

TeleTrust-Konferenz 2019

Bundesverband IT-Sicherheit e.V. (TeleTrust)

Berlin, 28.11.2019

Faktor Mensch - sichere Datenkommunikation
Faktor Maschine - Datensicherung und Restore

Uwe Schwellenberg, sayTEC AG



sayTEC

IT Sicherheit: Herausforderung für Mensch & Maschine

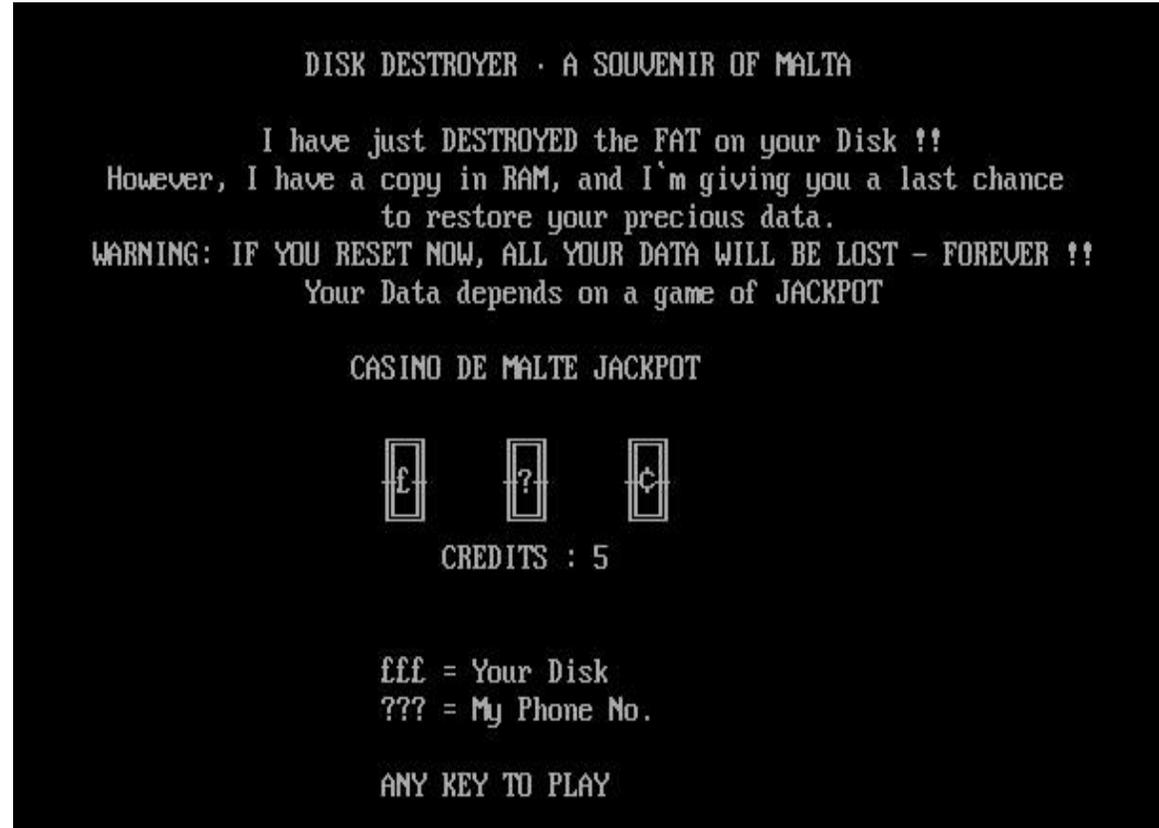
Ein  für IT-Sicherheit

30 Jahre Computervirus: Als die Rechner krank wurden

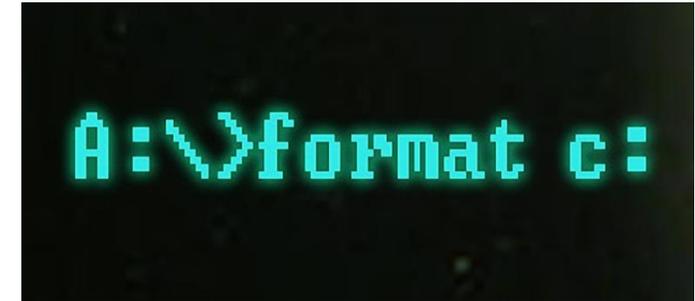
"Hab keine Angst, ich bin ein sehr netter Virus"

