SWS COMPUTERSYSTEME
Member of ACP Group

8. SWS Security Forum

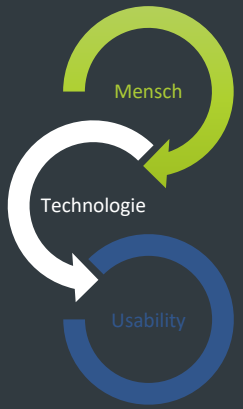
29.04.2021

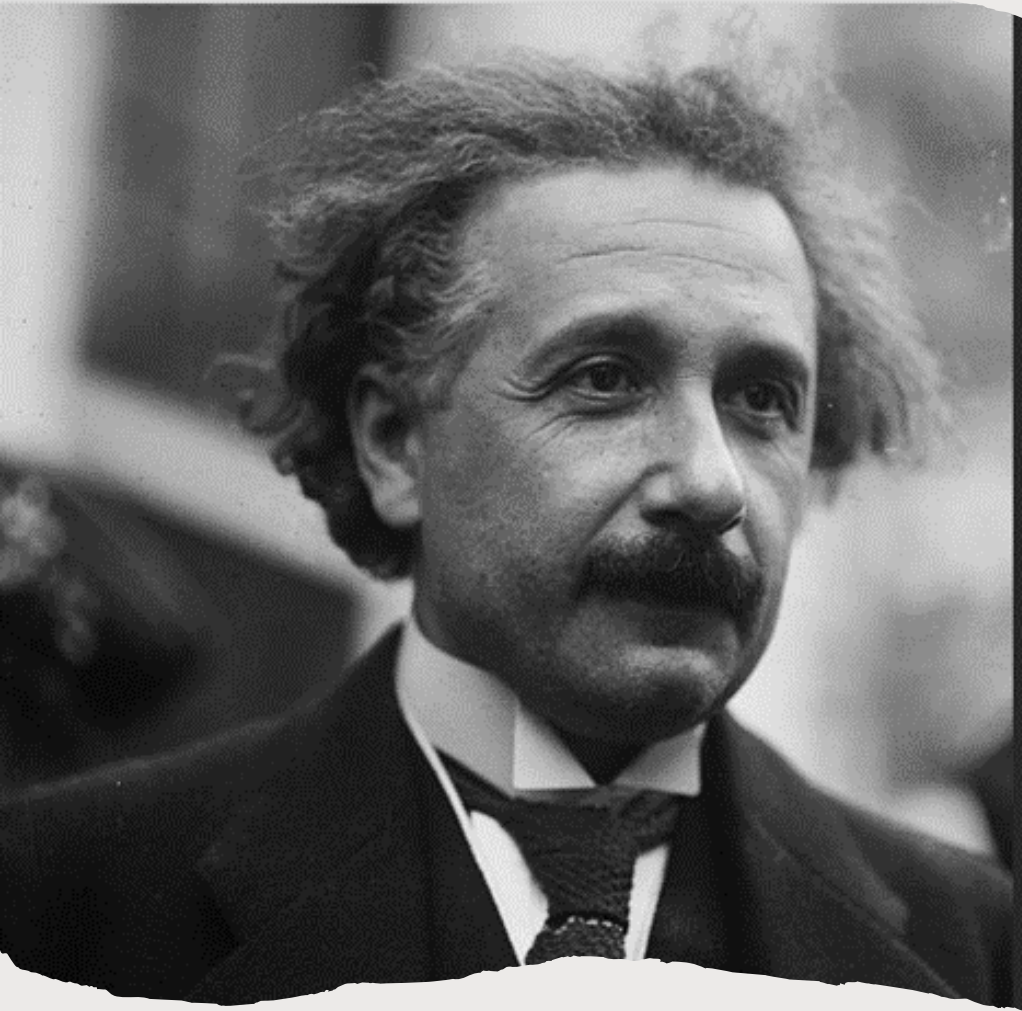
Mensch, Technologie, Sicherheit

Der Schutz vor Cyberattacken ist ein ständiger Balanceakt zwischen Sicherheit, Usability und Funktionsfähigkeit.“

Im Rahmen des 8. Security Forums der SWS Computersysteme AG haben wir uns selbst eine Aufgabe gestellt: Bewusstsein zu schaffen für die Bedrohungen von außen, gleichzeitig aber auch aufzuzeigen, wo im Zusammenspiel von „Mensch und Maschine“ kritische Situationen entstehen

In Zeiten der allgegenwärtigen Digitalisierung ist es fast unmöglich, die IT-Security ständig und ohne Unterstützung im Auge zu behalten. Wie stelle ich als Verantwortlicher sicher, dass meine Mitarbeiter Angriffe erkennen und die notwendigen Fähigkeiten besitzen, diese abzuwehren?





“To raise new questions, new possibilities, to regard old problems from a new angle, requires creative imagination and marks real advance in science.”

Die Security Formel?

- Neue Fragen (a)
- Neue Möglichkeiten (b)
- Alte Probleme (c) – Neuer Blickwinkel (d)
- Kreative Vorstellungskraft (e)
- Fortschritt in der Wissenschaft (f)

$$S(f)=(a+b – c(d))*e$$

Neue Fragen

- Wie verändert 4.0 unsere Umwelt
- Was verändern Ereignisse wie Pandemien
- Was lernen wir aus den jüngsten Ereignissen
- Wie sieht die (Arbeits)-welt in Zukunft aus
- …

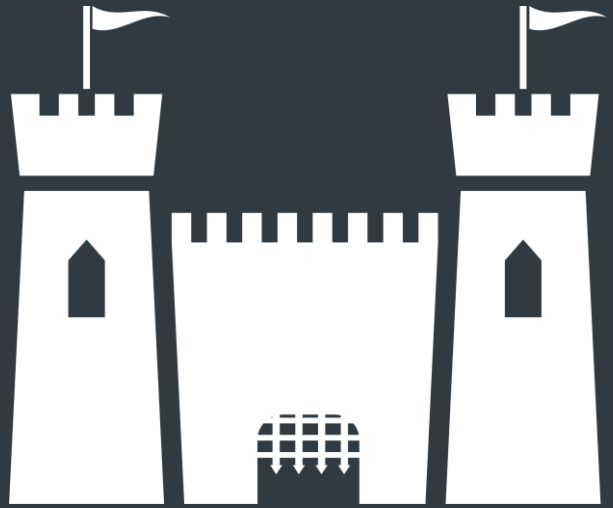
Aktuelle Trends – aber sicher

- Cloud (Public, Privat, Hybrid)
- Digital Workplace/Mobile Enterprise
- IIoT
- Managed Services
- SOC/SIEM
- …

SWS COMPUTERSYSTEME
Member of ACP Group

Alte Probleme…

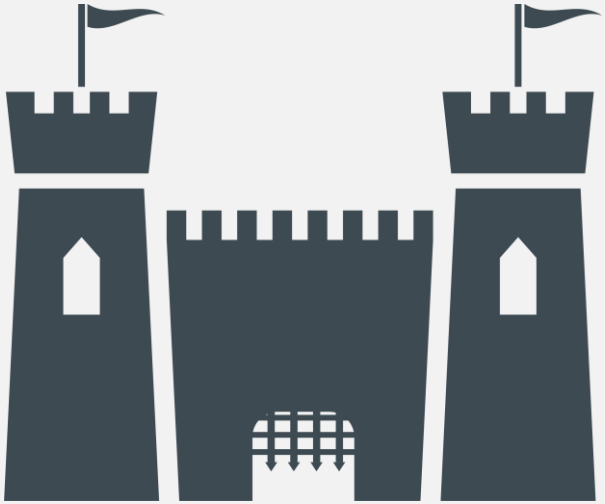
… aus einem neuen Blickwinkel zu betrachten



