Slide 1

GVO

Gewerbeverband Oberzentrum e.V.

# GVO25
# Sicherheit in der Digitalisierung

COMPETITION
IT-MANAGEMENT

---

COMPETITION
IT-MANAGEMENT

## Profil

Gründung: 2003 (GmbH seit 2013)

Mitarbeiterzahl: 6

Branche: ITK Systemhaus

Leistungen: IT-Service, Beratung, Value Added Reseller

Schwerpunkte: Managed Service, IT-Sicherheit, Infrastrukturprojekte

Slide 2

COMPETITION
IT-MANAGEMENT

# Big Brother is watching you.

Zitat: George Orwell 1903-1950



- Schon 1949 wusste George Orwell was uns heute beschäftigt
- Er dachte aber der Staat sei das Überwachungsorgan
- Heute sind es private Organsationen, Kriminelle und auch Staaten (Bsp. China)

Um hier einen Überblick zu bekommen klären wir heute einige Technologien, zeigen Risiken auf und erklären Maßnahmen

Slide 3

COMPETITION IT-MANAGEMENT

# Ablauf

- EU-DSGVO / GDPR
- Digitalisierung, Industrie 4.0, IoT, Blockchain
- Risiken und Maßnahmen
- Szenarien

Slide 4

DICLAIMER: Dies ist keine Rechtsberatung und wir dürfen hier keine verbindlichen Auskünfte erteilen!

- DSGVO = Datenschutzgrundverordnung
- GDPR = General Data Protection Regulation
- Personenbezogenen Daten:
    - Namen, Fotos, Telefonnummern, Adresse, Kundennummer, E-Mail-Adresse, IP-Adresse, etc.
    - Von: Personal, Kunden, Lieferanten, Partnern, etc.
- Voraussetzungen:
    - Einwilligung
    - Vertragserfüllung
    - Rechtliche Verpflichtungen
    - Berechtigtes Interesse des Verantwortlichen

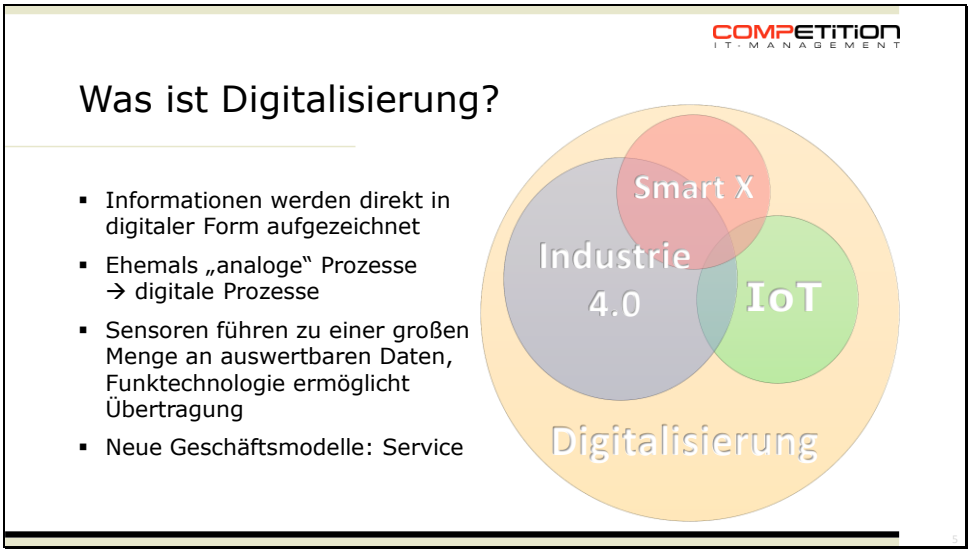
Wichtigste Punkte:

- Datenschutzbeauftragter ab 10 Mitarbeitern
- Internetauftritt überprüfen
- Auftragsverarbeitung prüfen und umsetzen
- Vorgehen im Falle einer Datenpanne, Meldepflicht
- Betroffenenrechte
- Technisch-Organisatorische Maßnahmen
- Ggf. Verzeichnis von Verarbeitungstätigkeiten

Gefahr bei Nichtumsetzung:

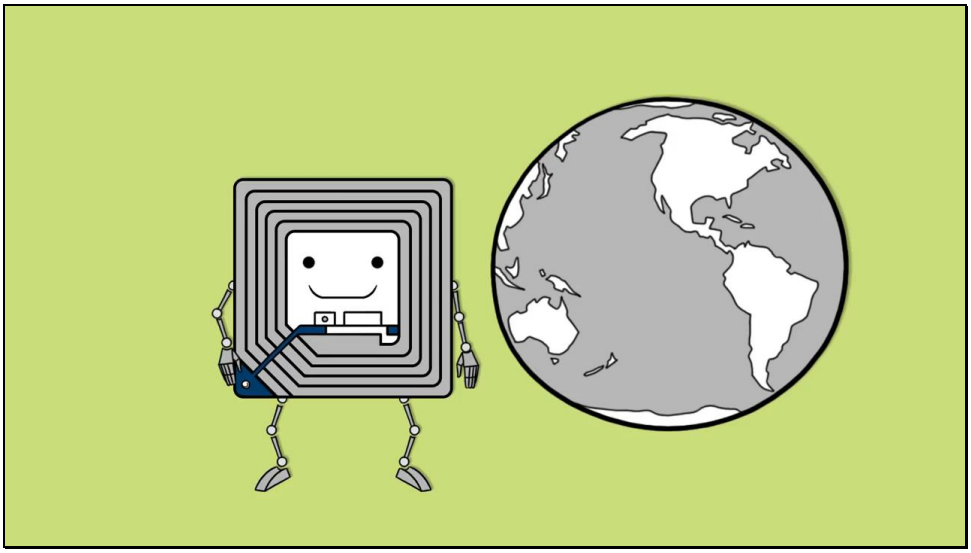
- Strafmaß wurde massiv erhöht (20 Mio, 4% globaler Vorjahresumsatz)
- Bei Vorfall: Reputationsverlust bei Kunden/Nutzern/Lieferanten

Slide 5




- Deep Learning/ Machine Learning
- AI – Artificial Intelligence = Künstliche Intelligenz

