
genua.
Trust No One
Sichere Verwaltungsdigitalisierung
mit Zero Trust?

Ausgangslage

Funktionierende IT wird immer kritischer

- **Mehr Digitalisierung**
  kritischer Geschäftsprozesse und Daten
- **Mehr Abhängigkeit**
  von funktionierenden digitalen Prozessen
- **Mehr Anforderungen**
  an Verfügbarkeit, Integrität und Vertraulichkeit

Usability essentiell für Akzeptanz

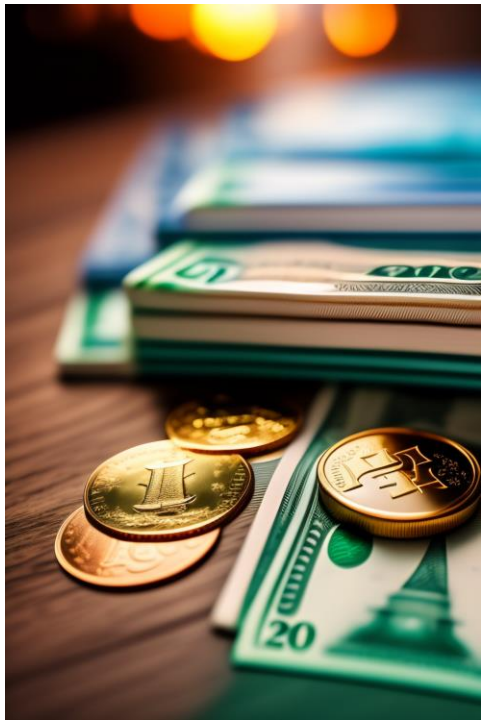
- Unterstützung **neuer Arbeitsweisen**
- **Ungestörtes Arbeiten** trotz IT-Sicherheit, Datenschutz und Compliance
- **Zusatzaufwände** müssen gering bleiben

Konkurrierende Anforderungen

Stabilität,
Verfügbarkeit

Integrität,
Vertraulichkeit

Agilität, Flexibilität,
dynamisches Umfeld



Bezahlbarkeit

Zunehmender Kontrollverlust

- Steigende **Komplexität**

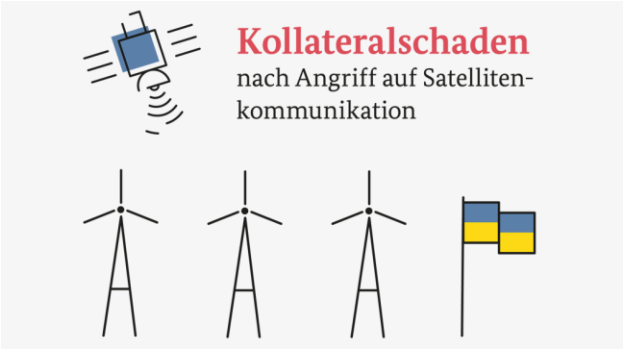
  → abnehmende Beherrschbarkeit
- Mehr **Verantwortung** auslagern

  → Risiken behalten
- Mehr **Verschlüsselung**

  → weniger Kontrollmöglichkeiten

Steigende Verwundbarkeit

- Wachsende **Attraktivität als Ziel** für Angreifer
- Wachsende **Angriffsfläche**
- Zeitnahe **Updates nicht ausreichend**



https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

Steigende Verwundbarkeit

Anwendungen

Kompromittierte Exchange-Server
Zunahme von Angriffen per Mail

Fragen an IT-Sicherheitsverantwortliche:

- Sind die aktuellen Updates auf Exchange-Servern eingespielt?
- Wie groß waren die Zeitfenster zwischen dem Bekanntwerden von Exchange-Server-Schwachstellen und dem Ausrollen der Patches?
- Kam es in der Vergangenheit bereits zu Auffälligkeiten beim Exchange-Betrieb?
- Wurden die vom BSI bereitgestellten Empfehlungen umgesetzt?

https://www.heise.de/news/Exchange-Luecken-BSI-ruft-IT-Bedrohungslage-rot-aus-5075457.html

Affected commercial services include Amazon Web Services, Cloudflare, iCloud, Minecraft: Java Edition, Steam, Tencent QQ and many others. According to Wiz and EY, the vulnerability affected 93% of enterprise cloud environments.

Wikipedia
https://en.wikipedia.org › wiki › Log4Shell

Log4Shell - Wikipedia

Remote Zugänge

Aktive Ausnutzung einer Schwachstelle in Fortinet SSL-VPN

Datum 13.12.2022

https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2022/2022-283701-1032.pdf

Remote-Code-Schwachstelle in PulseConnect Secure SSL-VPN-Gateway

Datum 03.05.2021

https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-208085-1012.html

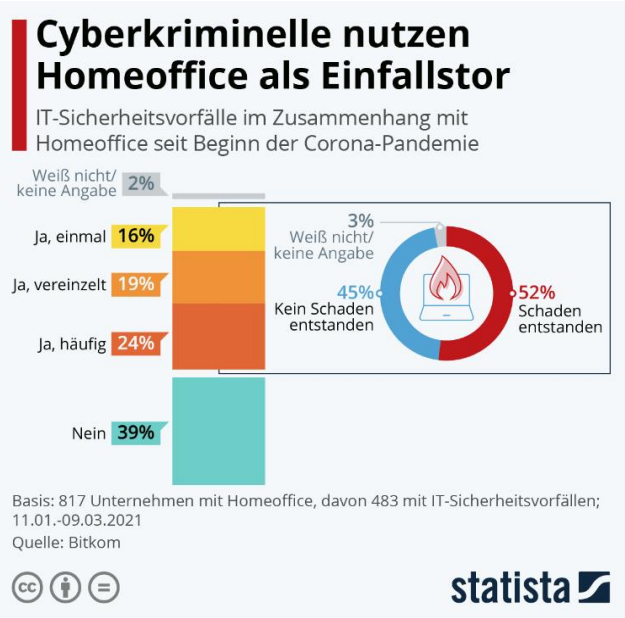
Juniper-Skandal: China übernahm angeblich Hintertür in Netzhardware

Vor Jahren sorgte eine Hintertür für Kopfschütteln, die Juniper wohl selbst in seine Produkte eingebaut hatte und die dann jemand übernahm. Das war wohl China.

kompromittieren. Wer davon wusste, hätte nicht nur VPN-Verkehr entschlüsseln, sondern auch alle Spuren solch eines Angriffs verschwinden lassen können. Das

https://www.heise.de/news/Juniper-Skandal-China-uebernahm-angeblich-Hintertuer-4942914.html