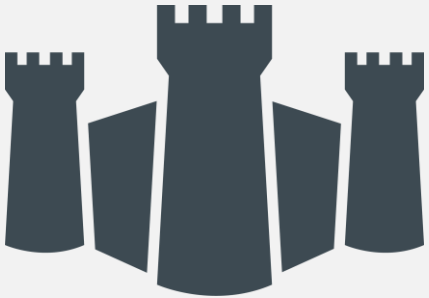
Alte Probleme…

… aus einem neuen Blickwinkel zu betrachten

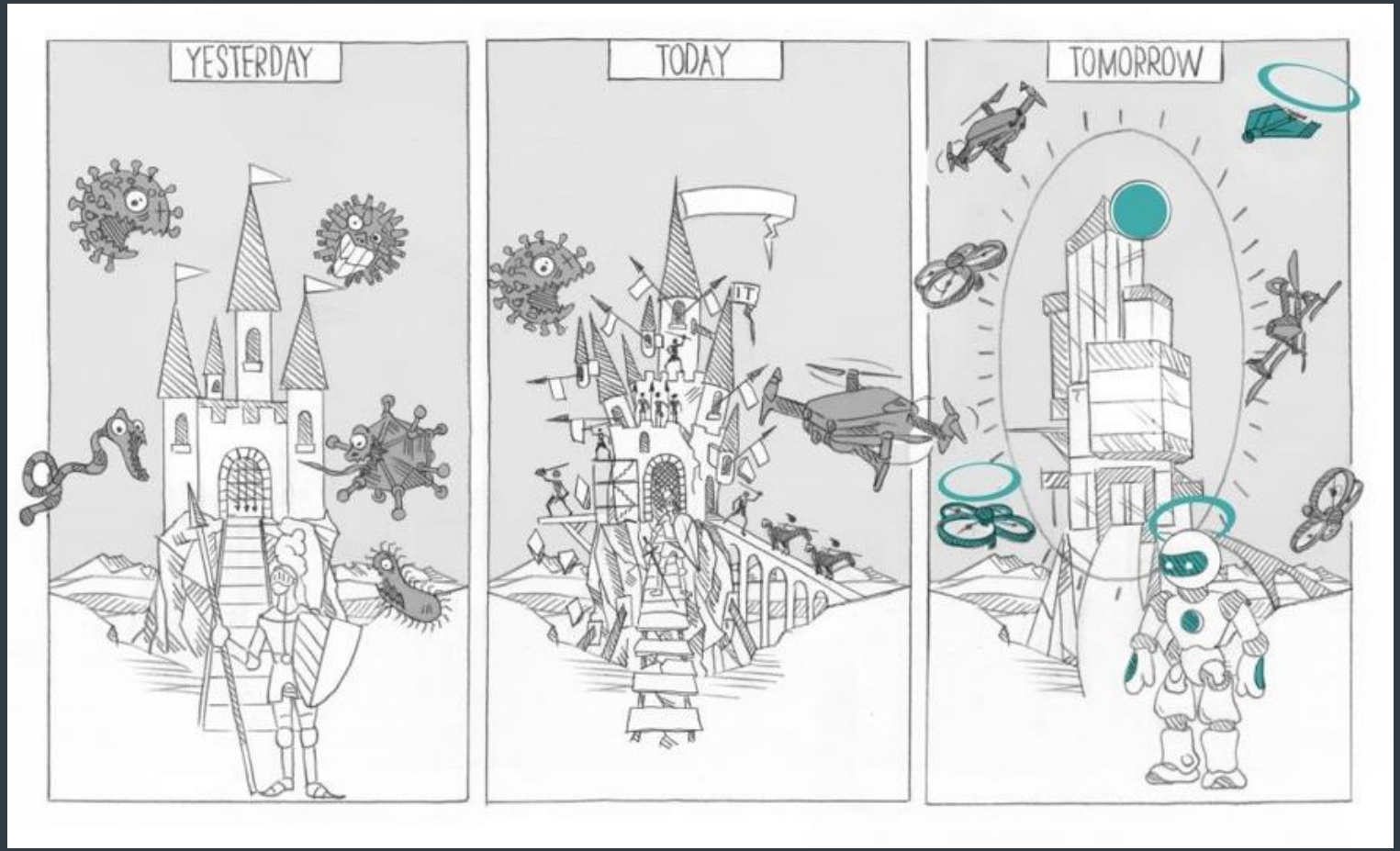
Homeoffice



Niederlassung



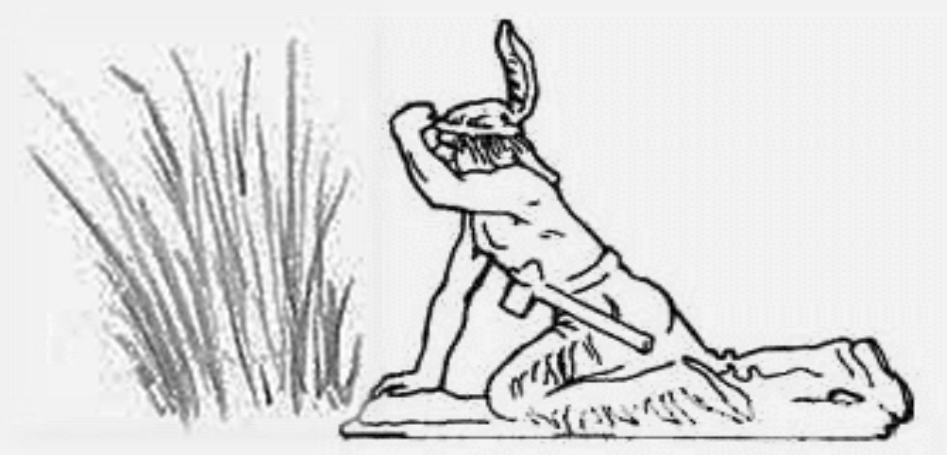
SWS COMPUTERSYSTEME
Member of ACP Group

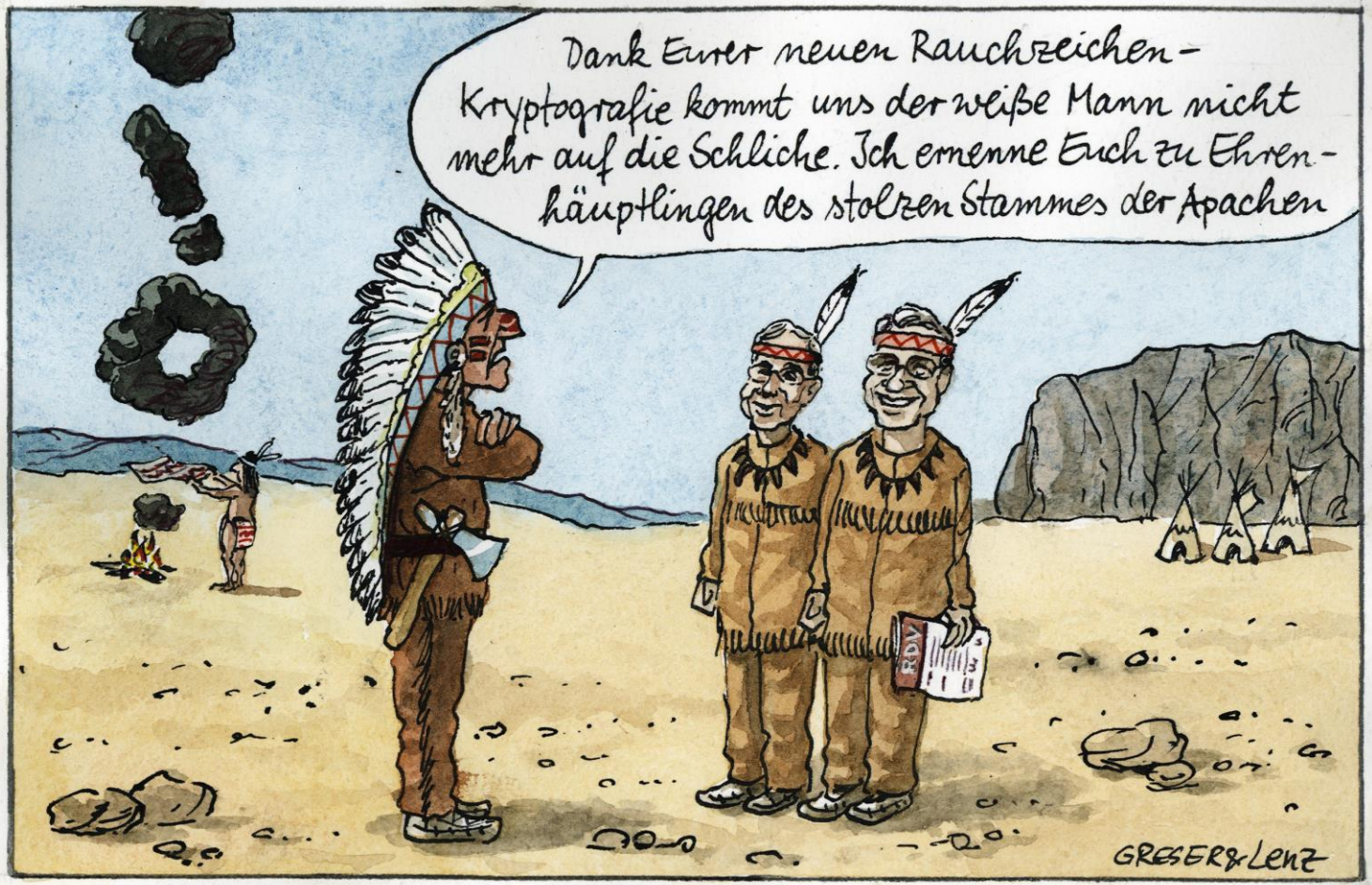


Bedrohungen

- Verlust von betrieblichen Daten
- Verlust oder Abfluss PII bzw. besonders schützenswerter Daten (Art. 9 DSGVO), >Erpressung mit deren Verkauf oder Veröffentlichung
- Mangelnde Transparenz

Authentizität, Integrität, Vertraulichkeit





Aus den Anfängen von Datenschutz und Datensicherheit

War das wirklich der CEO, der gerade am Telefon eine Überweisung angeordnet hat – oder eine Maschine?