SPIEGEL ONLINE

Sie ließen den Bildschirm blinken oder meldeten ihre Attacken brav beim Nutzer an.



Backup gemacht? Ansonsten ist die Festplatte bald leer



IT Security Bilanz Deutschland

Cyberfälle auf Platz 2

Allianz Risiko-Barometer 2019

Cyber-Kriminalität in Deutschland:

Der Gesamtschaden ist von 55 Milliarden Euro in 2018 auf **102,9 Milliarden Euro 2019** pro Jahr gestiegen

Bitkom Studie

Bislang höchstes DSGVO-Bußgeld in Deutschland

in Höhe von **14,5 Millionen Euro** gegen die Deutsche Wohnen

70 % der Industrieunternehmen

wurden Opfer von Angriffen, Datendiebstahl oder Spionage

23 Arbeitstage IT-Downtime

pro Jahr in Deutschland durch IT-Ausfall

200 Tage bis zur Aufdeckung von Hackern im System

Über 34 Mio. Schwachstellen in AWS EC2 (Amazon), in Azure Virtual Machine (Microsoft) und in der GCP Compute Engine (Google)

Cloud Threat Risk Report

Jeder fünfte Handwerksbetrieb war bereits Opfer einer Cyberattacke!

Basis: Forsa befragte im Februar 2019 insgesamt 500 Handwerksbetriebe in Deutschland

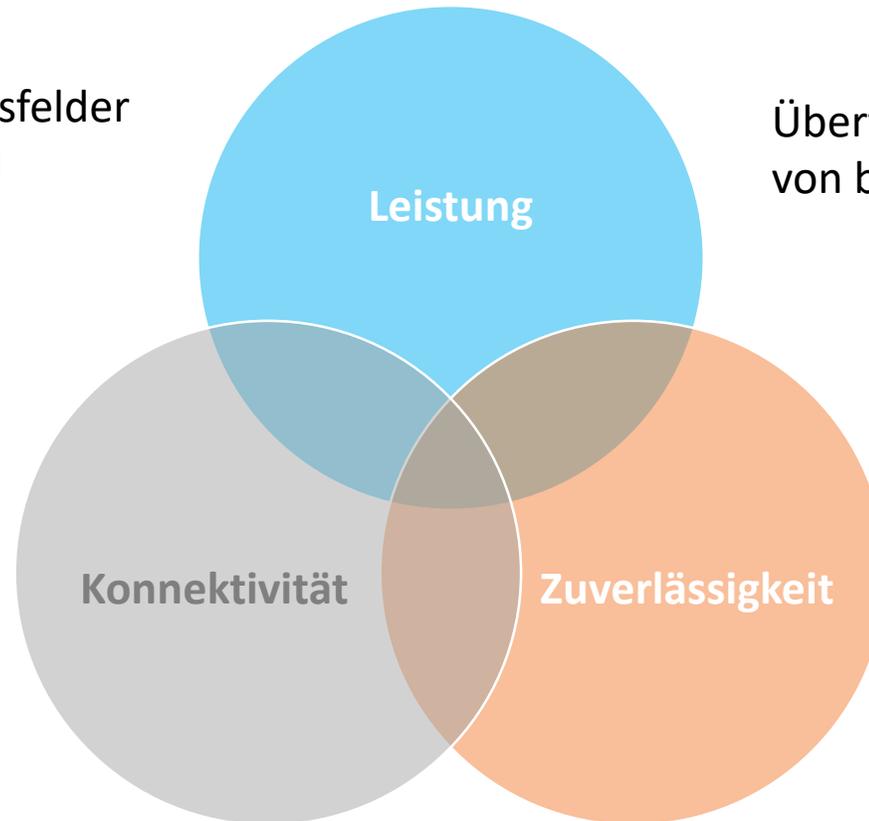
5G- ist die neue Herausforderung an IT-Sicherheit