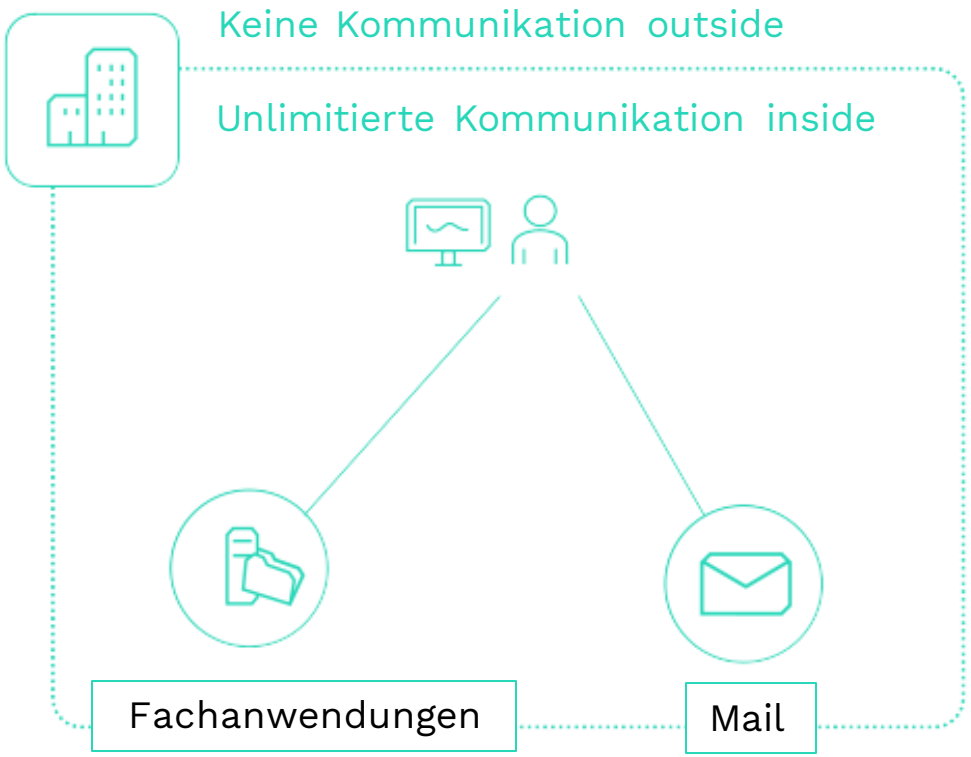
Mobilität



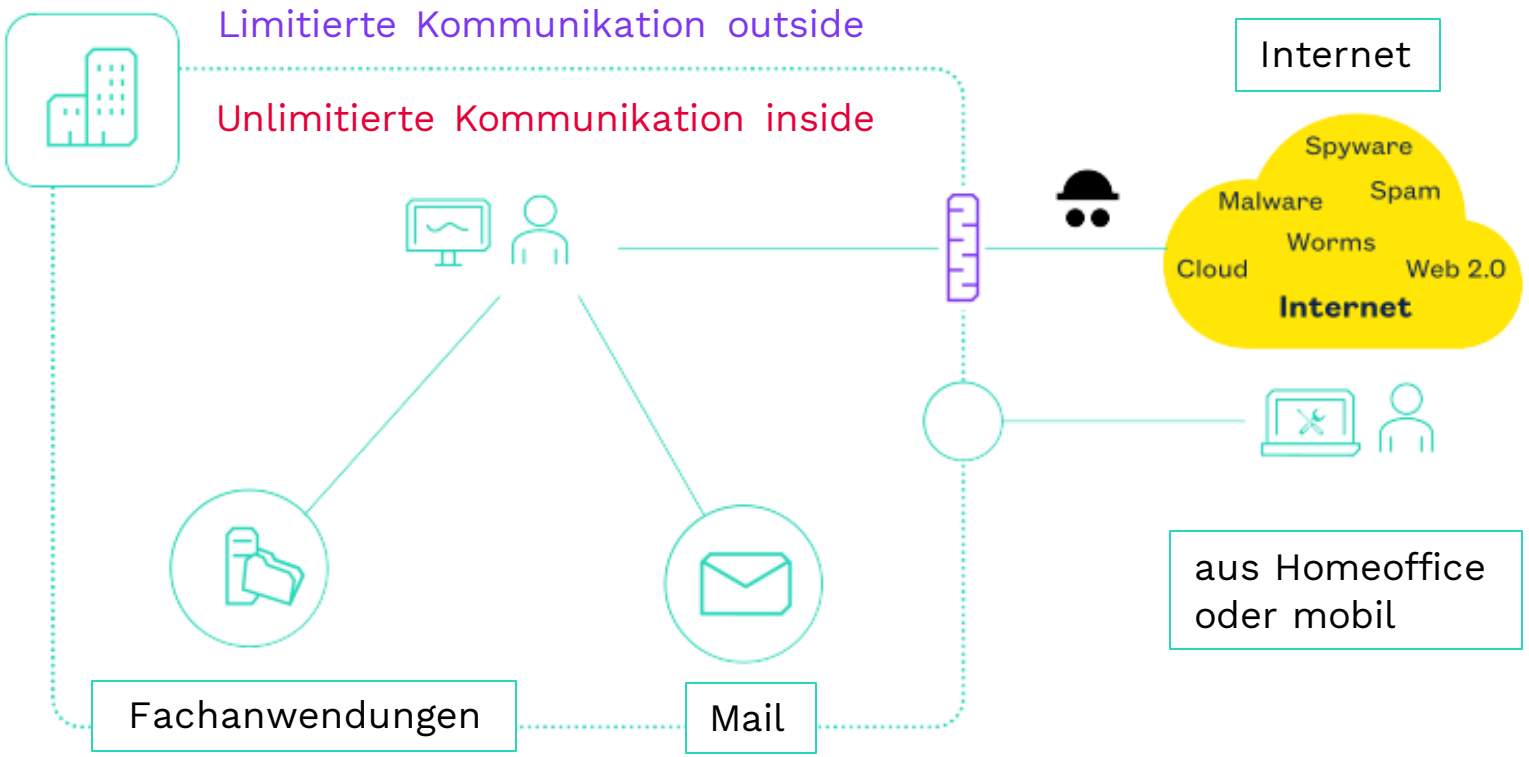
https://de.statista.com/infografik/25605/it-sicherheitsvorfaelle-im-zusammenhang-mit-homeoffice-seit-beginn-der-corona-pandemie/