Quelle: https://www.inside-it.ch/de/post/werden-nun-auch-deepfake-voicemails-fuer-ceo-fraud-verwendet-20200728

Deepfake – richtig oder falsch?

Quelle: ZDF

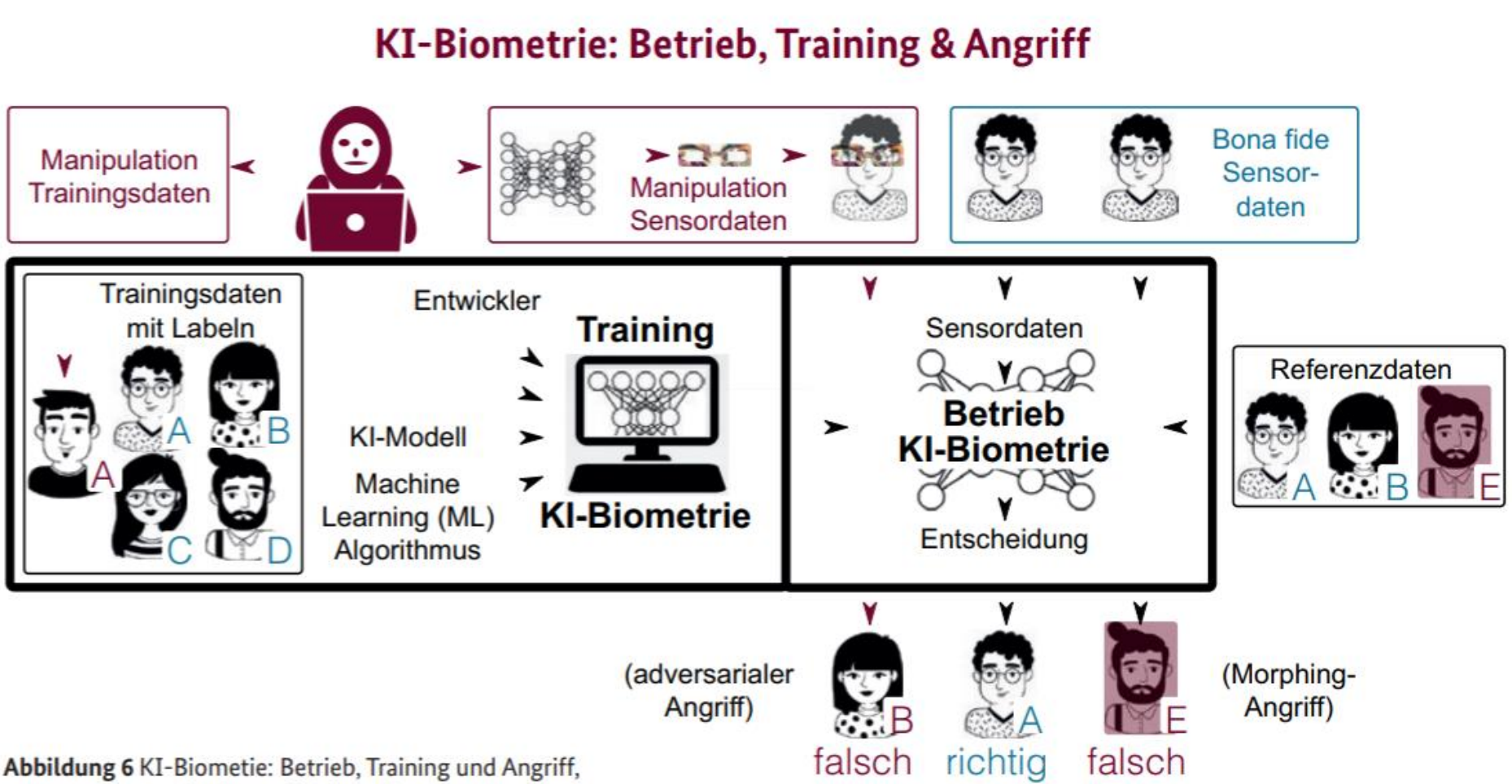


Abbildung 6 KI-Biometie: Betrieb, Training und Angriff, Quelle: https://de.freepik.com, BSI

DEEPFAKES– abgeleitet von den Begriffen Deep Learning und Fake – sind simple aber bösartige Mittel der Manipulation von Bild-, Video oder Audiodateien, bei der biometrische Merkmale wie bspw. Aussehen oder Stimme von CEOs täuschend echt imitiert werden, sozusagen CEO-Fraud 2.0. Die Folgen eines erfolgreich durchgeführten Deepfake können für Unternehmen sowohl aus Datenschutzgründen als auch aus finanzieller Sicht verheerend sein.

Quelle: EbnerStolz Wirtschaftsprüfer

Bedrohungslage

Quelle: BSI Lagebericht 2020

Cyber-Sicherheitslage für Deutschland 2020

Aktion und Reaktion

117,4 MIO. neue Schadprogramm-Varianten

2019: 114 MIO.

durchschnittlich **322.000** neue Schadprogramm-Varianten pro Tag

in Spitzenwerten **470.000**

76 % ist der Anteil unerwünschter SPAM-MAILS an allen in den Netzen des Bundes eingegangenen Mails

▶ 2019: 69 % ◀

24,3 MIO. Patientendatensätze waren Schätzungen zufolge international frei im Internet zugänglich

BOT täglich bis zu **20.000** BOT-INFEKTIONEN deutscher Systeme

419 KRITIS-Meldungen

▶ 2019: 252

▶ 2018: 145

52.000 WEBSEITEN wurden wegen enthaltener Schadprogramme durch die Webfilter der Regierungsnetze gesperrt

35.000 Mails mit Schadprogrammen wurden durchschnittlich pro Monat in deutschen Regierungsnetzen abgefangen

109.000 Abonnenten Bürger-CERT

▶ 2019: 105.000

▶ 2018: 100.000

rund **100** Produkte und Standorte hat das BSI im Bereich Common Criteria zertifiziert

mehr als **4.400** Mitglieder der Allianz für Cyber-Sicherheit

▶ 2019: 3.700

▶ 2018: 2.700

rund **1.700** registrierte KRITIS-Anlagen

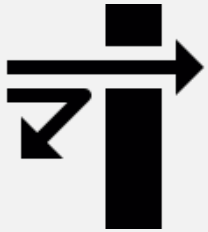
knapp **7 MIO.** Meldungen zu Schadprogramm-INFEKTIONEN übermittelte das BSI an deutsche Netzbetreiber

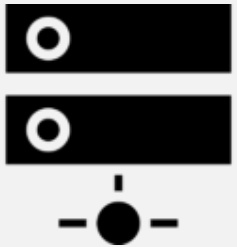
Herausforderungen

- Endpunkt-Management (Arbeitsstationen, Server und Drucker)
  - Transparenz über alle vorhandenen Geräte?
  - Aktualität von Betriebssystem, Anwendungen und Firmware/BIOS
  - Schwachstellen-Management
  - Patch-Management

Herausforderungen

- Infrastruktur-Management (aktive Komponenten)
  - Transparenz über alle vorhandenen Geräte?
  - Aktualität des Betriebssystems
  - Schwachstellen-Management
  - Patch-Management



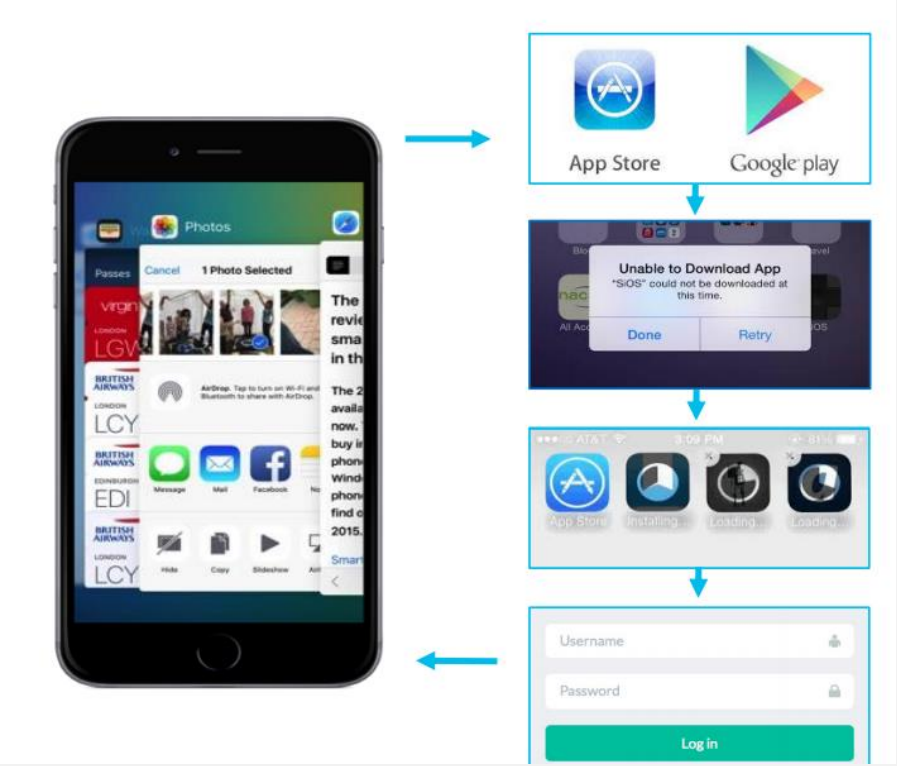


Herausforderungen

- BYOD
  - Trennung von privaten und betrieblichen Daten
  - Persönlichkeitsrechte des Mitarbeiters
  - OS noch unterstützt / Patchlevel?
  - Einsatz feststellbar?