Aber auch das Fundament für neue Entwicklungen in Wirtschaft, Gesellschaft und IT

Es entstehen neue Anwendungsfelder für Industrie, Wissenschaft und Entertainment.

Übertragungsgeschwindigkeiten von bis zu zehn Gigabit pro Sekunde

1.000.000
Geräte pro km²



höhere Geschwindigkeit und niedrigere Latenz (Verzögerung) < 1 ms Funklatenzzeit

Das 5G-Netz wird so reaktionsschnell wie das menschliche Nervensystem.

Fazit:

5G macht den Einsatz neuer Technologien erst richtig möglich

Neue Herausforderungen für Mensch und Maschine

- Schutz der Kommunikation
 - Mensch & Maschine
 - Maschine & Maschine
- Reduktion der Komplexität der IT
- Verfügbarkeit von IT-Infrastrukturen
- Handling der Datenmengen

Anforderungen an eine moderne und verlässliche IT-Infrastruktur:



Secure Access

- ✓ Schutz vor Angriffen
- ✓ Zugangssicherheit zu Netzwerken
- ✓ Hochsichere mobile + stationäre Arbeitsumgebungen
- ✓ Externe und interne Netzwerksicherheit



Datenredundanz

- ✓ Sicherung, Wiederherstellung und Auslagerung
- ✓ Erfüllung der DGSVO, Compliance, KonTraG, Basel II
- ✓ Reduzierung der IT Komplexität
- ✓ Ausfallssicherheit & Verfügbarkeit.

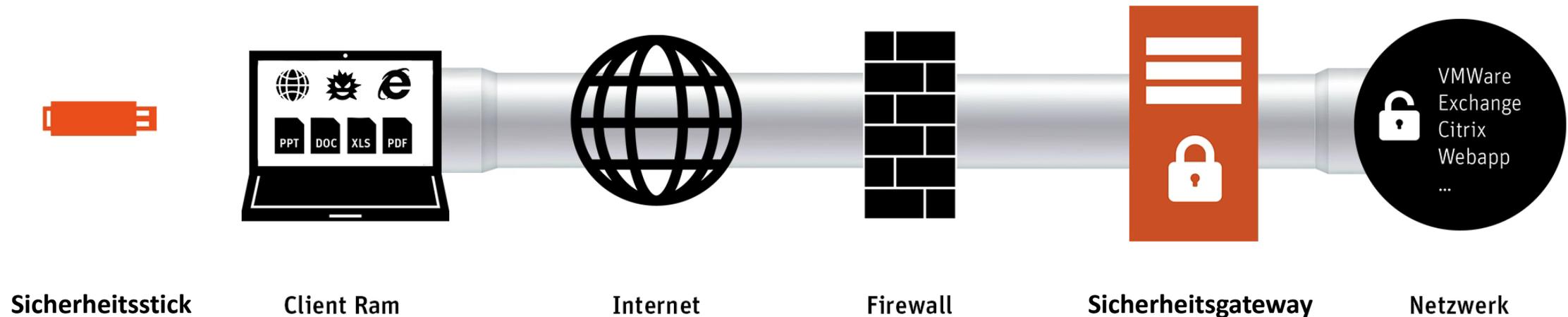


Hot Standby

- ✓ Hot Standbyplattformen für kritische Infrastrukturen

Zugangssicherheit für Netzwerke – VPN weitergedacht!