Lösungsansätze

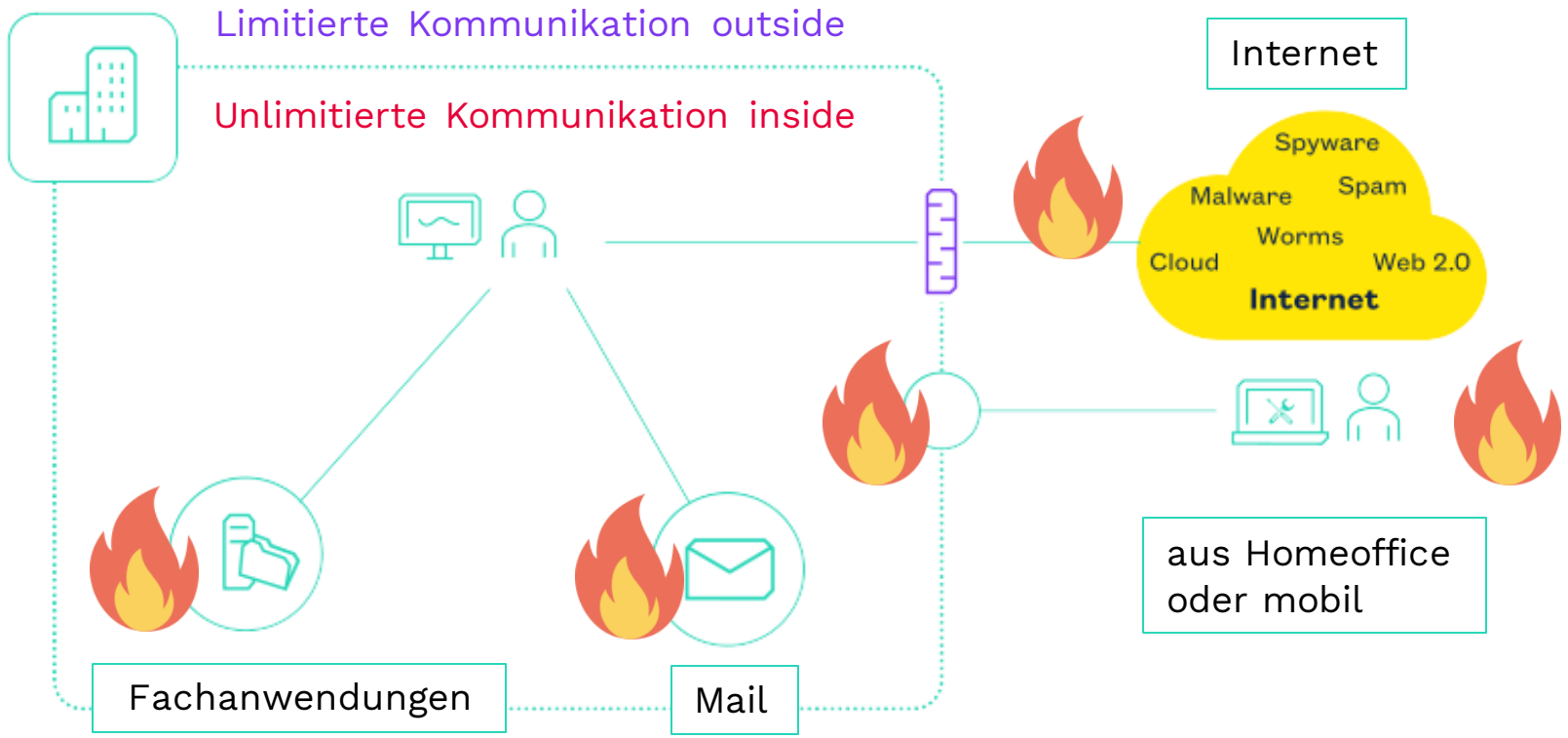
IT-Infrastruktur: Gestern



IT-Infrastruktur: Heute



Angriffsflächen für Angreifer



Lösungsansätze - Reaktiv

Sicherheitslücken schließen - Updates

- Kommen zu spät oder gar nicht

Schaden verringern - Monitoring, Reaktion, Recovery

- Fehlende Planbarkeit von Vorfällen
- Geleakte Daten bleiben öffentlich
- Temporär eingeschränkte Verfügbarkeit

Lösungsansätze - Proaktiv

Erreichbarkeit der Lücken verhindern

- Angriffsfläche verkleinern

Auswirkungen verringern

- Datenabfluss, C&C und Ausbreitung bremsen

Menge und Schwere von Lücken verringern

- Security by Design

→ **Mehr Zuverlässigkeit, Ruhe und Planbarkeit**

Zero Trust für proaktive Sicherheit

Nur so viel Zugriff wie **nötig**

- Just in time, just enough

Nur so viel Zugriff wie **akzeptabel**

- Vertrauen in Kommunikationspartner

Trust But Verify: Überprüftes Vertrauen

Vertrauen in **Dienst**

- Identität, Sicherheit

Vertrauen in **Benutzer**

- Identität, Gerätesicherheit, Umgebung

Vertrauen in **Netz**

- Verschlüsselung

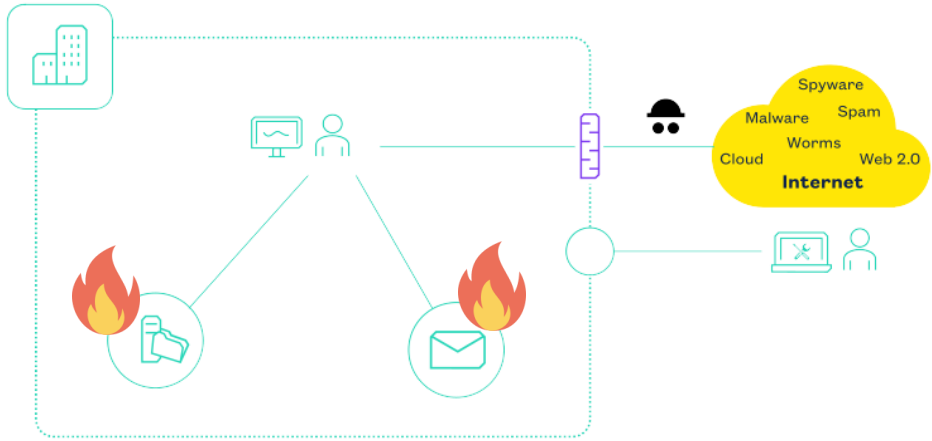
Zero Trust Konkret:
Schutz vor kompromittierter Anwendung