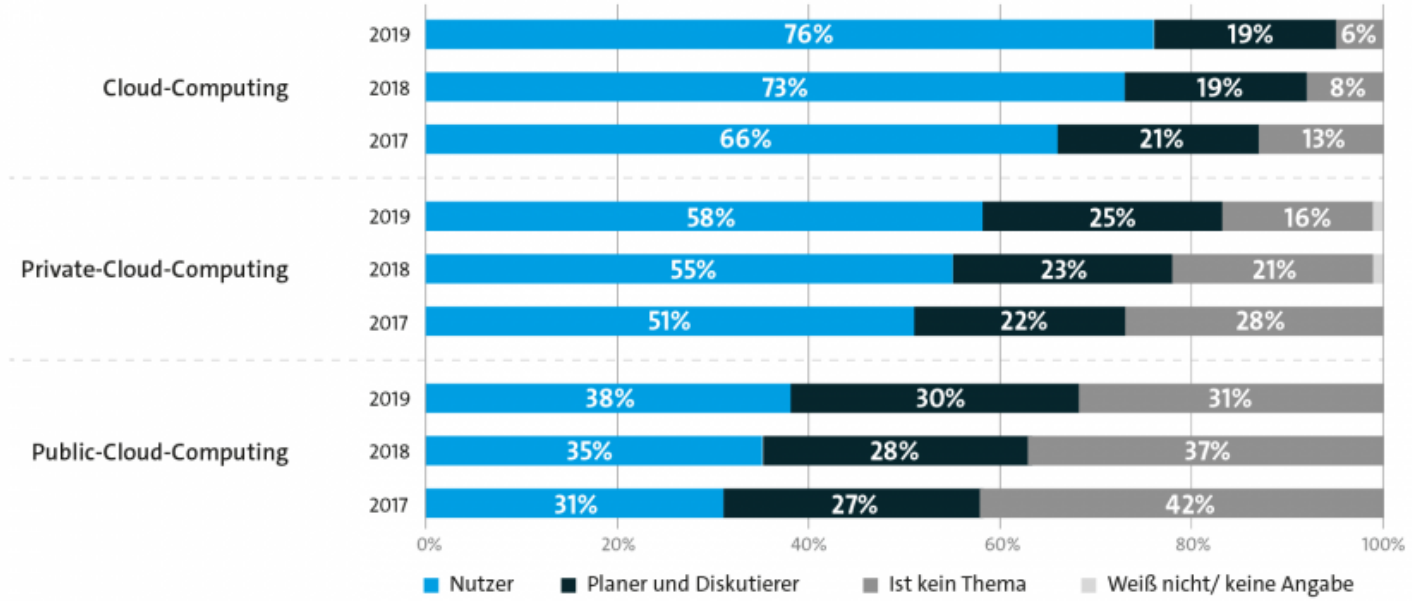
- PUOCE / COPE
  - Nutzungsrahmen genau zu definieren
  - Trennung von privaten und betrieblichen Daten

Mobiler Zugriff auf digitale Anwendungen und sensible Unternehmensinformationen



Drei von vier Unternehmen nutzen Cloud-Computing

Inwieweit nutzt Ihr Unternehmen bereits Cloud-Computing bzw. plant oder diskutiert den Einsatz?



Basis: Alle befragten Unternehmen (2019: n=555 | 2018: n=553 | 2017: n=557)
von 100 Prozent abweichende Werte ergeben sich aus Rundungsdifferenzen. | Quelle: Bitkom Research

Herausforderungen

- Cloud
  - Verwendete Applikationen
  - Dateiablage
  - Zugriffsschutz
  - Shadow IT
  - DNS Einträge

SWS COMPUTERSYSTEME
Member of ACP Group

Notebook wird im Heim-WLAN genutzt und infiziert sich
→**Wie stoppen Sie Angreifer vor einer Datenexfiltration?**
→**Wie unterbinden Sie Command & Control Verbindungen?**

User ruft schadhafte Domains / Anhänge z.B. in privaten Mails auf
→ **Wie überprüfen Sie diese Dateianhänge?**
→**Wie unterbinden Sie gefährliche Webseiten - auch im Heim WLAN?**
→**Sehen Sie welche User besonders eifrig klicken? (Risikoanalyse!)**

Email

Der Angriffsvektor #1! Dateien und Informationen werden ungehindert empfangen und versendet

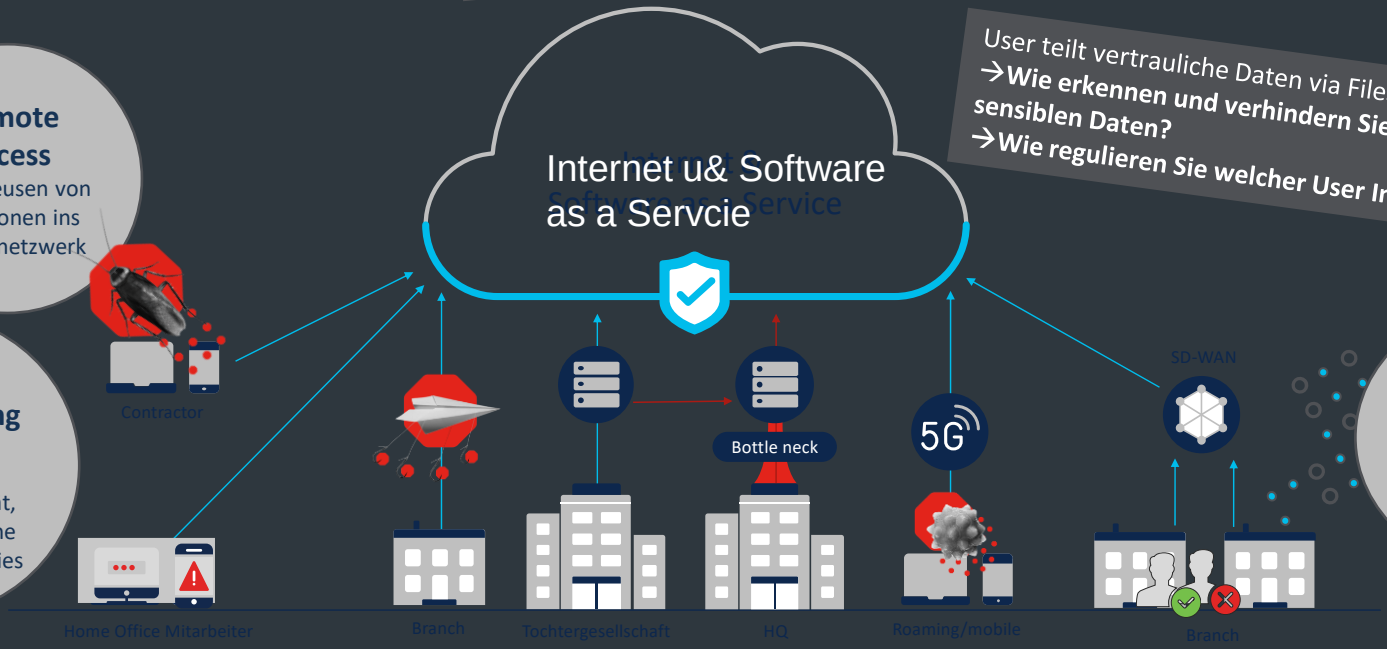
User teilt vertrauliche Daten via FileSharing Plattform
→**Wie erkennen und verhindern Sie den Verlust von sensiblen Daten?**
→**Wie regulieren Sie welcher User Inhalte teilen darf?**