Sicherer Zugang in Ihr Netzwerk und wirksamer Datenschutz gegen Angriffe von innen und außen



- Keine virtuelle Netzwerkkarte notwendig
- Keine separate SW-Installation notwendig
- Prüfung bereits am Client
- Verbindung auf der Applikationsebene

- Keine Netzwerk-Netzwerkkopplung
- Kein Zugriff von außen möglich
- Keine verbleibenden Spuren auf Client Rechner

Kommunikationssicherheit bereits vor dem Client-PC



Anwender
Biometrie



Anwender
PIN für
Biometrie



Storage HW
AES 256 Bit
verschlüsselt



Anwender
Zertifikat
2048 Bit

Sicherheitsblock 1

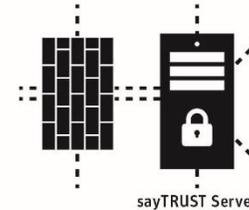
PKI mehrstufige Persönliche Identifizierung.
Sicherheit vor Aktivierung des Clients



VPSC-Tunneling
direkt aus dem
Client
Prozesspeicher



Diffie-Hellmann-
Kommunikations-
Schlüssel aus
Client-RAM



APP-Socket
Verlängerung vom
Client-RAM

Sicherheitsblock 2

Verbindungssicherheit Defense in Depth.
Sicherheit vor der Kommunikation



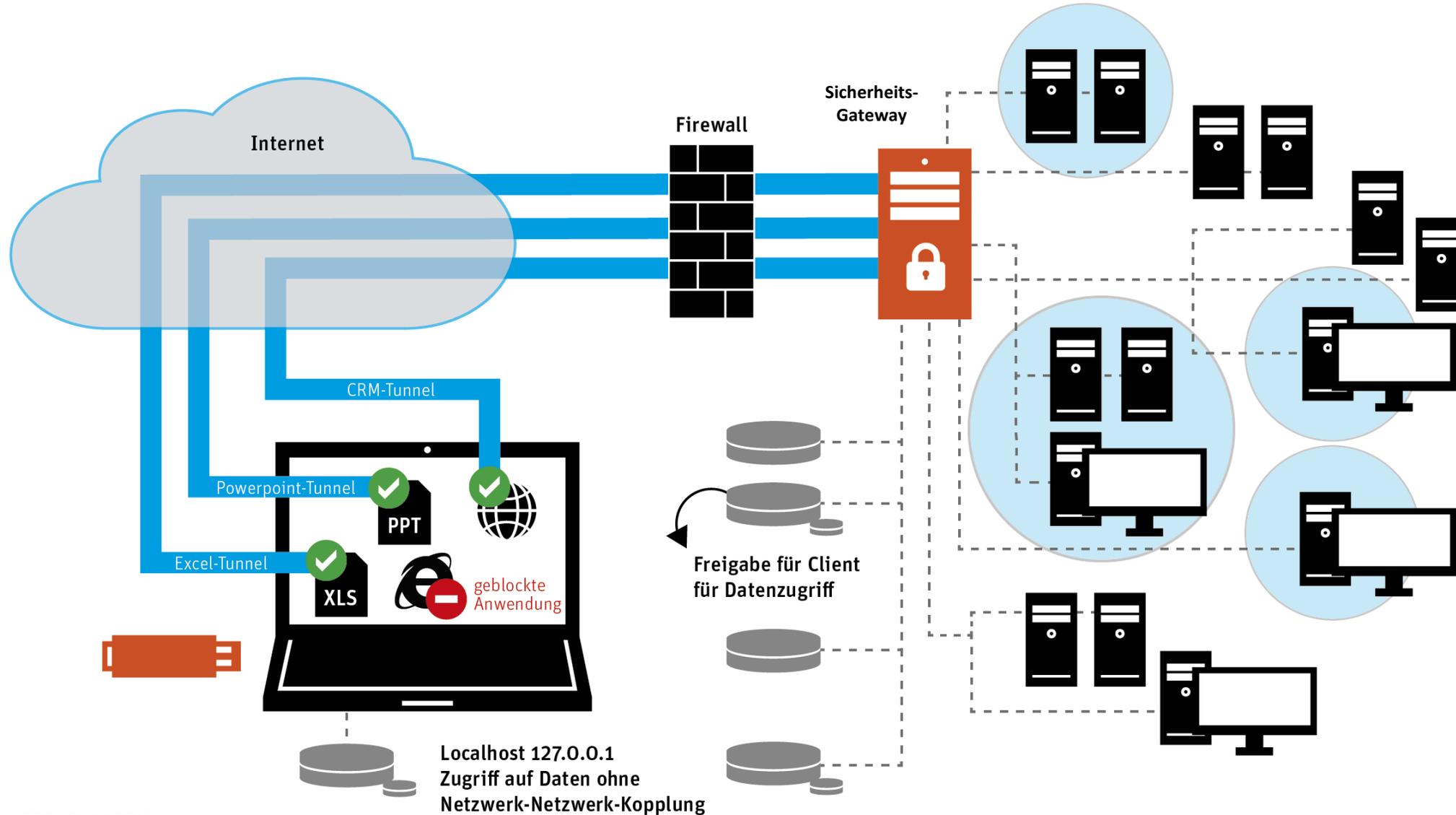
Das 2048 Bit Anwenderzertifikat
des VPSC Kommunikations-Clients,
das durch die eigene CA signiert
und überprüft wurde, ermöglicht
Zugriffe auf lokale, mobile oder
remote Anwendungen.