Restriktion der Kommunikation am Dienst

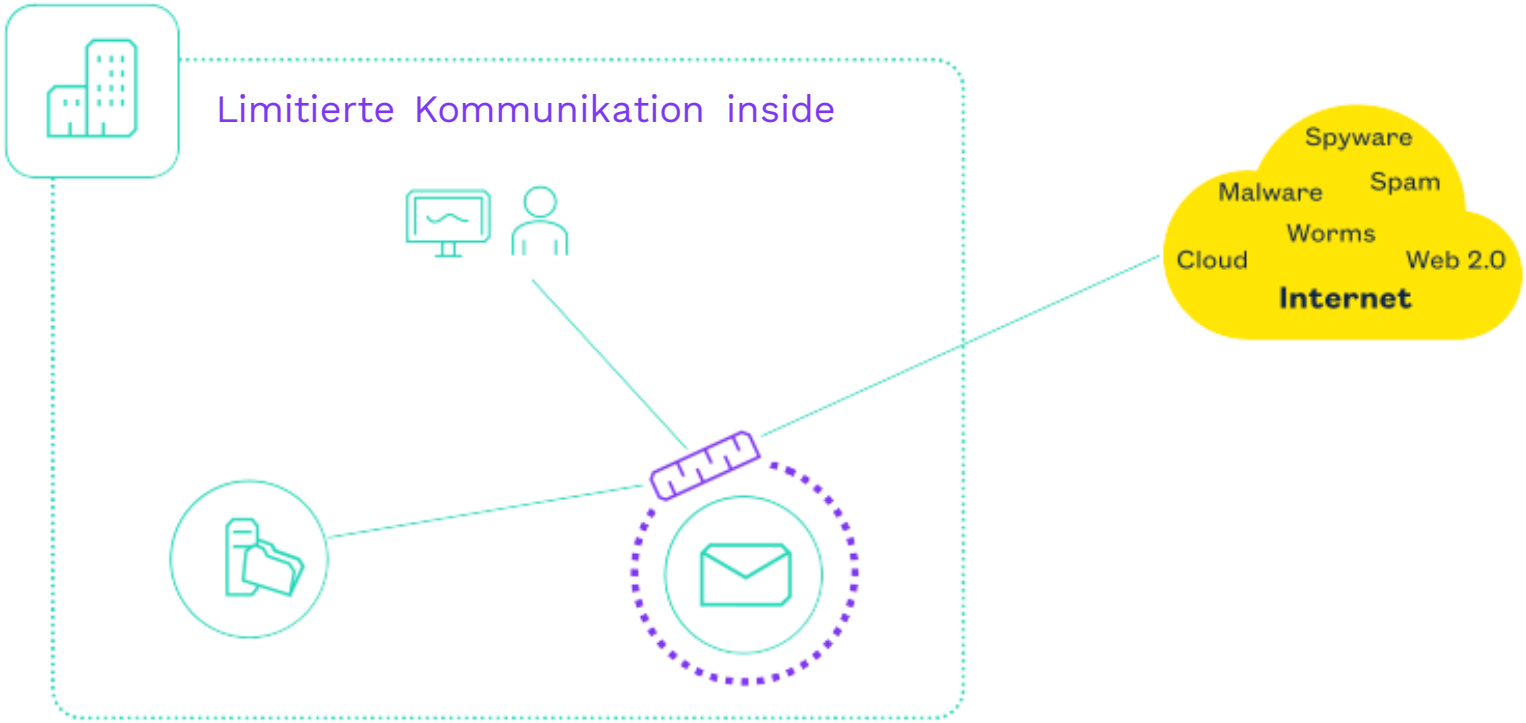
- **eingehend**: Angriffe von außen oder lokalem Netz
- **ausgehend**: C2, Exfiltration, Ausweitung Infektion

Umsetzung durch

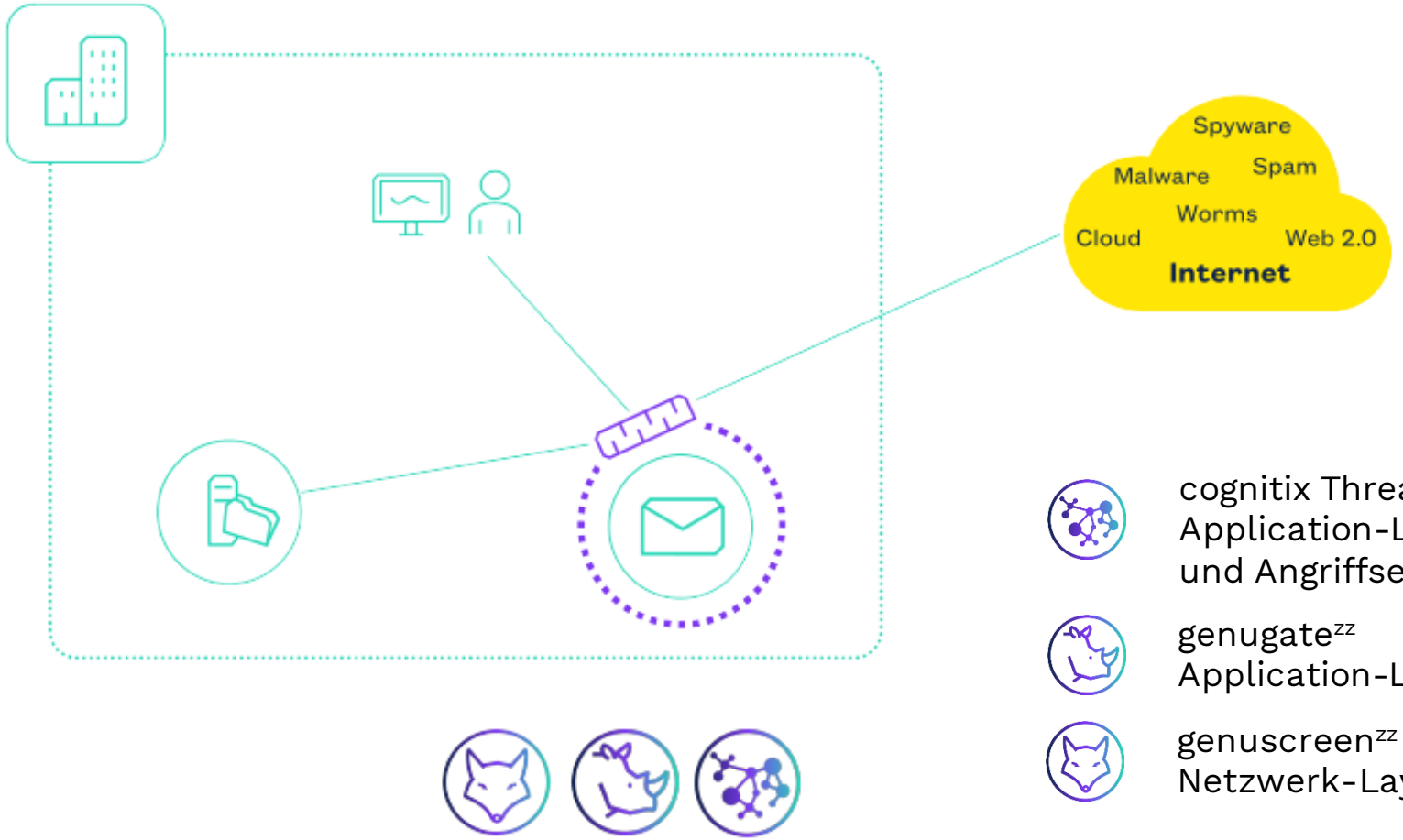
- **Mikroperimeter** selektiv um einzelne Systeme
- **Mikrosegmentierung** des gesamten inneren Netzes