Remote Access

Einschleusen von Infektionen ins Firmennetzwerk

Direkter Internetzugang & SaaS

Oft keine Visibilität, Kontrolle und keine einheitlichen Policies

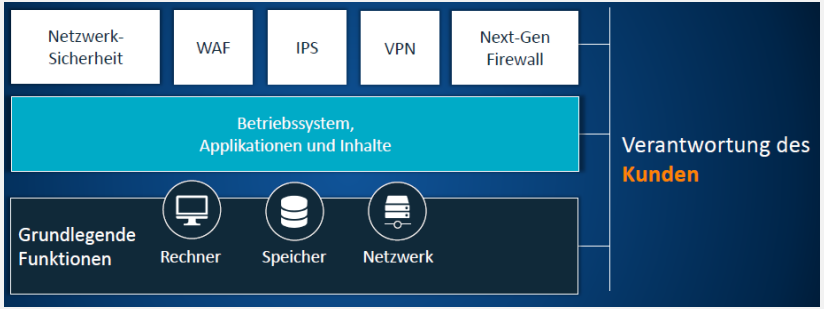


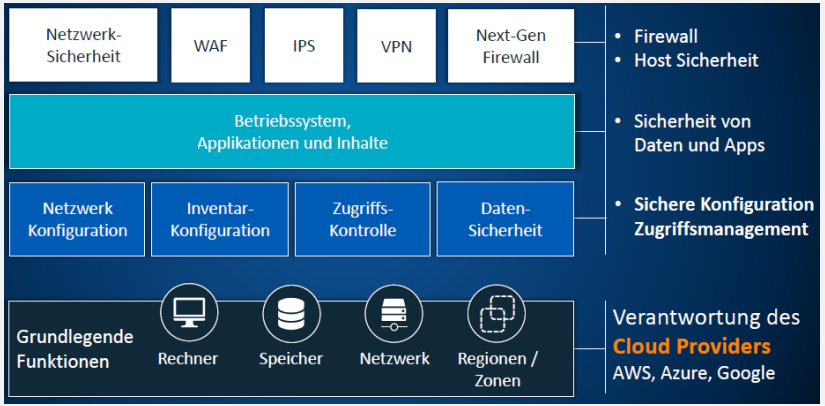
Apps zur Dateiübertragung

Fehlende Visibilität und Kontrolle

Herausforderungen

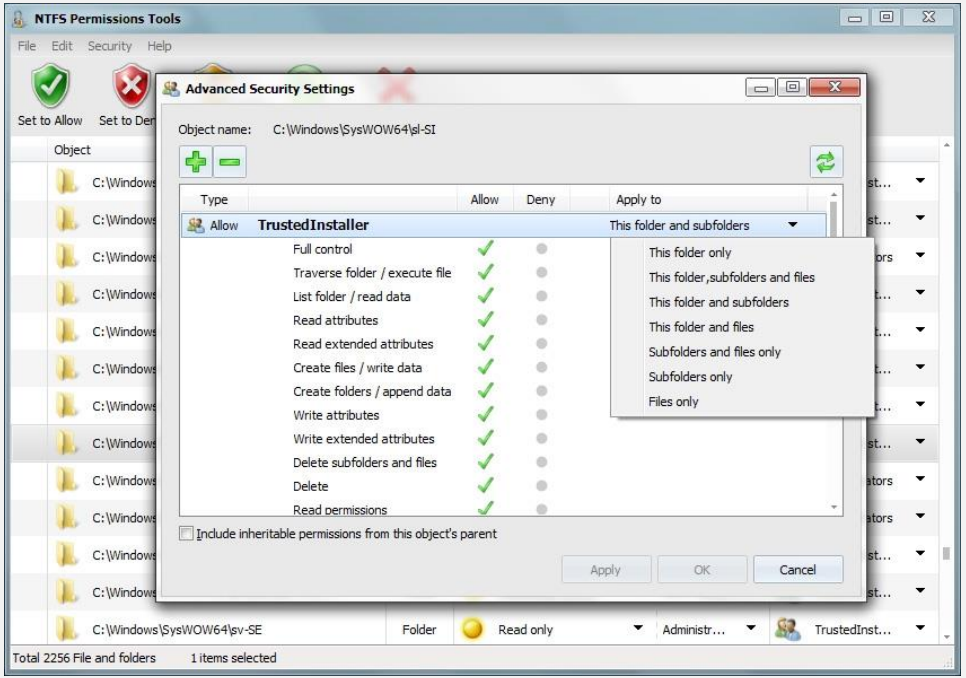
- Fehlerhafte Konfiguration von Cloud-Diensten
  - On-prem und webbasiert
  - Überwachung von Änderungen





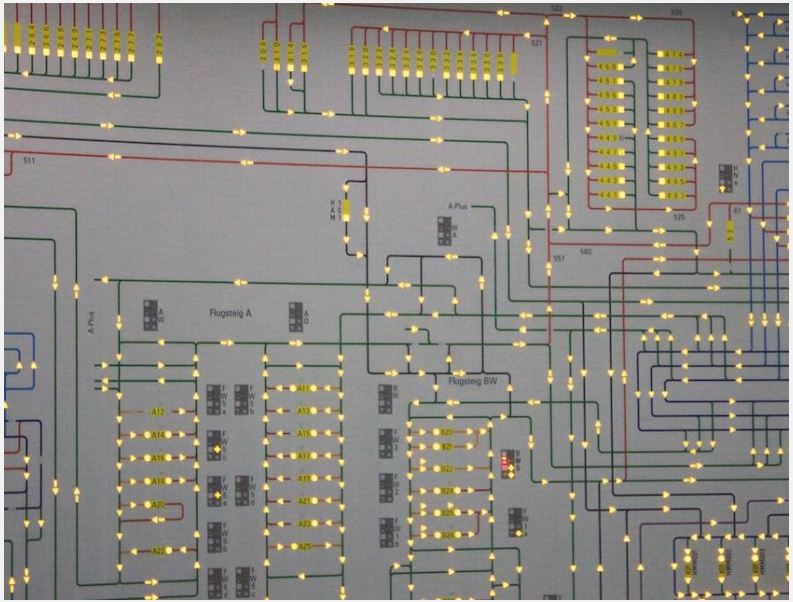
Weitere Herausforderungen

- Dateiberechtigungen
  - Übersicht?
  - Soll-Zustand?
  - Welche Benutzer können auf eine bestimmte Datei zugreifen?
  - Auf welche Dateien kann ein bestimmter Benutzer zugreifen?
  - Was wurde wann von wem zugegriffen / verändert?