Sicherheitsblock 3

Überwachung vor dem Netzwerk

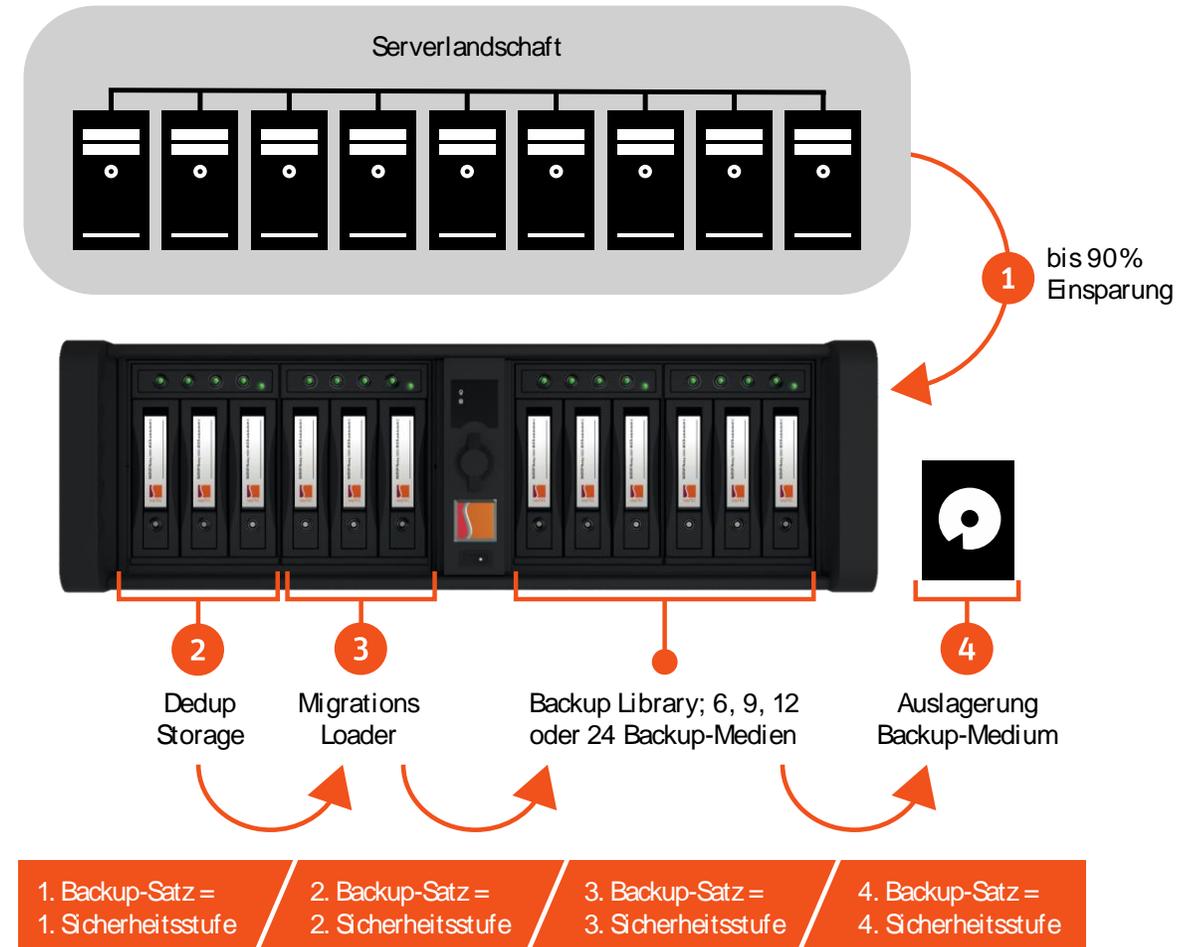
Deutliche Vereinfachung in der Datenkommunikation