Mikroperimeter um Dienst



genua Produkte für Mikroperimeter



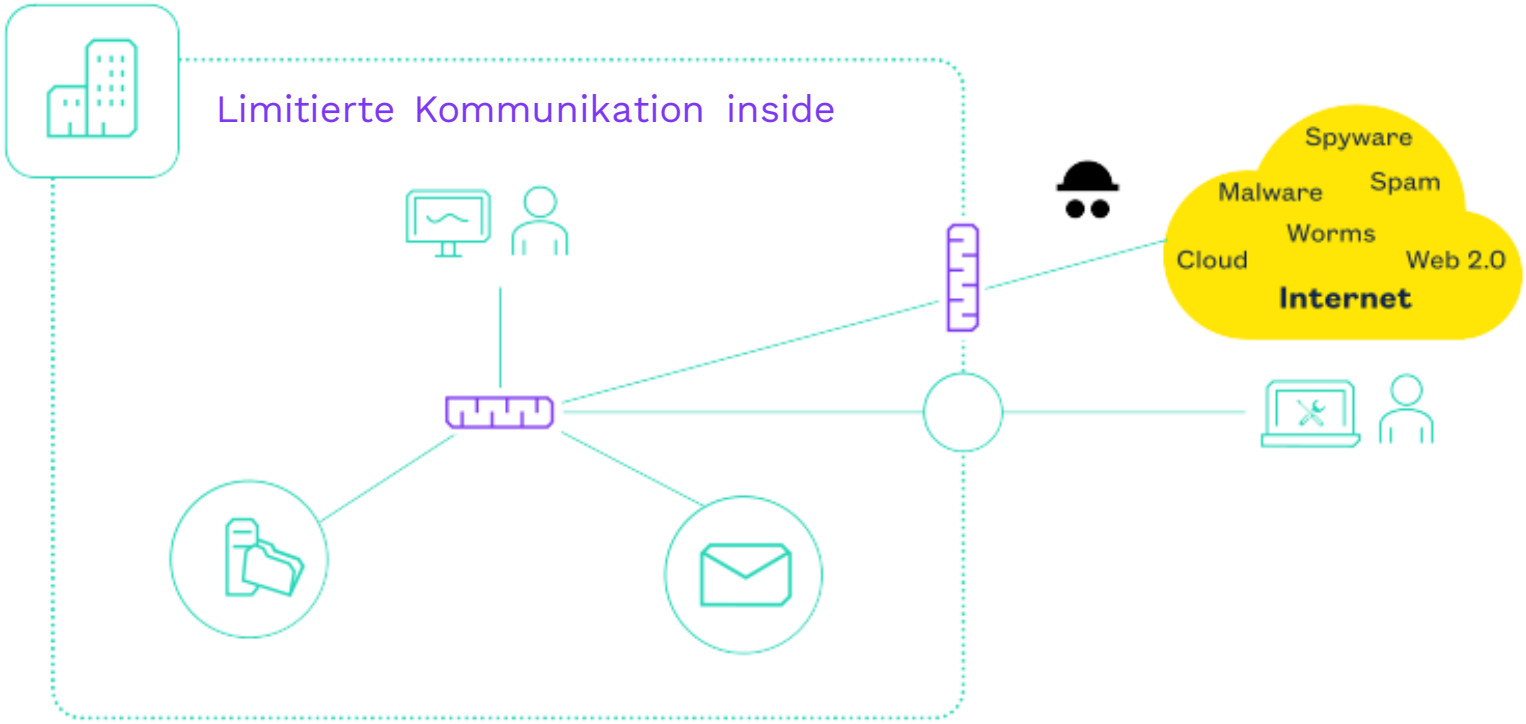
cognitix Thread Defender
Application-Layer Mikrosegmentierung
und Angriffserkennung

genugate[zz]
Application-Layer Firewall

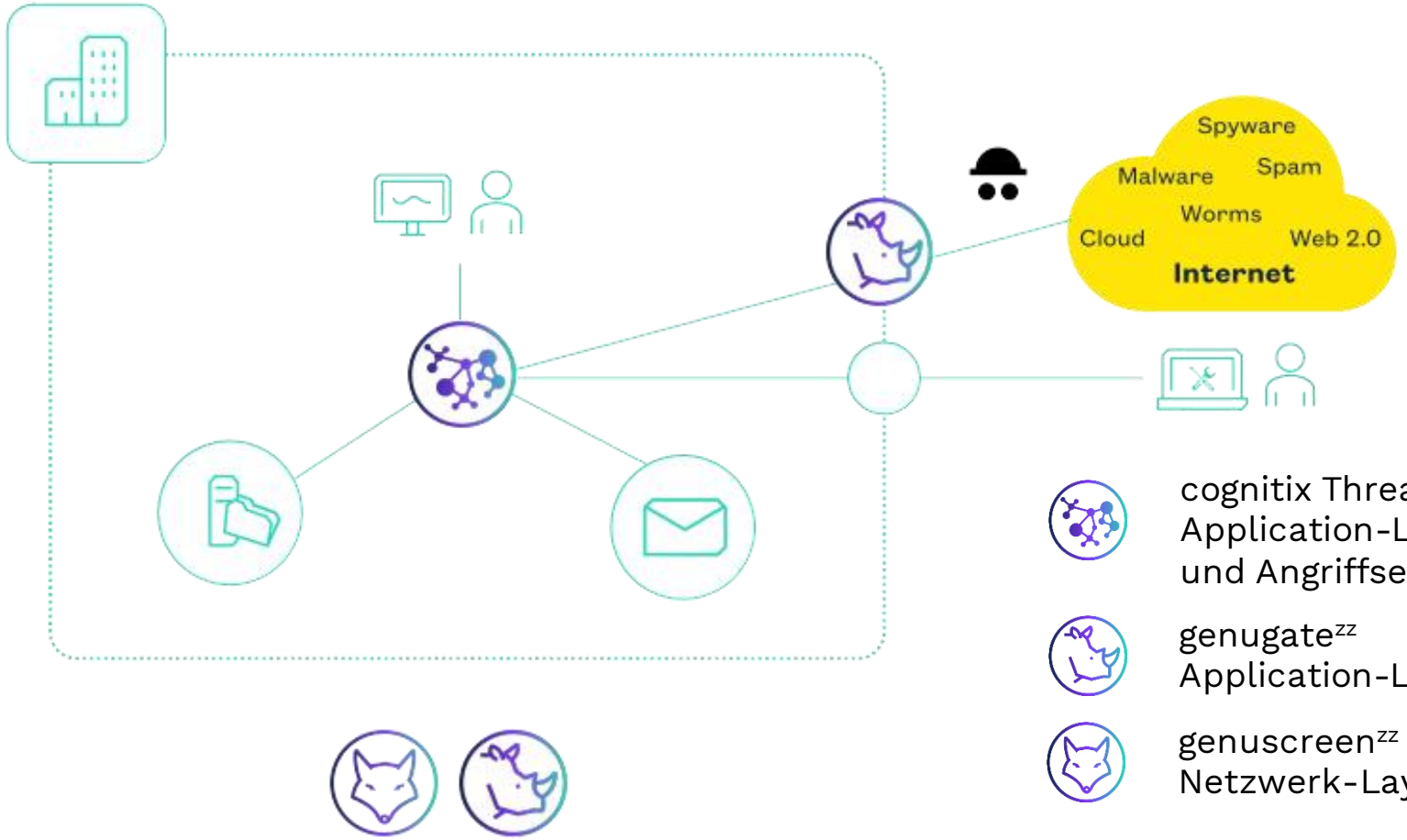
genuscreen[zz]
Netzwerk-Layer Firewall

[zz]EAL4+, VS-NfD, NATO RESTRICTED, RESTREINT UE/EU RESTRICTED

Mikrosegmentierung im LAN



genua Produkte für Mikrosegmentierung



cognitix Thread Defender
Application-Layer Mikrosegmentierung
und Angriffserkennung