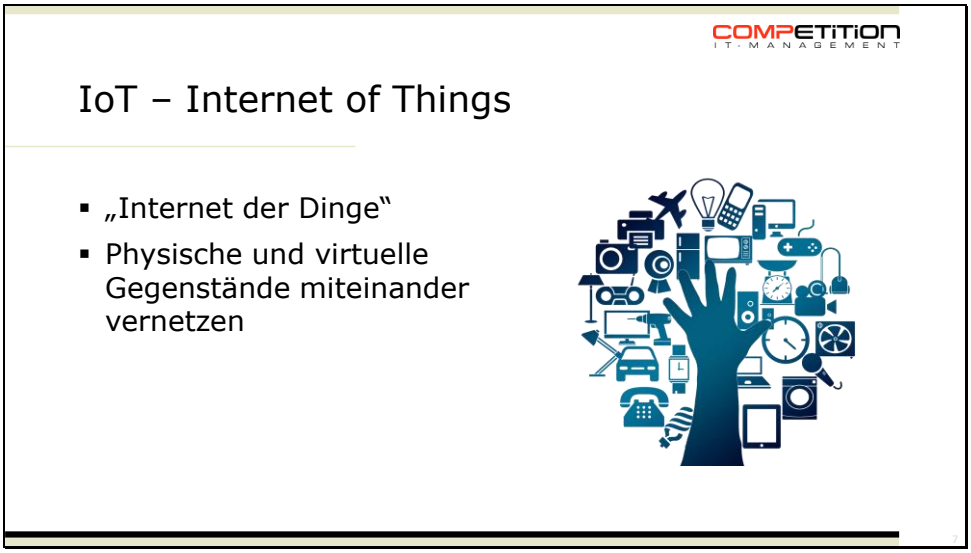
Slide 6



https://www.youtube.com/watch?v=SjypoaixIQg

- Industrielle Revolution: mechanische Produktionsanlagen
- Industrielle Revolution: arbeitsteilige Massenproduktion
- Industrielle Revolution: Einsatz Elektronik und IT → Automatisierung

Slide 7




- Basis für Digitalisierung
- Auch Dinge im Privathaushalt → Kühlschrank, Lichtschalter, etc.
- Mit Netzwerkschnittstellen ausgestattet
- CPS = Cyberphysische Systeme
  Verbund netzwerk- und softwaretechnischer Komponenten mit mechanischen und elektr. Teilen  miteinander vernetzt
  z.B.: Fahrerassistenzsysteme, Verkehrssteuerung, Energieversorgungsmanagementsysteme, etc.

Slide 8

Sendung mit der Maus – Bitcoin
https://www.youtube.com/watch?v=8zeg_R-PMAw

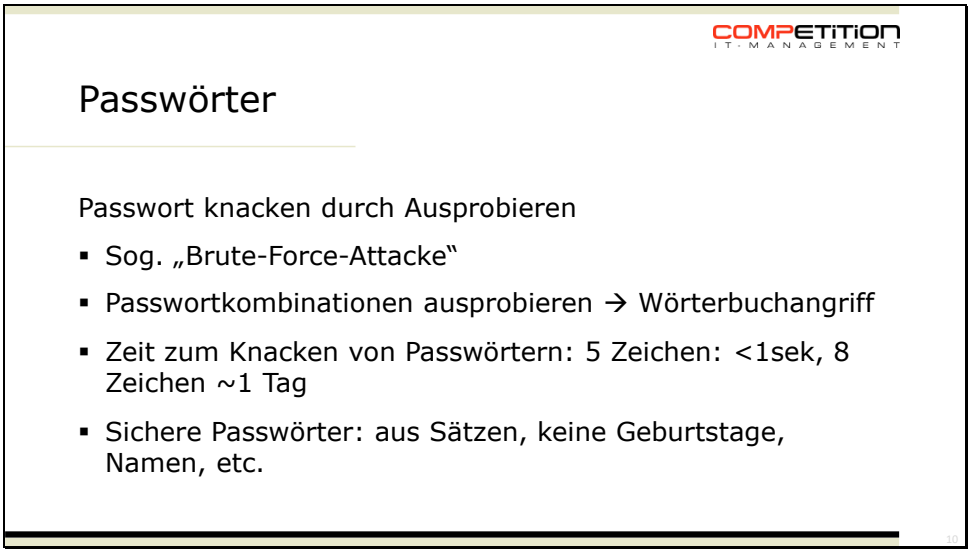
- Verteilte, verschlüsselte, selbstprüfende Datenbank
- Nicht auf den Finanzmarkt beschränkt
- Alle verteilten, verkettbaren Ereignisse abbildbar
- Beispiel: Bitcoin

Slide 9

Risiken und Maßnahmen

Zur:
- Datenübermittlung
- Datenhaltung
- Datenzugriffssicherung

Slide 10

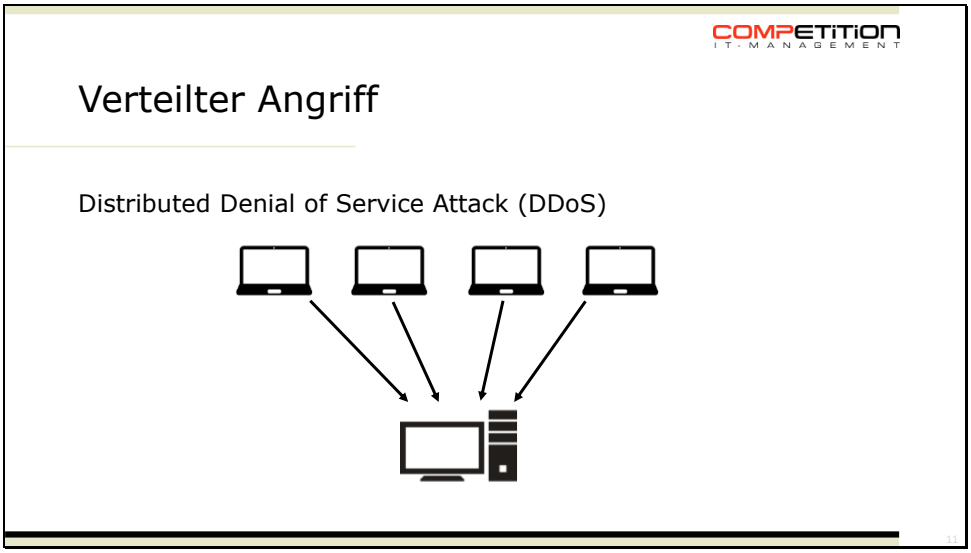



- Brute Force = Rohe Gewalt
- Jede mögliche Kombination wird ausprobiert
- Anzahl möglicher Kombinationen = (Anzahl möglicher Zeichen)$^{\text{Länge des Passworts}}$
- Hinweis:
  Benutzen Sie keine angeblichen Passwort-Tester im Internet. Dies kann eine Methode von Kriminellen sein, um an Passwörter zu kommen.

