



IT Sicherheit im Gesundheitswesen

Dr.-Ing. Marten Neubauer
Field Director Healthcare

DELLTechnologies



Bessere Patientenversorgung durch Innovation

Dell Technologies Lösungen für das
Gesundheitswesen

DELLTechnologies

Gemeinsam Leben verändern durch den Einsatz von Menschen, Anbietern und Technologie

UNSER ZIEL

Gesundheit



Daten getriebene Gesundheitsversorgung

Bildung



Gleichberechtigter Zugang zu Technologie für alle

Wirtschaftliche Chancen



Besserer finanziellen Zugang für unterversorgte Menschen.

Dauerhafte
Ergebnisse für

1 Milliarde
Menschen

UNSER ANSATZ

Strategisches Spenden



Kollaborative Ökosysteme.
Digitale Inklusion &
Kompetenzaufbau

Auswirkungen auf die Gemeinschaft



Spenden & Freiwilligenarbeit
(Technik) Pro bono

Soziale Innovation



Gesellschaftliche Plattformen.
Allgegenwärtige Technologie.

Gestiegene Erwartungen von Patienten und medizinischem Personal an die IT

Die digitale Kluft schließen

Transformation der IT im Gesundheitswesen mit einem Fokus auf den Patienten. Bereitstellung von IT as a Service

Innovation beschleunigen

Neue Technologien wie KI/ML, Datenmanagement, Edge und 5G werden die Patientenversorgung neu definieren

Neue klinische und geschäftliche Realitäten

Nutzung von Technologie und Automatisierung, um Personalengpässe zu reduzieren und die Produktivität zu steigern



Gesundheitsbranche: Bereit für das, was als nächstes kommt

Wichtige neue Technologien im Gesundheitswesen

5G

530 Mrd. \$ Produktivitätssteigerung bis 2030¹

Intrinsische Sicherheit

40 Millionen US-Bürger wurden im Jahr 2021 von Datenschutzverletzungen im Gesundheitswesen betroffen²

Digitale Zwilling

>65% CAGR für den Markt für den digitalen Zwilling im Gesundheitswesen von 2020-2025³

Kognitiv AI

100 Milliarden US-Dollar an jährlichen Einsparungen durch Big Data sowie KI und ML⁴

Quanten Computing

Healthcare Quanten Computing wird von 2020-30 eine CAGR von >40% haben⁵

Dell Technologies Lösungen für das Gesundheitswesen

Verbesserung der Patientenversorgung mit innovativen Lösungen

VEREINFACHTHE HEALTH IT DATA
FABRICS

VEREINFACHTHE HEALTH IT DATA
FABRICS

Multi-Cloud-Ökosystem



Dell Alliances
Healthcare Cloud



Klinische
Workloads as-a-
Service



Branchenführende
Healthcare IT

Vernetztes Arbeiten



Digitaler
Arbeitsplatz im
Gesundheitswesen



Vertrauenswürdige
Geräte,
Zugänge & Daten



Diagnose &
Bildgebung

Edge im Gesundheitswesen



Pflege im
Multiversum



Betriebsoptimierung



Medizinische
Daten am Edge

Personalisierte Medizin



Next-Generation-
Sequenzierung



Digitale
Pathologie



HPC & Forschung
as-a-Service



Sichere Patientenversorgung

Daten- und Bedrohungsschutz | Cyber Resilienz | Verwaltete Erkennung und Reaktion



APEX für das Gesundheitswesen

APEX-Konsole | APEX Cloud Services | APEX Kundenspezifische Lösungen

Sichere Patientenversorgung

Umfassende Sicherheit für Mitarbeiter, Netzwerk, Endpunkte, Daten und Recovery

Daten- und Bedrohungsschutz

Wir entwickeln eigensichere Infrastrukturplattformen und Geräte, die es Gesundheitsdienstleistern ermöglichen, große Datenmengen zu generieren und zu verarbeiten und gleichzeitig sicherzustellen, dass IT-Assets sicher, geschützt und verfügbar sind.