genugate[zz]
Application-Layer Firewall

genuscreen[zz]
Netzwerk-Layer Firewall

[zz]EAL4+, VS-NfD, NATO RESTRICTED, RESTREINT UE/EU RESTRICTED

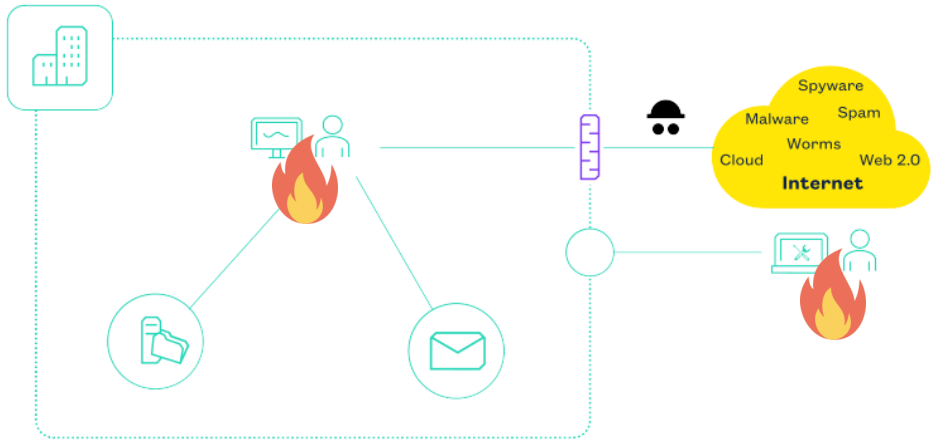
Konkret: Schutz vor kompromittiertem Nutzer

Schutz auf **Netzebene**

- Zugangskontrolle zum Netz
- Kommunikation im Netz

Schutz auf **Anwendungsebene**

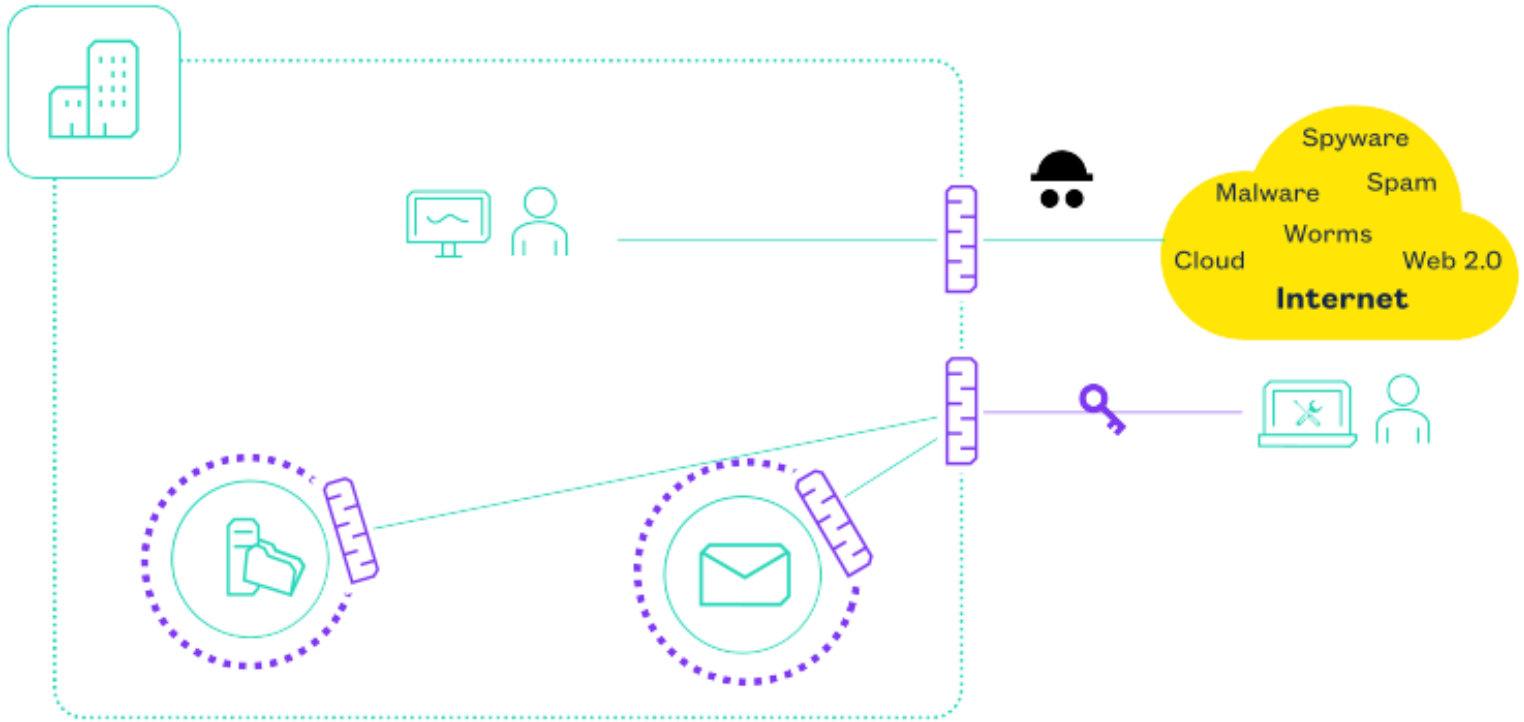
- Zugangskontrolle zur Anwendung
- Zugriffskontrolle innerhalb Anwendung: Daten, Aktionen



Umsetzung durch Kontrollfunktionen

- in VPN-Einwahlknoten
- Zugangsproxy vor Anwendung
- in Anwendungslogik

Granulare Trust Zugriffskontrolle



Identitäten für managebare Kontrolle

Zero Trust erlaubt Anforderungen an Sicherheitsbedarf ausrichten

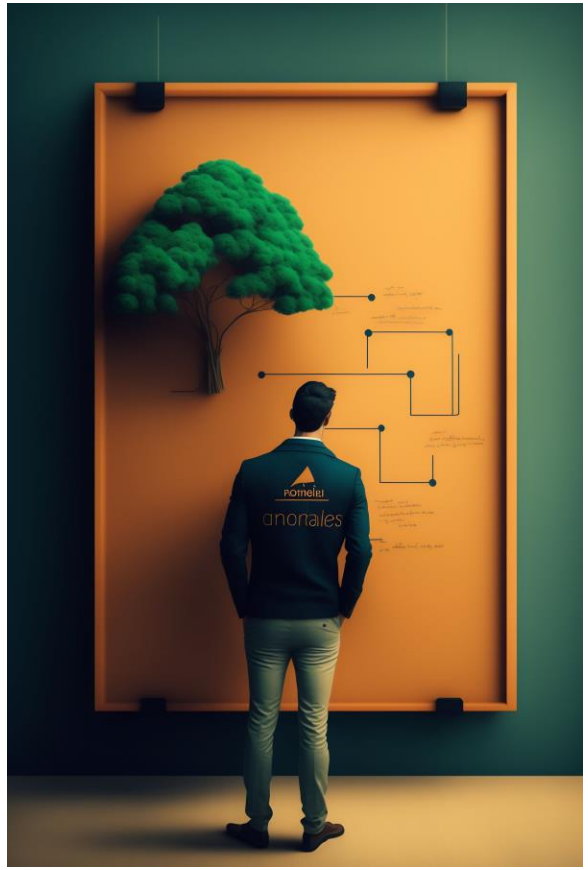
→ höhere **Akzeptanz** bei Anwendern, weniger Konflikt mit IT