- https://www.sicherheitstest.bsi.de
- https://haveibeenpwned.com/

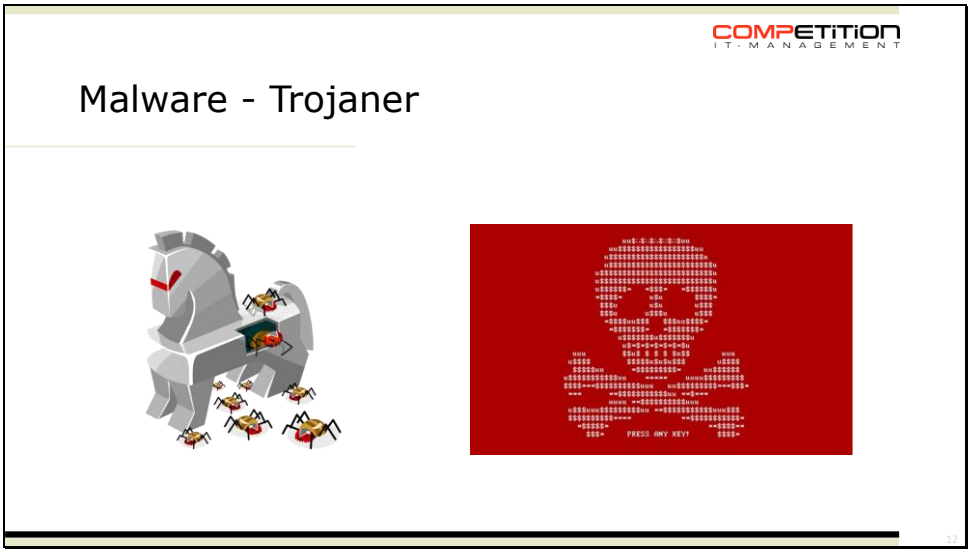
p

Slide 11



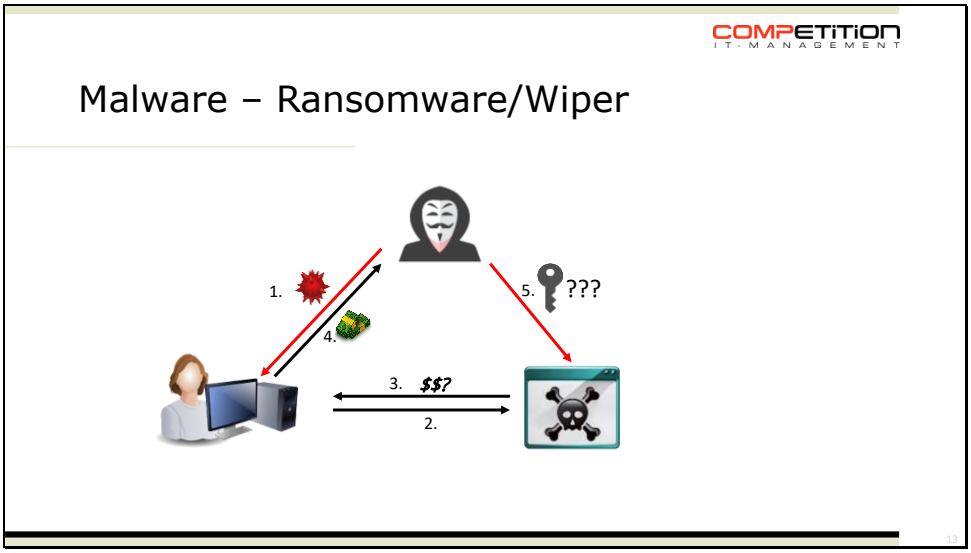

- dt.: Dienstverweigerung → System ist nicht mehr funktionsfähig wegen Überlastung
- Viele „kompromittierte“ PCs (Botnetz) schicken Anfragen an Opfer-System  kann Menge an Anfragen nicht bearbeiten

Slide 12



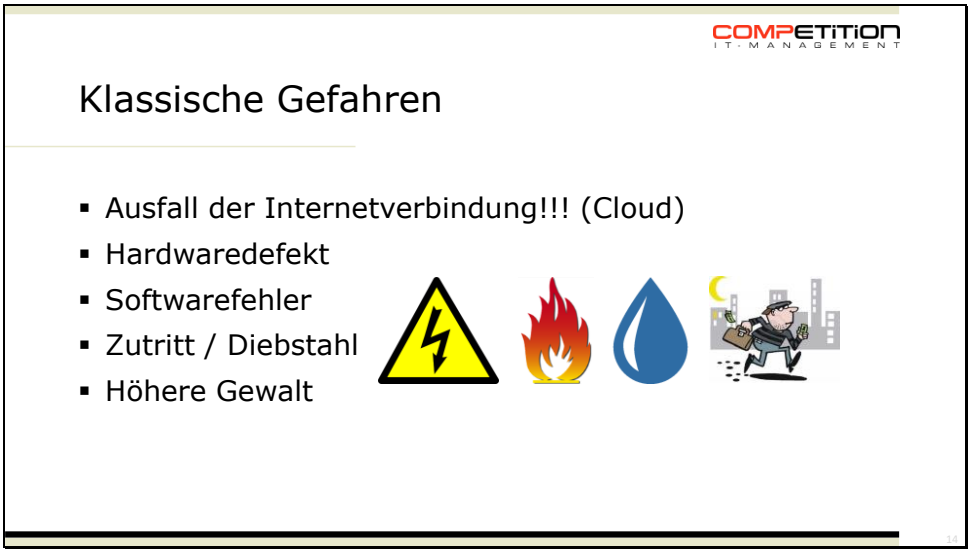

- Trojaner: geben sich als „nützliches/harmloses“ Programm aus
- Viren/Würmer: verbreiten sich selbstständig
- Scareware = darauf angelegt, den Benutzer zu verunsichern und ihn dazu zu verleiten, schädliche Software zu installieren oder für ein unnützes Produkt zu bezahlen
- Spyware = forschen den Computer und das Nutzerverhalten aus und senden die Daten an den Hersteller
- Adware = zeigt ungewünschte Werbung an