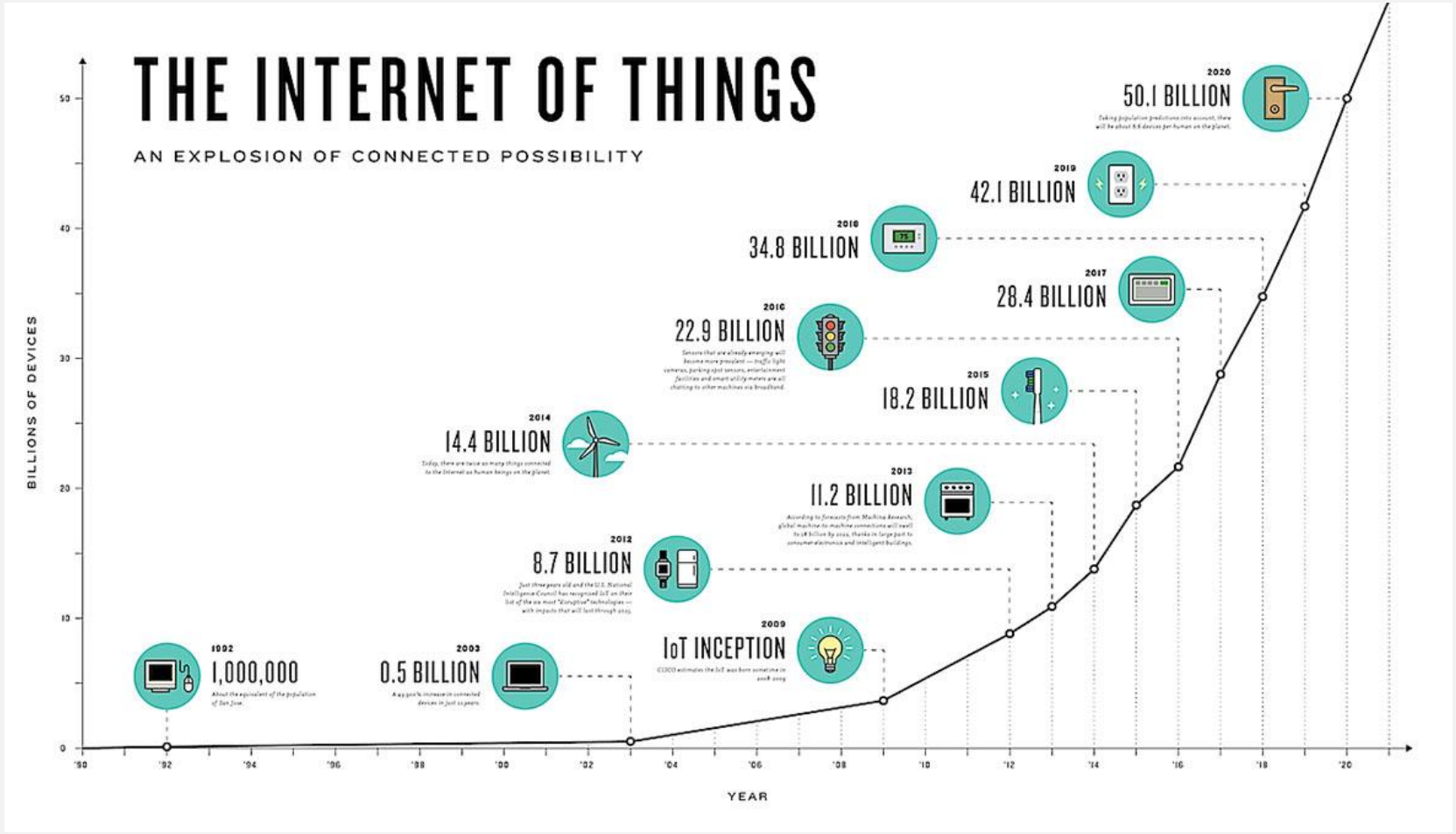


Herausforderungen

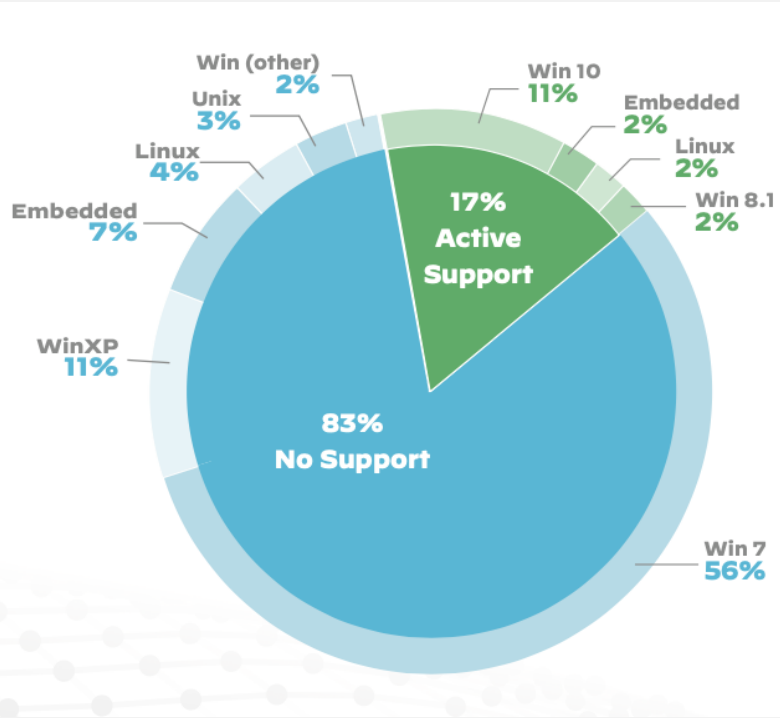
- Was ist der „Normalzustand“?
  - Welche Geräte loggen was und wo?
  - Welches Gerät spricht mit welchem?
  - Welche Internet-Kommunikation ist normal?
- Mangelhafte Reaktionsfähigkeit

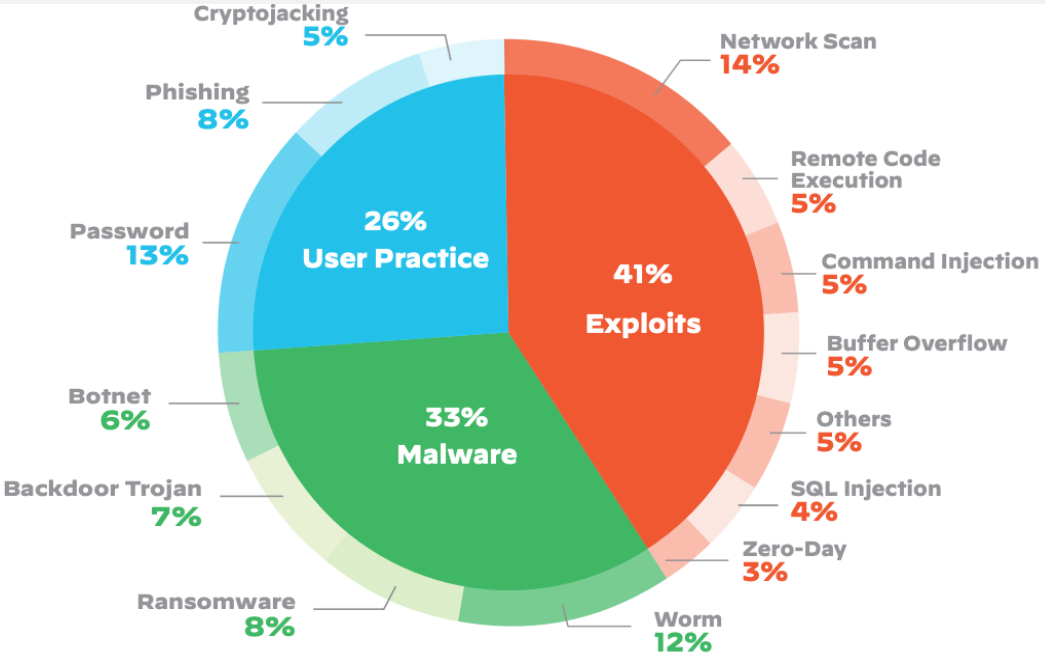


Neue Technologie (Möglichkeiten)
Neue Angriffsflächen


THE INTERNET OF THINGS
AN EXPLOSION OF CONNECTED POSSIBILITY
BILLIONS OF DEVICES
YEAR
1992
1,000,000
About the equivalent of the population of San Jose.
2003
0.5 BILLION
A 499.9% increase in connected devices in just 11 years.
2009
IoT INCEPTION
2012
8.7 BILLION
2013
11.2 BILLION
2014
14.4 BILLION
Today, there are twice as many things connected to the Internet as human beings on the planet.
2015
18.2 BILLION
2016
22.9 BILLION
2017
28.4 BILLION
2018
34.8 BILLION
2019
42.1 BILLION
2020
50.1 BILLION

Herausforderungen (IoT)

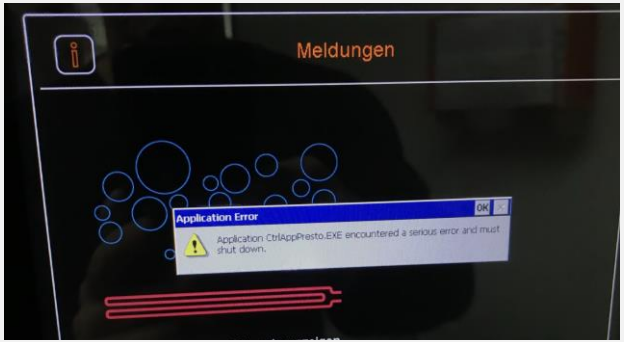




Quelle: www.paloaltonetworks.com, IoT Threat Report 2020

Herausforderungen (IoT)

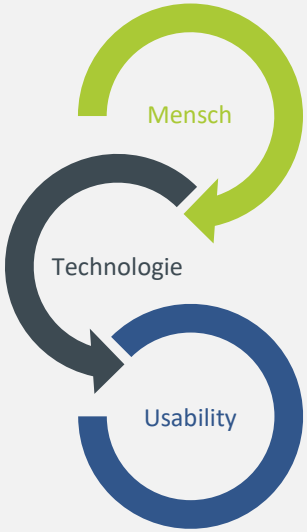
- OT Devices (u. a. Drucker, medizinische Geräte, embedded OS)
  - Betriebssysteme meist veraltet / proprietär
  - Patches nicht vorgesehen / unterstützt
  - Proprietärer Kommunikationsstack
  - Sicherheit nicht im Fokus der Entwicklung



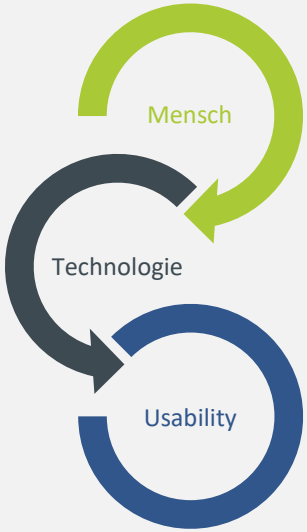
Herausforderungen

- Mobile Geräte
  - Verlust
  - Kompromittierung
  - Datenschutz, Datenabfluss
  - Lifecycle / Updates
  - Konfigurationsmanagement

SWS „menschliche Firewall“



Bedrohungen von Innen



90+% of today’s data breaches are caused by human error (Vericon Data Breach Report, Cyber Security Intelligence Index)

Lösungsansätze

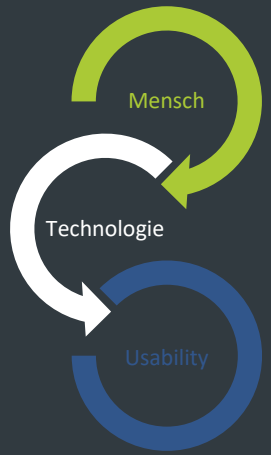
Der menschliche Faktor

- Awareness
  - Sensibilisierung der Mitarbeiter
  - Wachsamkeit bei Internet und E-Mail
  - Informationsschutz
  - Umgang mit „Social Engineering“
  - Umgang mit „Social Media“
  - Umgang mit Geräten und Medien
  - Gesunder Menschenverstand

Der Mensch als Sicherheitsrisiko?

„Technik vs. Mensch:
Was nutzt ein hoher technischer Standard
Wenn die Schwachstelle Mensch umgangen wird?”