Netzwerk-trennung, Single-Sign-On, Sicherheit und Komfort



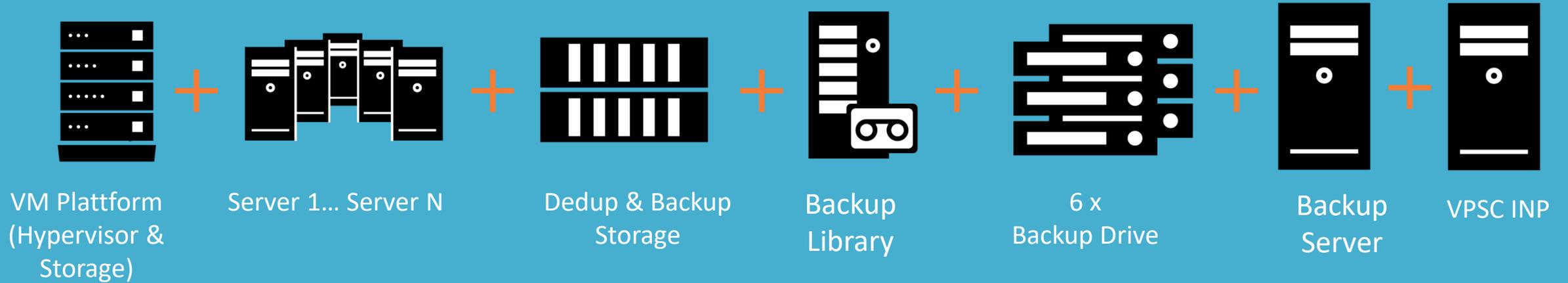
Neue, mehrstufige Backuptechnologie

- 1 Erste Backup-Stufe**
 Datensicherung erfolgt auf der Dedup-Einheit mit bis zu 90% Reduzierung der Sicherungsdatenmenge (erster Backup-Satz).
- 2 Zweite Backup-Stufe**
 Aus dem Dedup-Backup-Datensatz werden die Tagessicherungen auf die entsprechenden Laufwerke geschrieben = Zeit- und Platzeinsparung. Der zweite Backup-Satz läuft innerhalb der Appliance ohne Netzwerkressourcen ab.
- 3 Dritte Backup-Stufe**
 Die Backup-Sätze können zu vollständigen Wochen-/Monatssicherungen migriert werden. Zeiteinsparung. Dieser Vorgang läuft automatisch im Hintergrund in der Appliance ab.
- 4 Vierte Backup-Stufe**
 Auslagerung in eine sichere Umgebung.