Slide 13



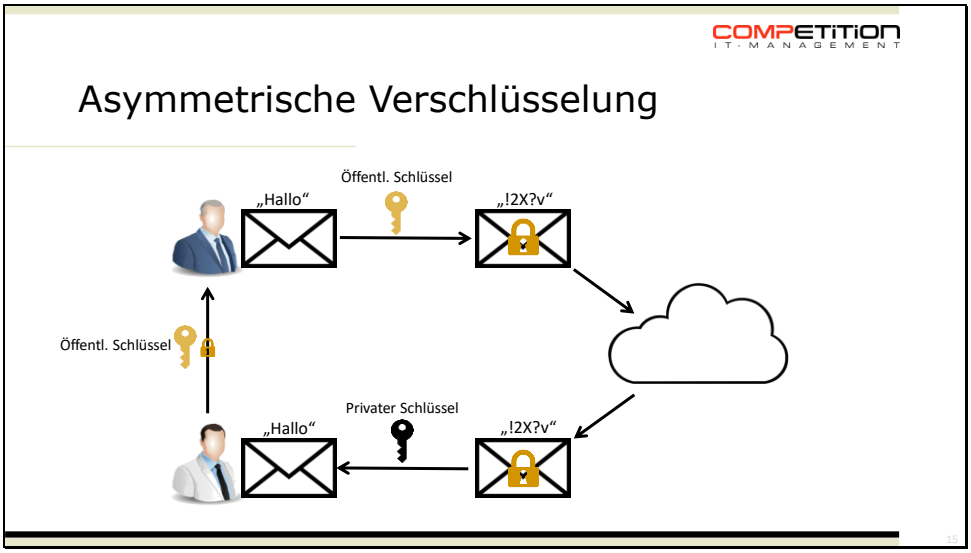

- Schadprogramm gelangt, z.B. durch gefälschte E-Mail, auf System
- Beim Ausführen wird System (komplett) verschlüsselt
- Aufforderung Geld auf unbekanntes Konto einzuzahlen, um Daten zu retten
- Opfer fühlt sich genötigt dem Täter das Geld zu überweisen
- Täter verspricht, den Entschlüsselungs-Key herauszugeben → Erfolg dessen sehr fraglich
- Sonderform Wiper: z.B. NotPetya – Daten werden nur zum Schein verschlüsselt ⍰ Komplettverlust

Slide 14



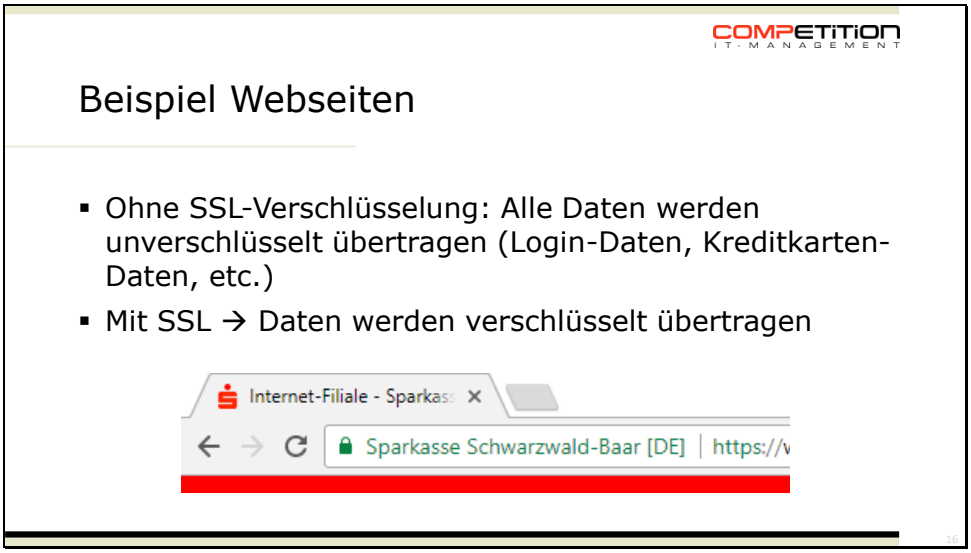

- Ausfall der Internetleitung, Störung der Internetleitung → Cloudlösungen dann nicht mehr erreichbar
- Je nach Reaktionszeit kann es bei Hardware-Ausfällen zu unterschiedlich langen Betriebsausfällen kommen
- Maßnahmen:
    - Fallback-Leitung
    - Hardware-Redundanz
    - Backup/Archivierung
    - Zutrittskontrolle/Zugangskontrolle