Digitale Identitäten als Anker von Zugriffsentscheidungen

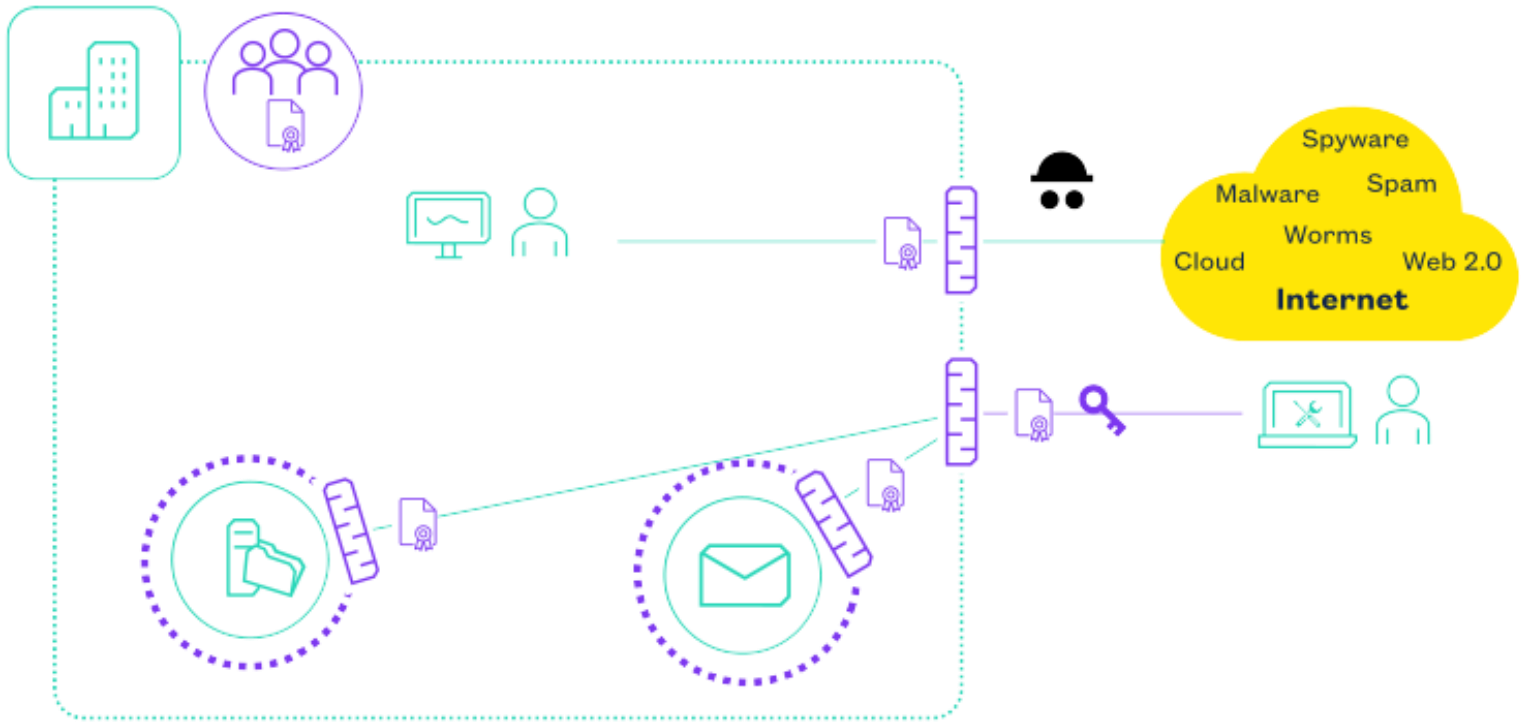
- Ortsunabhängig → tauglich für Cloud und Mobilität

Ausgerichtet an betrieblichen Strukturen und Prozessen

- Mehr **Verständlichkeit**, **Automatisierung**, einfachere **Compliance**
- **Effizienz** durch Integration von IT-Sicherheit in Arbeitsprozesse