Cyber-Resilienz

Dell Technologies nutzt die Breite und Tiefe unseres End-to-End-IT-Ökosystems, um Sicherheitslösungen zu entwickeln, die mit der zunehmenden Bedrohungskomplexität umgehen können.

Management von Erkennung und Reaktion

Wir helfen bei der Sicherung von Gesundheitsumgebungen über Endpunkte, Netzwerke und Clouds hinweg, indem wir unsere offene, Cloud-native Plattform nutzen, die die Kraft des menschlichen Intellekts mit Erkenntnissen aus Sicherheitsanalysen kombiniert, um Erkennung und Reaktion zu vereinheitlichen.

Cyber Attacken: Ransomware

Noch stärkerer Fokus auf Ransomware



Entwicklung von einfacher Malware zu „anspruchsvollen Erpressung“



Geringes Risiko
Hoher Ertrag
As a Service
Verfügbar auch für Nicht-Experten
Business Modell, das sich vervielfältigen lässt



„Status ignoriert“



Zunahme von Supply Chain
Angriffsvektoren sind VPN,
RDP, Phishing
vermehrt Angriffe über VPN
Appliances, häufig über
kritische Accounts im Urlaub
und am Wochenende

Quellen: US Cybersecurity & Infrastructure Security Agency (CISA), NSA, FBI, NZCSC

DELL Technologies

Ransomware

Business Impact



73%

der Unternehmen wurden
Ziel einer Ransomware
Attacke
Steigerung um 33%
gegenüber 2021



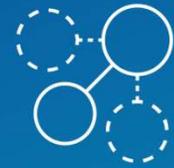
37%

der Betroffenen mussten in
der Folge Personal entlassen.
35% verloren deshalb
Führungskräfte



33%

mussten ihr Geschäft
temporär aussetzen



67%

Erlitten einen Schaden zwischen 1 und
10 Mio. USD, 4% 25 - 50 Mio.
Durchschn. Bereinigungskosten
betragen 2021 1,6 Mio.€.
Aufgrund der Komplexität der Angriffe
ist 2022 eine Verdopplung zu erwarten.

Quellen: US Cybersecurity & Infrastructure Security Agency (CISA), Recorded Future, censuswide

Ransomware

Es zahlt sich nicht aus, zu zahlen!



42%

42% zahlten Lösegeld



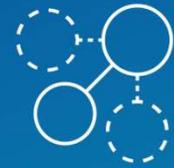
80%

der Unternehmen, die bezahlten, wurden ein zweites Mal angegriffen, 85% davon innerhalb eines Monats für höhere Forderung



27%

bezahlten, weil sie kein Backup hatten
34% bezahlten, weil sie kein Personal für das Recovery hatten



42%

der Unternehmen bekamen alle ihre Daten zurück (2021: 51%)

Quellen: US Cybersecurity & Infrastructure Security Agency (CISA), Recorded Future, censuswide

DELLTechnologies

Entscheidungsfindung Lösegeld

- Ist es sicher, dass die Erpresser ihre Zusagen einhalten?
- Könnten die Daten durch die Entschlüsselung zerstört werden?
- Könnte eine Lösegeldzahlung aufgrund der Herkunft der Angreifer eine Straftat sein?
- Motiviert die Lösegeldzahlungen die Täter zu weiteren Angriffen?
- Existieren weitere Risiken, die durch die Lösegeldzahlung nicht abgedeckt sind?

Treffen Sie Vorsorge, damit Sie nicht bezahlen müssen! Die Kosten für die Vorsorge sind auf jeden Fall niedriger, als die kombinierten Kosten für Lösegeld und dazugehörige Recoveryaufwände, insbesondere bei multiplen Angriffen.