Slide 15



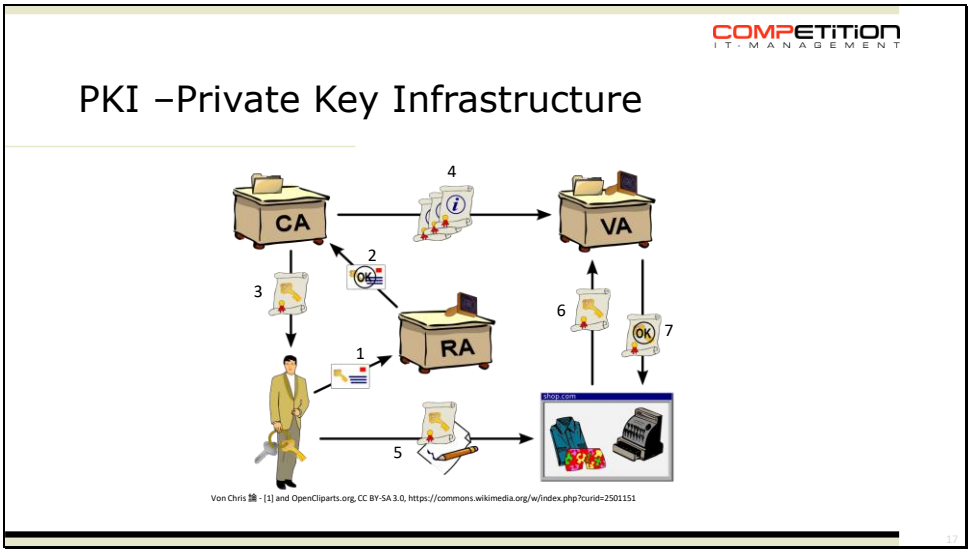

- privater Schlüssel → nur Nutzer persönlich
- öffentlicher Schlüssel → für alle einsehbar
- Analogie: Briefkasten mit Schloss  jeder der Adresse (öffentlicher Schlüssel) kann Nachrichten einwerfen, aber nur Besitzer des privaten Schlüssels kann Briefe rausholen
- Ende-zu-Ende-Verschlüsselung: Nachricht ist auf dem gesamten Weg von Absender zu Empfänger verschlüsselt und nur mit privatem Schlüssel von Empfänger zu entschlüsseln

Slide 16



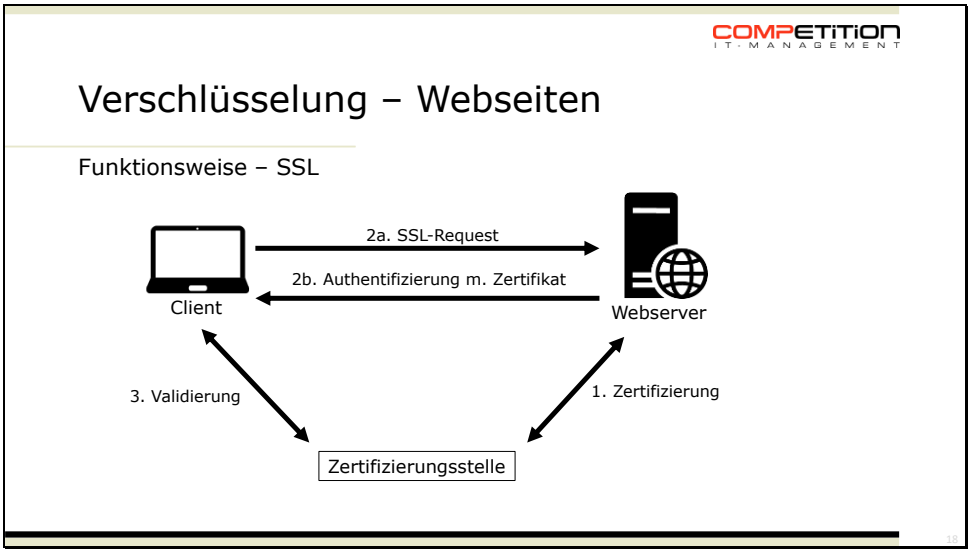

- Webseitenbetreiber muss Zertifikat beantragen → von Zertifizierungsstelle ausgestellt
- Zertifizierungsstelle überprüft Richtigkeit der Daten
- Aktuell: Google Chrome warnt ab Juli 2018 vor Webseiten ohne https in Adressleiste erscheint „Nicht sicher“
- Überprüfen Sie Ihre Webseite!

Slide 17

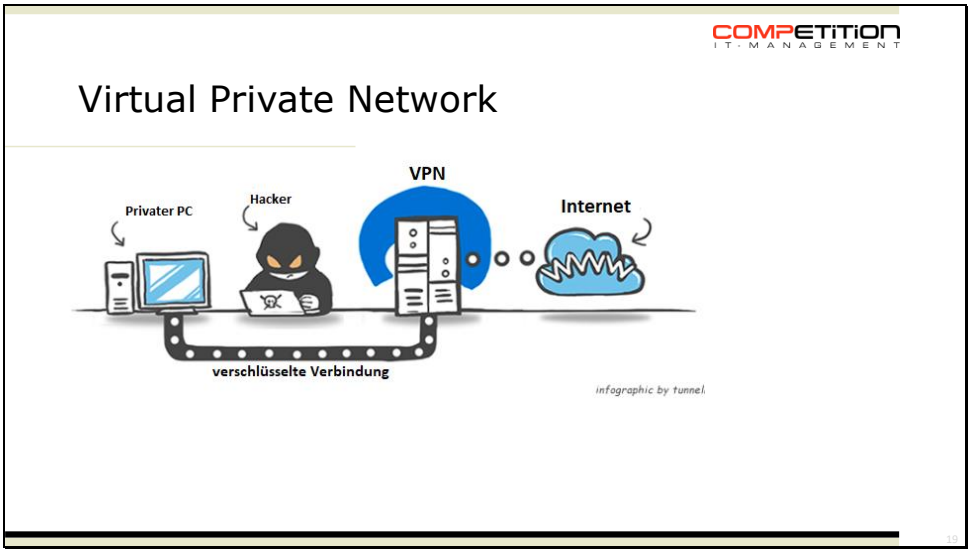



- Nutzer beantragt bei RA (Registration Authority) Zertifikat (1)
- RA prüft Angaben und genehmigt ggf. Antrag, gibt Antrag an CA (Certification Authority) weiter (2)
- CA signiert Zertifikat und stellt Zertifikat an Nutzer aus (3), informiert VA (Validation Authority) über Gültikeit und Nutzer des Zertifikats (4)
- Nutzer zeigt Zertifikat bei Anfragendem vor (5)
- Anfragender lässt Zertifikat von VA validieren (6,7)

Slide 18


COMPETITION
IT-MANAGEMENT
Verschlüsselung – Webseiten
Funktionsweise – SSL
2a. SSL-Request
2b. Authentifizierung m. Zertifikat
Client
Webserver
3. Validierung
1. Zertifizierung
Zertifizierungsstelle