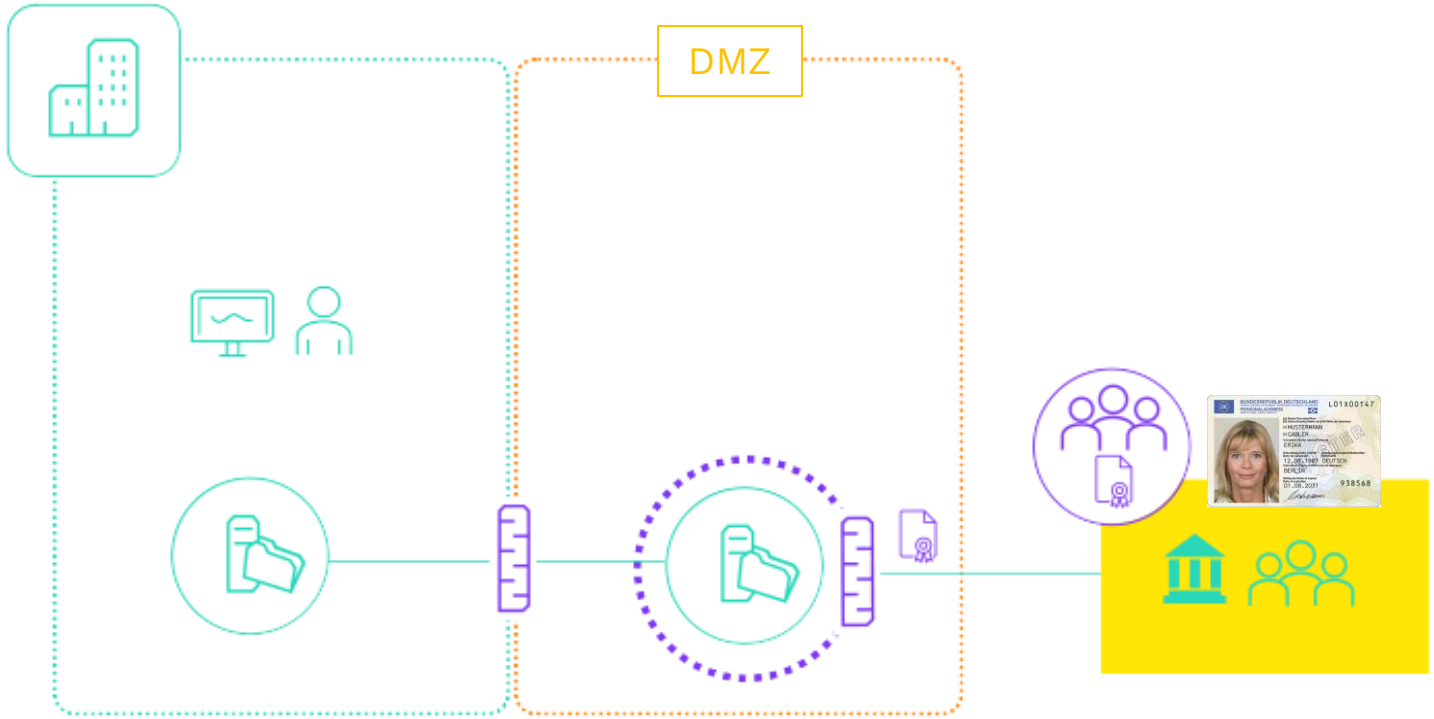


Identitätsbasierte Zero Trust Zugriffskontrolle



- ☑ Identität
- ☑ Gerät
- ☑ Umgebung

Zero Trust für OZG



- ☑ **Identität**
- ☑ Gerät
- ☑ Umgebung

Vertrauen als Grundlage

Weitere Quellen des Vertrauens

Vertrauen in **Sicherheit der verwendeten Produkte**

- Security by Design, Komplexität, Drittkomponenten, …

Vertrauen in **Hersteller**

- Kompetenz, Werte

Vertrauen in **verwendete Technologien**

- Unbewusste oder gezielte Designschwächen

Nötiges **Vertrauen abhängig vom Schutzbedarf** der Prozesse und Daten

Wie bekommt man mehr Vertrauen

Mehr Vertrauen durch **ganzheitliche Kontrolle**

- Kommunikation: Nutzer, Gerät, Ort
- Implementation: Open Source vs. Closed Source
- Legal: welcher Gesetzgebung unterliegt Hersteller

Robusteres Vertrauen durch **Defense in Depth**

- Mehrere Kontrollschichten
- Restriktive Ausführungsumgebungen
- Separation unsicheren Inputs von sensitiven Daten

Kritisches Vertrauen in Sicherheitsprodukte

Firewalls, VPN, ... sind an **kritischen Positionen im Netz**

- Sollen schützen - nicht zusätzliche Gefahr darstellen

Entsprechend sehr **hohe Anforderungen an Design und Qualität**

- genua baut seit 2002 EAL4-zertifizierte und zugelassene Produkte

Security by Design ist in unserer DNA

Trust No One? → Trust But Verify!

Softwareupdates alleine sind nicht ausreichend

- Kommen zu spät oder gar nicht

Proaktive Absicherung bringt Ruhe und Zuverlässigkeit

- Mehr Planbarkeit, höhere Verfügbarkeit

Zero Trust verbessert die proaktive Absicherung

- genua unterstützt Sie – heute und in Zukunft

IT-Sicherheitslösungen
für den öffentlichen Bereich

SecurITy made in Germany

genua. Ein Unternehmen der Bundesdruckerei

Transparente Qualitätssicherung: **Zulassungen und Zertifizierungen vom BSI** dokumentieren die hohe Sicherheitsleistung unserer Lösungen.

Rechenzentrum

vs-diode
Hochsichere Einbahn-Datentransfers bis GEHEIM

Cloud Security Gateway
Umfassender Schutz für private Cloud Services

genubox
Kontrollierte Remote Maintenance

Liegenschaft

genuscreen
Sichere Vernetzung mit VS-NfD-Zulassung

Behörde

cognitix Threat Defender
Anomalieerkennung und Reaktion auf Bedrohungen

genuscreen
Sicherheitszonen im Netzwerk mit VS-NfD-Zulassung

genugate
Robuster Netzwerkschutz mit VS-NfD-Zulassung

genucenter
Komfortable und effiziente Administration

Mobile Mitarbeiter

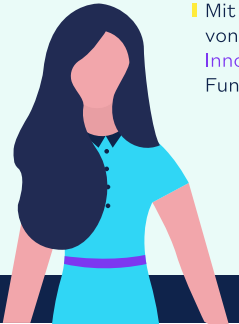
genuconnect
VPN Software Client mit VS-NfD-Zulassung für unterwegs

Homeoffice

genucard
IT-Security im Homeoffice mit VS-NfD-Zulassung

Damit die Digitalisierung gelingt, benötigen wir solide IT-Infrastrukturen. Dafür setzen wir auf verlässliche Lieferanten und fordern unabhängige Qualitätsnachweise wie Zertifizierungen und Zulassungen vom BSI.

VPN-Lösungen schützen vertrauliche Kommunikation innerhalb unserer großen Netze vor Lauschangriffen.



Mit Smart Government profitieren auch wir von den Potenzialen der digitalen Transformation. Innovative IT-Sicherheitslösungen bilden das Fundament für diese Entwicklung.

Zugelassene Software Clients schützen eingestufte Daten auch unterwegs und erlauben so mobiles Arbeiten.

Dank genucard arbeiten unsere Mitarbeiter flexibel und sicher im Homeoffice.

Teil der Bundesdruckerei-Gruppe bdr.

Infografik: 2issue, Grafiken: shutterstock

Wir sind für Sie da.

Lassen Sie uns gemeinsam die Digitalisierung sicher gestalten!

Los geht’s!

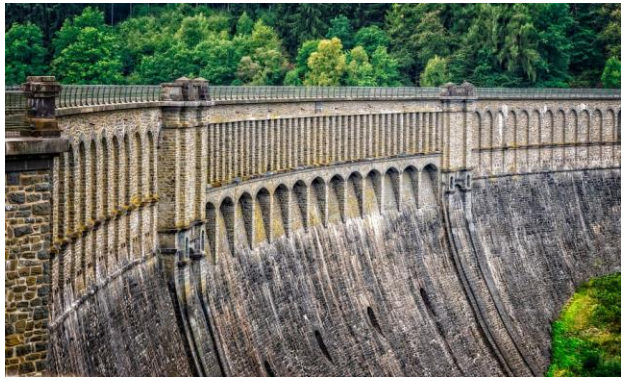
Kontakt

genua GmbH
Domagkstraße 7
85551 Kirchheim bei München

T +49 89 991950-0
F +49 89 991950-999
M info@genua.de

www.genua.de

Diskussionsvorschläge



Proaktive Absicherung von IT-Infrastrukturen

- Verständnis der eigenen Infrastruktur
- Relevanz proaktiver Absicherung in dieser
- Herausforderungen bei der Umsetzung

Rolle der Mitspieler bei der IT-Sicherheit

- Grundsicherheit von Anwendungen und IT-Komponenten
- Einbindung der Anwender (Mitarbeiter)
- Regularien (Zulassungen, CRA, ...): wichtig oder Störfaktor
- IT-Sicherheitslösungen: Hoffnungen vs. Realität