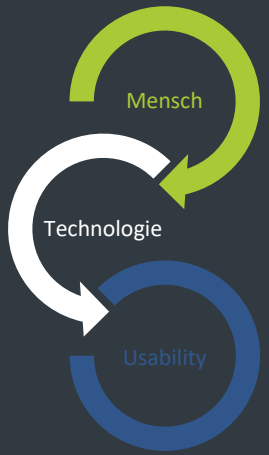
Quelle: 15. Deutscher IT-Sicherheitskongress, Andreas Rieb, Universität der Bundeswehr München



Der Mensch als Sicherheitsrisiko?

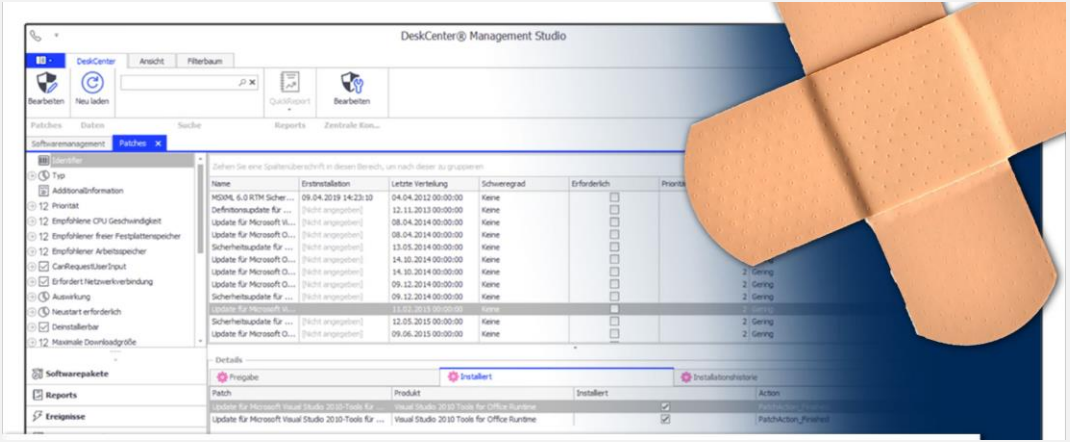
Das wird auch in Zukunft so bleiben – den Fehler werden immer gemacht und das ist weiterhin menschlich

> Deshalb Technologie + menschlicher Faktor



Lösungsansätze

- Ganzheitliches Asset-Management
  - IT
  - OT
  - Mobile
  - Infrastruktur
- Ganzheitliches Patch-Management
  - IT
  - OT
  - Mobile
  - Infrastruktur
  - alle Apps
  - Firmware / BIOS



Lösungsansätze

Zentrales Logging aller relevanten Komponenten, z.B.

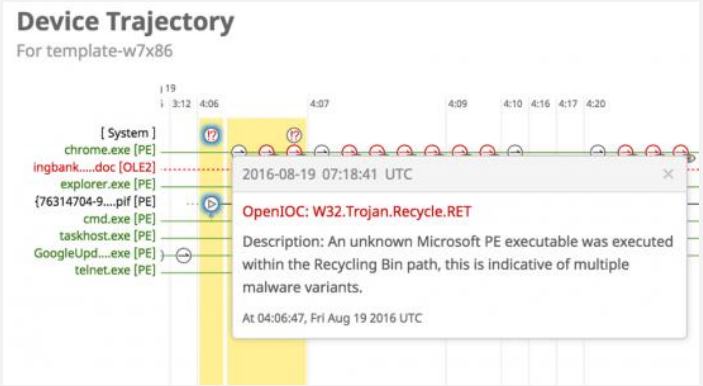
- Benutzerkonten
- Anwendungen
- Infrastruktur
- Sicherheitskomponenten

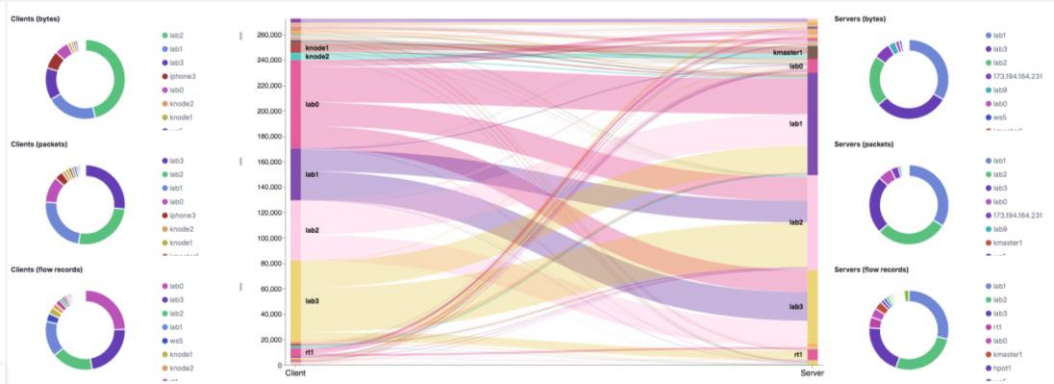
Multifaktor Authentifizierung

- Kombination von „Wissen“ und „Besitz“
- Schutz vor Identitätsdiebstahl
- Mindestens für privilegierte Konten + Remote Zugriff

Lösungsansätze

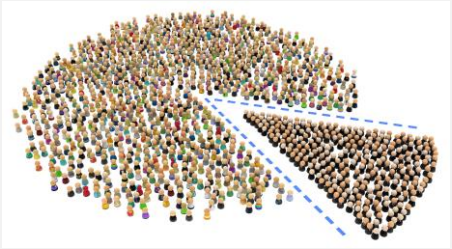
- Endpunkt Transparenz
  - Was passiert auf den Endpunkten?
  - Wohin wird kommuniziert?
  - Wurden Daten kopiert?
  - Sind Daten abgeflossen?
- Kommunikations-Transparenz
  - Netzwerk-Verkehrsbeziehungen
  - Netzwerk-Protokolle
  - Dauer, Volumen, Häufigkeit





Lösungsansätze

- Netzsegmentierung physikalisch und/oder logisch
  - OT priorisieren
- Absicherung aller Netzwerkanschlusspunkte
  - Drahtlose Protokolle berücksichtigen
- Verschlüsselung mobiler Geräte + Datenträger
  - Berücksichtigung von ThinClients

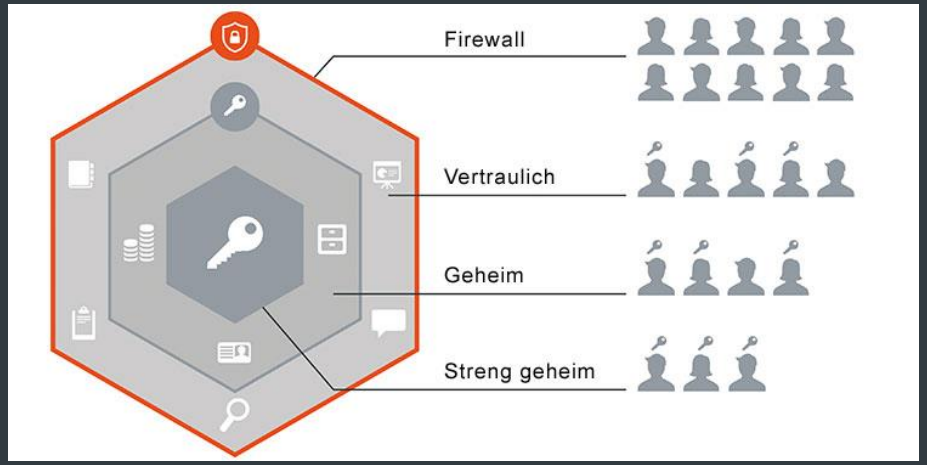


Lösungsansätze

- Transparenz in der Verwaltung von (privilegierten) Benutzerzugängen
  - Soll-Struktur
  - Dokumentierter Prozess zur Vergabe von Zugriffsrechten, Reviews
  - Überwachung von Veränderungen
  - Dokumentation der Verwendung privilegierter Konten

Lösungsansätze

- Transparenz in der Rechtestruktur des Dateisystems
  - Soll-Struktur festlegen, optional Verschlüsselungskonzept
  - Dokumentierter Prozess zur Vergabe von Zugriffsrechten, Reviews
  - Überwachung von Veränderungen
  - Überwachung der Dateizugriffe



Lösungsansätze

- E-Mail Protection
  - Link- und Attachment-Schutz
  - Sandboxing, Retrospektive Erkennung
- Endpoint Protection
  - Dateianalyse, Verhaltensanalyse, Ransomware-Schutz, Exploit Prevention
  - Geräte verschlüsseln, Start nur mit PIN/Pwd/Biometric
- Compliance Monitoring
  - Feststellung der Änderung sicherheits- und business-relevanter Settings

Lösungsansätze

- DNS absichern
  - Erste Verteidigungslinie, auch für Mobiles
  - Schutz vor Malware, Ransomware
  - Unerwünschte Kategorien unterbinden, Jugendschutz
  - Datenabfluss verhindern
  - Schutz für OT

Lösungsansätze

- Cloud Visibilität herstellen
  - Verwendete Applikationen
  - Shadow IT
  - Cloud Zugriffssteuerung
- Eigene Cloud absichern
  - Zugriffsrechte monitoren
  - Schnittstellen überwachen
  - Compliance Monitoring

Weitere Sicherheitsaspekte

- Zero Trust Modell
  - Fortwährende Prüfung von Identitäten und Geräten
- Kein Internetzugriff als Admin
  - Selbstschutz, bzw. an FW erzwingen
- Endpunkt Firewall aktivieren
  - Auch in Domain-Netzwerk
- Backup, Backup, Backup!
  - Medien trennen, Cloud Backup? Restore regelmäßig prüfen!