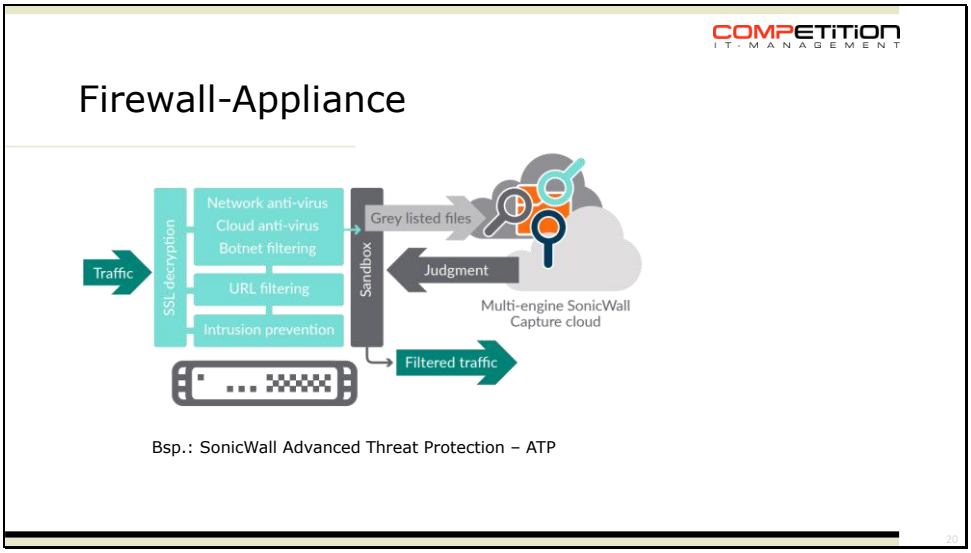
Slide 19




Einsatzzwecke:
- Anbindung von Außenstandorten
- Home-Arbeitsplätze / Reisendes Personal
- Einzelgeräte z.B. Smart Meter, Telefoniegeräte, Mobilgeräte im Außeneinsatz

Wichtig: nicht nur klassischer Ansatz von manueller Einwahl, auch in Geräten hinterlegte Schlüssel/automatischer Verbindungsaufbau für IoT interessant (z.B. durch fremde Industrienetze “durchtunneln”)
Hinweis Firewall: Wenn Verbindungen nur von außen nach Innen geprüft werden kann hier ein Sicherheitsproblem existieren

Slide 20




Risiko:
- Geräte stehen ungeschützt im Internet
- Alle Dienste auf den Geräten sind frei verfügbar

Lösung1 (Security by Design):
- So wenige Dienste wie möglich auf den Geräten
- Dienste so sicher wie möglich umsetzen

Lösung2 – auch ergänzend -> Abschottung:
- Firewalls: Welche Art von Verkehr darf Firewall passieren?
- Capture-ATP: verschlüsselter Verkehr wird entschlüsselt → übertragene Dateien werden in Sandbox überprüft: wenn Risiko besteht → gelöscht, bzw. in Quarantäne verschoben
- Z.B.: Geräte aus dem internen Netz dürfen Webseiten aus dem Internet aufrufen, Geräte aus dem Internet dürfen nicht auf internes Netz zugreifen
- Intrusion Prevention/Detection: Datenverkehr wird auf bestimmte Muster untersucht ⍰ Verdächtiger Verkehr wird aufgezeichnet/verhindert

Slide 21

- Meltdown & Spectre: Durch Architektur/Funktionsweise können Prozesse Speicherbereiche auslesen → z.B. personenbezogene Daten, Passwörter, Kreditkartendaten, etc.
- „schnell“ veröffentlichte Updates können auch Fehlfunktionen nach sich ziehen ⍰ Updatemanagement
- Schwachstellen in Hard- und Software können für Angriffe ausgenutzt werden
- Bie IoT Geräten, großen Anlagen (Engerie/Industrie) oder auch in Sicherheitsbereichen (Medizintechnik, Fahrzeugelektronik) können mitunter lange dauern. Sind solange aber ausnutzbar = Gefahr
- Geräte können dann unter Umständen in Botnetzen eingesetzt werden
- Ältere Geräte oder billige Hardware/Noname/selbstgebastelte Hardware kann hier ein großer Nachteil sein

Slide 22

COMPETITION IT-MANAGEMENT

## Fazit: Technische Maßnahmen

- Aktuelle Hard-/Software Technologien:
  - geschützte Anlagen (USV, Zugangskontrolle…)
  - ATP Firewall-Appliances
  - Virenscanner mit ATP, AI Funktionalitäten
  - Angriffsgeschützte Datensicherung/-archivierung
- Datenübertragung/-speicherung
  - Verschlüsselung
  - Mehrfaktor-Authentifizierung
  - Moderne Redundanzsysteme (z.B. Hybrid-Cloud)
  - Schatten-IT regulieren (eigene innovative Strukturen schaffen)

22

Schatten-IT: Beispiel Entwicklungsfirma bei der Abteilung selbst einen Amazon Serivce gebucht hatte und geheime Daten in öffentliche Clouds schickte

Slide 23

COMPETITION IT-MANAGEMENT

# Organisatorische Sicherheit

Slide 24

COMPETITION IT-MANAGEMENT

# Organisatorische Risiken

- Steigender Zeitdruck → Nichteinhalten von Prozessen
- Fehlende Schulungen
- Mangelndes Bewusstsein für IT-Sicherheit
- Datenschutz

- Unter Zeitdruck werden eher Sicherheitsrichtlinien/Prozesse nicht eingehalten anstatt Produktionsverzögerungen oder Einbußen bei verkaufter Stückzahl in Kauf zu nehmen
- Einstellung: „Unsere Systeme sind sicher. Wir haben ja Firewall/Antivirus/etc. Also kann uns nichts passieren.“