Quellen: US Cybersecurity & Infrastructure Security Agency (CISA), Recorded Future, censuswide

Angriffsstrategie vs. Resilienzstrategie



Identifizieren



Schützen



Entdecken



Antworten



Genesen

Risiken bewerten

Sichern von Daten und reduzieren der Angriffsfläche

Bedrohungen entdecken

Abwehr von Bedrohungen

Wiederherstellung nach dem Angriff

VOR

WÄHREND

NACH



Erste Aufklärung



Phishing oder Exploit



Fuß fassen



Erweitern der Kontrolle



Ziel-Backups und kritische Systeme



Angriff starten

Verweildauer des Angreifers durchschnittlich 100+ Tage im Netzwerk

Sichere Dell Endgeräte

Für die sichersten kommerziellen PCs der Branche

Angriffe verhindern, erkennen und darauf reagieren

Dell SafeGuard and Response, powered by VMware
Ruß und Secureworks

**Sichere Verschlüsselung
Informationen & Daten
schützen**
Dell SafeData mit
Netskope und Absolute

**Zugriff auf Ihr Gerät
Sicher von überall**
VMware Workspace ONE

Über dem Betriebssystem

ENTDECKEN



VERHINDERN

REAGIEREN

**Stellen Sie sicher, dass
die Hardware bei
Lieferung
manipulationsfrei ist**
Dell SafeSupply Chain*

**Auf dem Bildschirm pflegen
Digitale Privatsphäre**
Dell SafeScreen
Dell SafeShutter

Unterhalb des Betriebssystems & integriert

**Verschaffen Sie sich
einen Überblick über
BIOS-Manipulationen**
Dell SafeBIOS

**Integrierte
Lösungen**

**Sichere
Benutzeranmeldeinformationen**
Dell SafeID

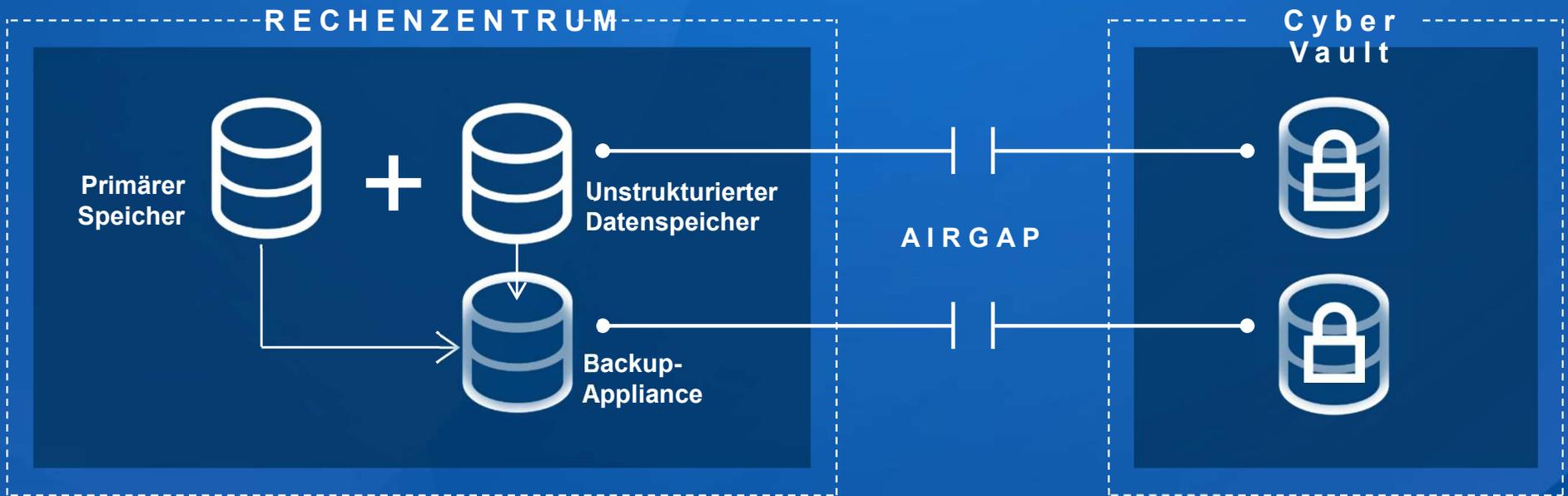
VOR

WÄHREND

NACH

Aufbau von Cyber-Recovery-Funktionen

Daten-Vaulting und -Recovery



Isolation



Unveränderbar



Intelligenz

The logo for Dell Technologies, featuring the word "DELL" in a stylized font where the 'E' is composed of three horizontal lines, followed by the word "Technologies" in a sans-serif font.