Reduzierung der IT Komplexität

Say NO to Complexity – say YES to Simplicity



Hot Standby

Der sekundäre Anwendungsfall
Im Notfall sofort reagieren
können

Die als kritisch definierten Serversysteme werden offline bereitgehalten und laufend aktualisiert. Tritt ein Ausfall eines kritischen Servers ein, wird dieses System innerhalb weniger Minuten neu gestartet.

So erreichen Sie maximale
Verfügbarkeit und
Ausfallsicherheit für kritischen
Infrastrukturen.



Anwendungsbeispiel für Verfügbarkeit und Ausfallsicherheit für kritischen Infrastrukturen

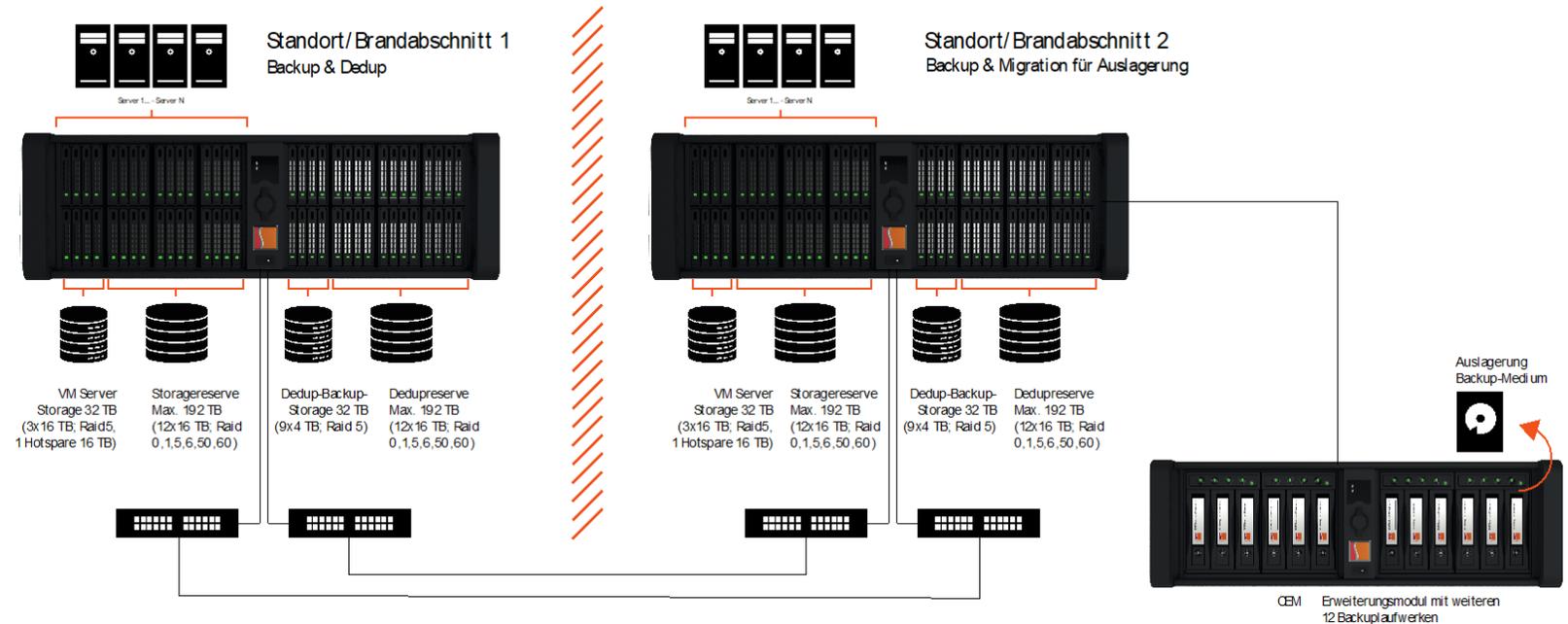
Die IT Sicherheits-Plattformen müssen neben den genannten Leistungen einen Primär- und Sekundär-Sicherungsvorgang sowie sekundäre Anwendungsfälle beherrschen.