Slide 25

COMPETITION IT-MANAGEMENT

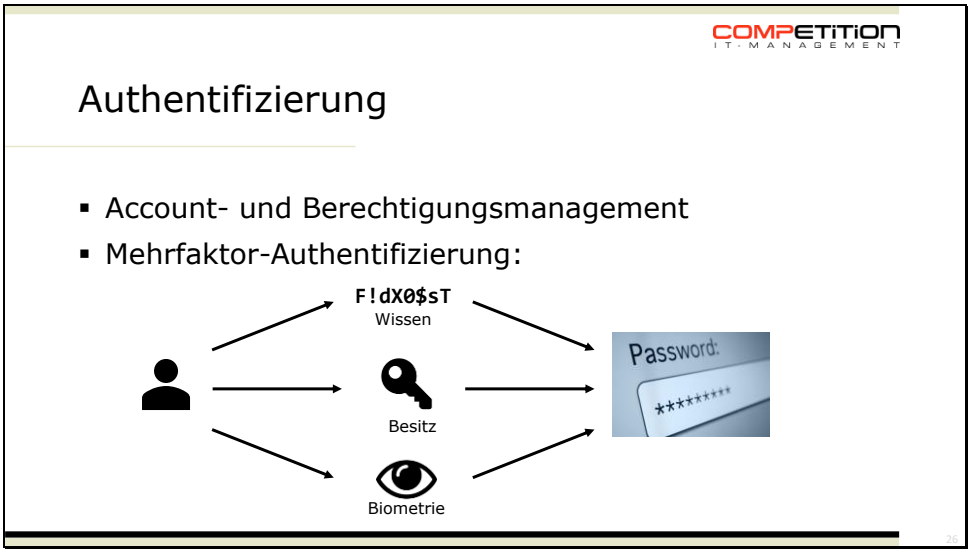
# Social Engineering

- Ausnutzen menschlicher Verhaltensweisen
- Ausspionieren von persönlichem/geschäftlichem Umfeld
- Ziel: Herausgabe v. vertraulichen Informationen, Kauf eines Produktes, Zahlungen
- Bsp.: Enkeltrick, Phishing, angebl. Techniker

27

- Ausnutzen menschlicher Verhaltensweisen
- Ausspionieren von persönlichem/geschäftlichem Umfeld
- Ziel: Herausgabe v. vertraulichen Informationen, Kauf eines Produktes, Zahlungen
- Bsp.: Enkeltrick, Phishing, angebl. Techniker
- Informationen auf Sozialen Medien können von Angreifern genutzt werden → Freundeslisten, Arbeitgeber, etc.

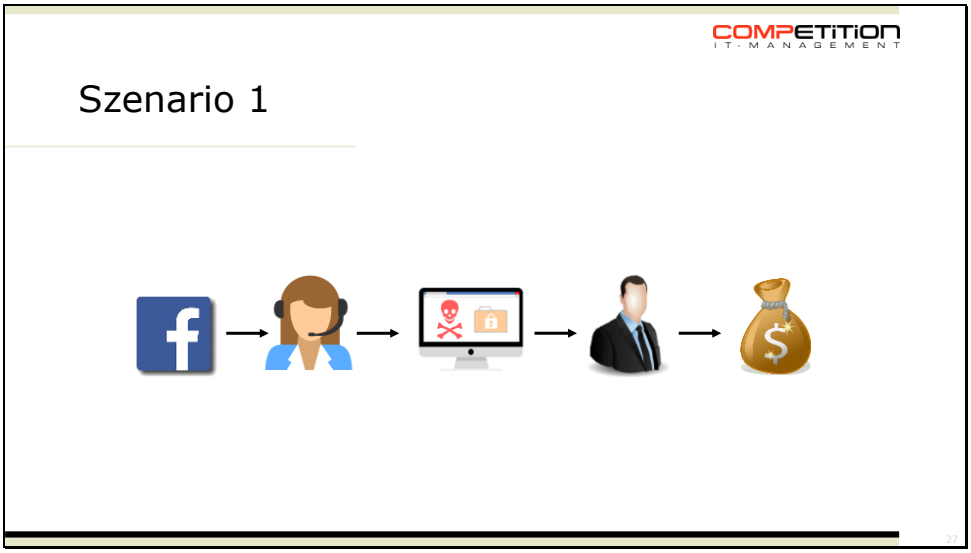
Slide 26




- Wissen: Passwort, PIN, Sicherheitsfrage
- Besitz: Schlüssel, Transponder, Zertifikat, Handy (Sicherheitscode per SMS)
- Biometrie: Fingerabdruck, Gesichtserkennung, Iriserkennung, Stimme, Tippverhalten

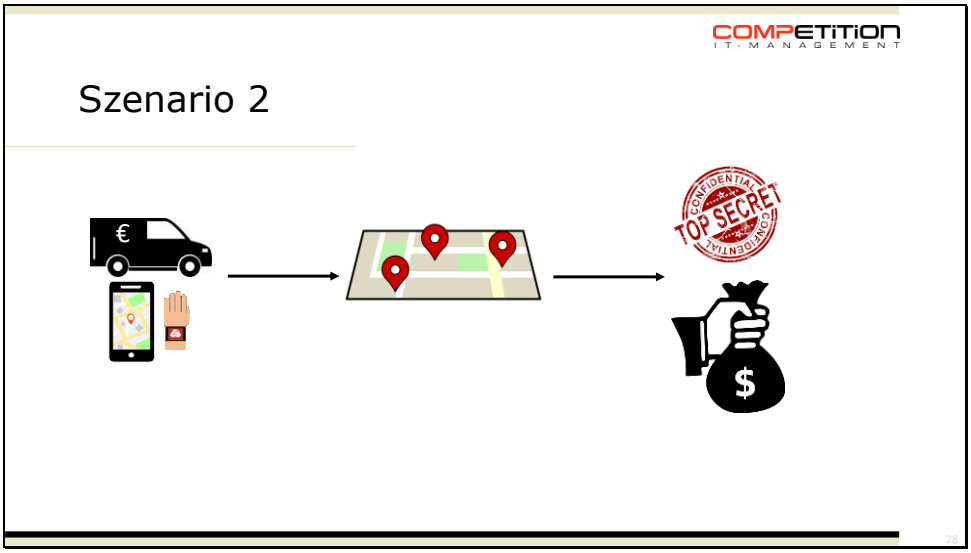
Prozesse:
- Besucheranmeldung
- Vernichtung von Druckerzeugnissen
- Schulungen
- Allg. Geschäftsprozesse (Zahlungsanweisungen per E-Mail)

