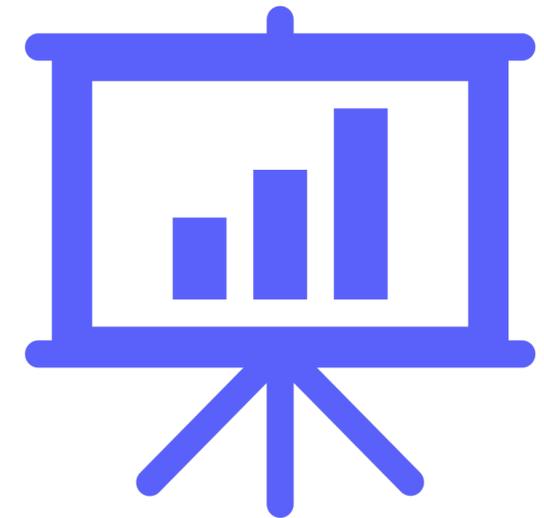
Datensicherung



Bride and Groom - Photo by Tiffany Dawn Nicholson



Kundendatenbank



Kronjuwelen

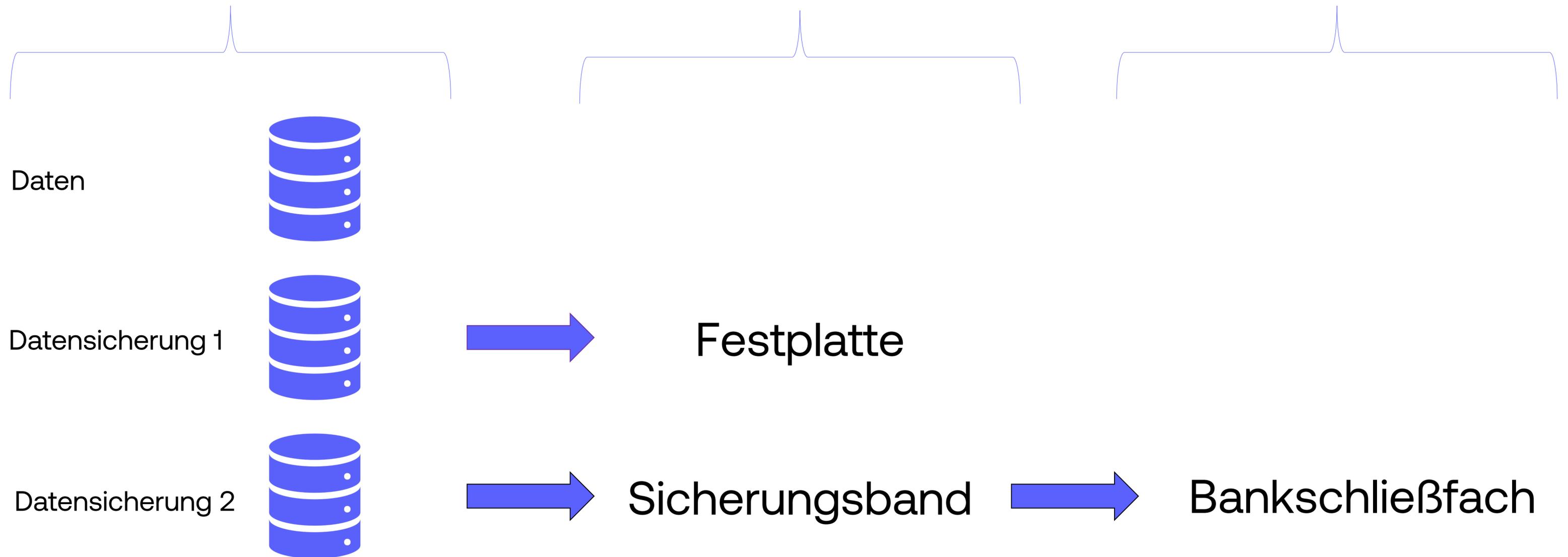
Individuelle Güter

IT-Notfallvorsorge Richtige Datensicherung

3 x Daten

auf 2 Medien

an einem entfernten Standort







Präsentation + Links:
linkla.ma/datenleck