Sekundäre Anwendungsfälle können zusätzliche Unternehmensserver, Test- und Entwicklungssysteme bis hin zu kompletten IT-Infrastrukturen sein.

Ein besonderer sekundärer Anwendungsfall ist die Offline-Bereitstellung unternehmenskritischer Server aus dem Sicherungssatz.

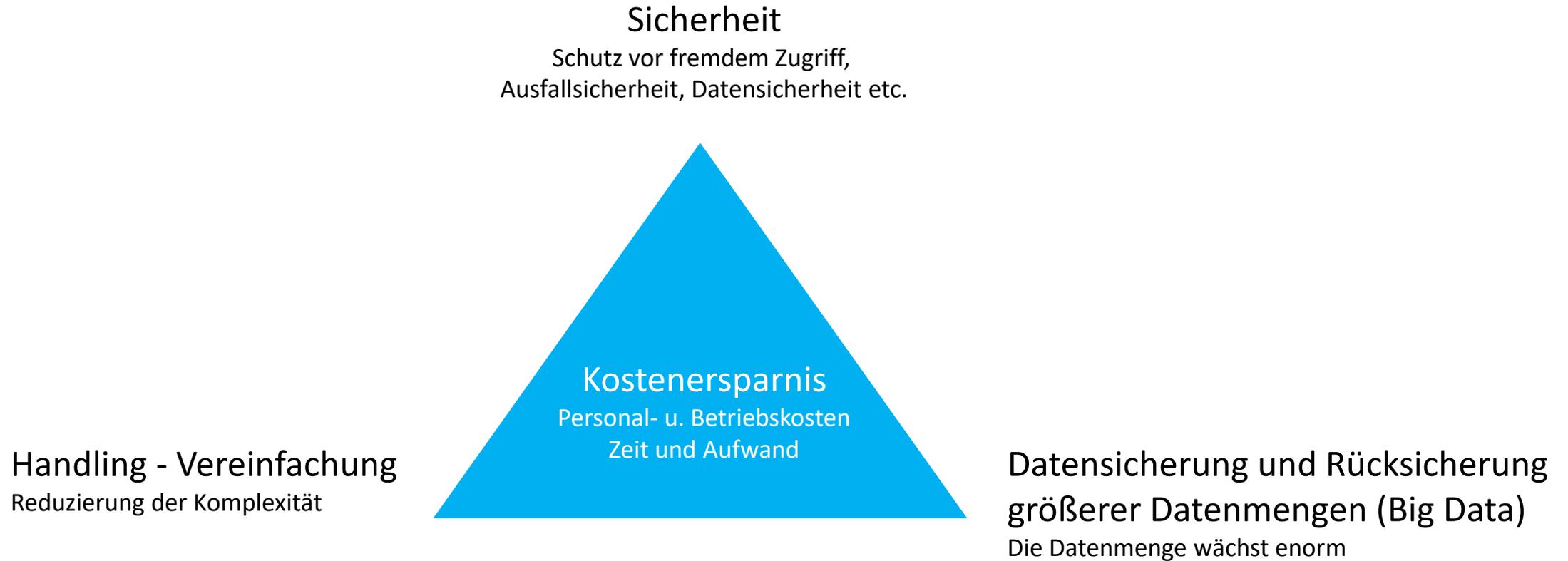
Die kritischen Systeme können unmittelbar aus der bereitgestellten Appliance in Betrieb genommen werden, z.B. bei einem Totalausfall der Serversysteme (Hardware und Software). Die als kritisch definierten Serversysteme werden offline bereitgehalten und täglich aktualisiert.

Konzept: Dedup & Migration + Ausfall & Verfügbarkeit



Vor welchen Herausforderungen steht die IT-Infrastruktur heute?

Das Trilemma des Marktes



» Vielen Dank für Ihre Aufmerksamkeit