Slide 27




- Mitarbeiter hat Facebook-Profil mit Firma und Telefonnummer
- Als Microsoft-Mitarbeiter getarnter Angreifer gibt vor wichtiges Update einspielen zu müssen
  → aufgrund von Unkenntnis folgt Mitarbeiter den Anweisungen ⍰ lädt Spyware herunter
- Angreifer erhält Einblicke in internen E-Mail-Verkehr ⍰ kann interne Struktur nachvollziehen (Wie spricht man sich an, Email-Signatur, etc.)
- Angreifer gibt sich als Geschäftsführer/CEO aus – CxO Fraud
- Anweisung an zahlungsbefugte Mitarbeiter ⍰ Hinweis auf Vertraulichkeit und Zeitdruck
- Umgehen von vorgegebenen Prozessen
- Rückfragen nur per E-Mail -> werden auch beantwortet
- Mitarbeiter tätigt Überweisung, meist Auslandsüberweisung, die nicht rückgängig gemacht werden kann

Slide 28




- Geldtransporte (wichtige Waren/Produktlieferungen) können durch verbaute Geräte (von Werksseiten) verfolgt werden
- Ebenso (private) Mobilgeräte/Fitnesstracker von Mitarbeitern/Fahrern
- Auf diesem Wege lassen sich Heat Maps erstellen → Analyse von Transportwegen/Mitarbeiterbewegungen
- Gibt u.U. Auskunft über Assets, Unternehmenskooperationen, etc.
- Diebstahl von Geschäftsgeheimnissen und/oder Geld/Technik/Produkten

Slide 29

COMPETITION
IT-MANAGEMENT

## Big Data

- Große Datenmengen
- Werden automatisiert verarbeitet
- Z.B.: Zahlungsverkehr, Einkaufsverhalten, Standortdaten, etc.
- Von PCs, Smartphones, Fahrzeugen, Wearables, etc.

29

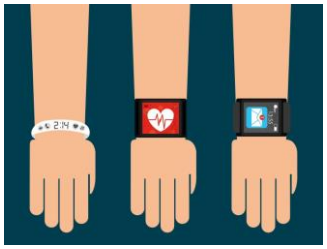
- ALLES hinterlässt Spuren im Internet
- Sowohl geschäftlich, als auch privat
- „Die Gedanken sind nicht mehr frei“ → Filterblase
- Regulierung notwendig  DSGVO

Slide 30

COMPETITION IT-MANAGEMENT

# Wearables

- Smart Watch, Fitness-Armbänder, Google Glasses
- Übertragen permanent Daten
- Beispiel: US-Militärbasen bekannt geworden durch Fitness Tracker Daten



Slide 31

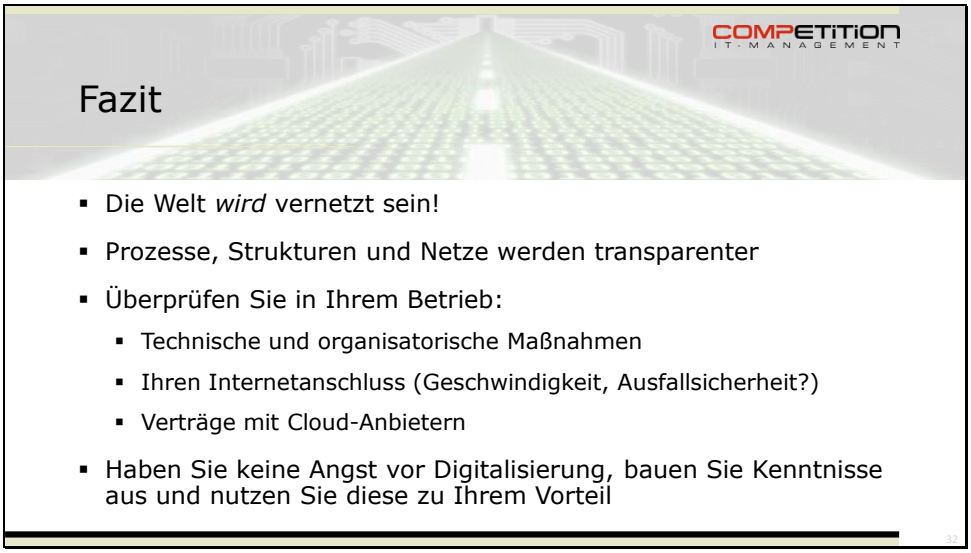
# Anlaufstellen – Digitalisierung, IT-Sicherheit

- Gewerbeverband Oberzentrum
- Innovationsnetzwerk Schwarzwald-Baar-Heuberg e.V.
- Digital Hub St. Georgen i.G.
- Cyberwehr Baden-Württemberg
- BSI – Bundesamt für Sicherheit in der Informationstechnik
- BWcon SIG Blockchain Stuttgart
- competition it-management GmbH



http://gvo-vs.de/
https://www.innovationsnetzwerk-sbh.de/
https://www.wirtschaft-digital-bw.de/massnahmen/digital-hubs/
https://www.bsi.bund.de
http://www.bwcon.de/fuer-das-netzwerk/special-interest-groups/sig-blockchain.html
https://competition-it.de/

Slide 32




- Man kommt um Digitalisierung nicht herum
- Nutzen Sie die Potenziale, bauen Sie Ihre Kenntisse aus, auch um den Gefahren zu begegnen
- Nutzen Sie diese Kenntnisse gerade auch über die Sicherheit zu Ihrem Wettbewerbsvorteil
- Schaffen Sie neue Verantwortlichkeiten im Unternehmen für IT-Sicherheit (CISO), nutzen Sie externes Know-How
- Analysieren Sie und bewerten Sie die Risiken in Ihrem Unternehmen und erstellen Sie eine Folgenabschätzung

Slide 33

COMPETITION IT-MANAGEMENT

## Danke! Fragen?

# Sicherheit ist eine Illusion.

Zitat: unbekannter Autor



Bedeuetet aber nicht, dass man nichts dafür machen sollte!

Slide 34

GVO

Gewerbeverband Oberzentrum e.V.

# Einladung zum Imbiss und Dialog

competition it-management gmbh
Peterzeller Str. 8
78048 Villingen-Schwenningen
+49 7721 681171-0
info@competition-it.de

COMPETITION
IT-MANAGEMENT