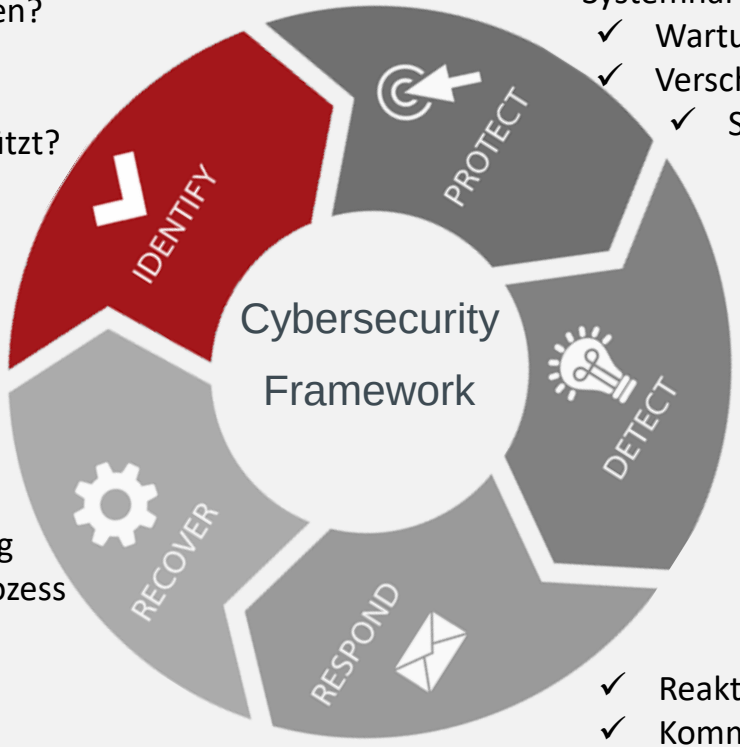
Weitere Sicherheitsaspekte

- USB Security, Windows Defender Config
- Mobile Device Management
  - Security Policy durchsetzen: PINs, Biometrics, Remote Löschung, Device Lifecycle, Patch Verfügbarkeit (auch für Apps), Auto-Update…
- Sichere Passwörter verwenden
  - Per Policy, evtl. Abgleich mit Leak-DBs oder -Diensten
  - Default-Passwörter aller verwendeten Geräte ändern
  - Passwort-Manager verwenden, evtl. Cloud-basiert, DB nicht lokal
- Mail Security im DNS umsetzen
  - SPF, DKIM, DMARC

Weitere Sicherheitsaspekte

- Notfallmanagement
  - Wiederherstellungs- und Wiederanlaufpläne für kritische Systeme
- Physische Sicherheit
  - Serverräume
  - Versorgungsleitungen: Strom, Daten…
- Synchronizität der Uhren aller Systeme
- Security ist ein Prozess, kein Zustand
  - Andauernde Prüfungen und Anpassungen notwendig

- ✓ Wo befinden sich Ihre Daten?
- ✓ Wer nutzt sie?
- ✓ Welchen Wert haben sie?
- ✓ Wie sind sie derzeit geschützt?
- ✓ Sind sie angreifbar?
- ✓ Wenn ja, woran liegt das?



- ✓ Zugriffsprozesse und Zugriffsschutz, rollenbasiertes Berechtigungskonzept
- ✓ Perimetersicherheit: Firewall-Regel-Überprüfung
- ✓ Endpoint-Sicherheit: EDR
- ✓ Systemhärtung (basierend auf Best Practice)
- ✓ Wartung (Change & Patch Management)
- ✓ Verschlüsselung, Datensicherheit
- ✓ Sensibilisierung und Schulung

- ✓ Auffinden sicherheitsrelevanter Ereignisse (SIEM, Log-Daten)

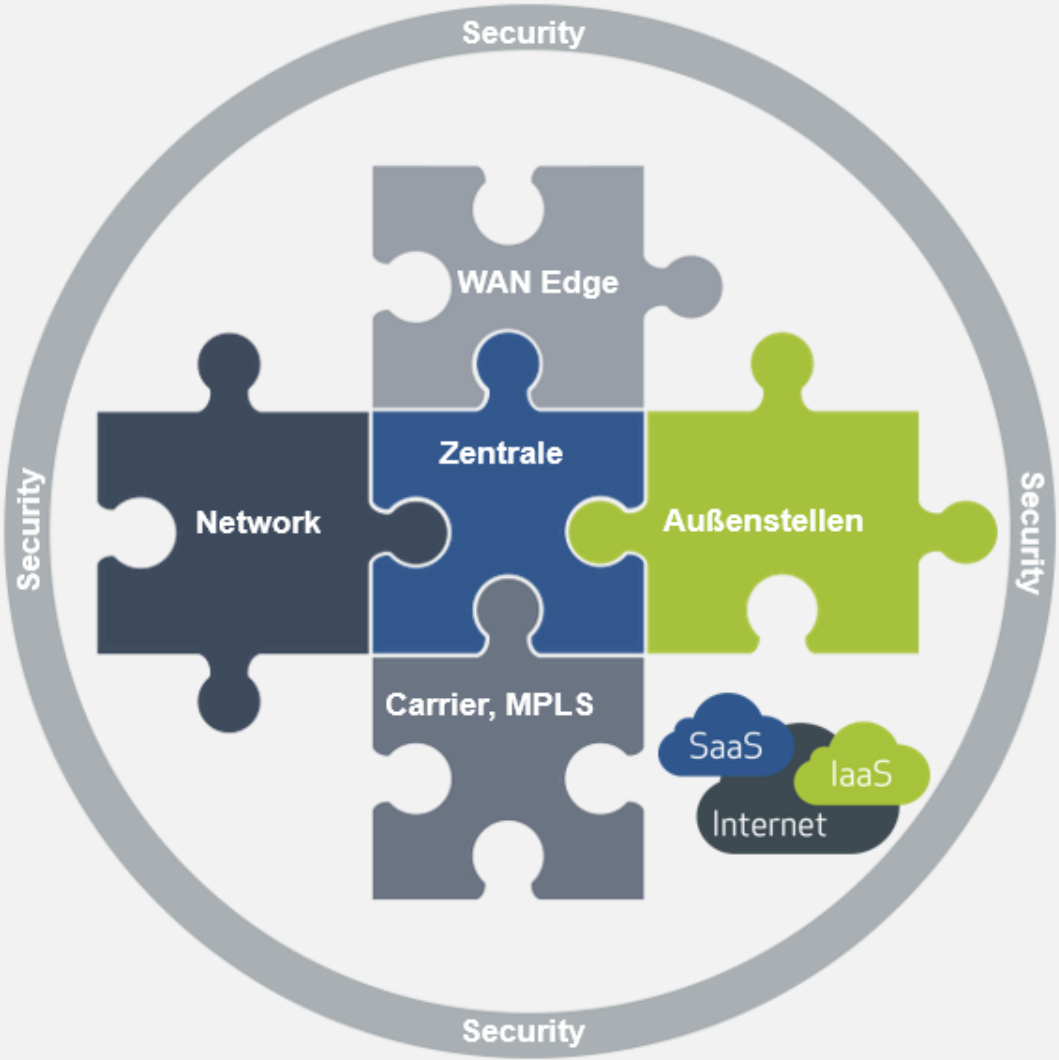
- ✓ Zurücksetzen
- ✓ Wiederherstellung
- ✓ Verbesserungsprozess

- ✓ Reaktion
- ✓ Kommunikation & Koordination
- ✓ Analyse der Attacke & Mitigation

Quelle: MITRE ATT&CK-Framework

Kreative Vorstellungskraft

Fortschritt



Fazit:

- Es gibt keine 100%ige Sicherheit

~~S(f)=(a+b – c(d))*e~~

- $\Delta S = \sum$ Behavior + Technologie + Strategie + Compliance

- IT Security und Informationssicherheit ist ein Prozess, der sich den ständigen Veränderungen anpassen muss

- IT Security ist Chefsache – D.h. Die Geschäftsleitung muss voll hinter einer IT Security und Informations-Sicherheits-Strategie stehen

SWS
COMPUTERSYSTEME
Member of ACP Group

SWS COMPUTERSYSTEME
Member of ACP Group

Vielen Dank für Ihre Aufmerksamkeit.

Fragen?

IT for innovators.
Member of ACP Group