DIGITALPAKT SCHULE 2022 VIRTUAL CONFERENCE

HERZLICH WILLKOMMEN

26. Januar 2022
digitalpaktschule-konferenz.de

VOGEL IT AKADEMIE

Die Themen

- ✓ Bildung im Fadenkreuz
- ✓ Bedrohung durch Ransomware => eine Betrachtung
- ✓ Vorschlag zum vollständigen Schutz vor Ransomware
- ✓ Arcserve® und die passende Lösung

Sven Haubold (Sven.Haubold@arcse

Bildung im Fadenkreuz

Warum sollte das Thema Datenschutz und Datensicherheit für Bildungseinrichtungen wichtiger sein als z.B. greifbare, „neue Endgeräte“ zu beschaffen?

SharePoint Online · Office 365 · Microsoft Teams · OneDrive for Business · Exchange Online

Die meisten Schule und Universitäten…

⇒ haben ihre IT-Systeme und -Anwendungen in den vergangenen 1,5 Jahren in die Cloud verlagert, um den Fernunterricht zu ermöglichen.

⇒ sind in jüngster Zeit Cyber-Attacken zum Opfer gefallen, prominente Beispiele sind die **Einrichtungen in Leipzig, Jülich, Stuttgart, Garching, Dresden, Karlsruhe und Freiburg**.

⇒ fast zwei Drittel der Bildungseinrichtungen berichten, dass ihre IT-Sicherheit hinter der steigenden Komplexität ihrer Systeme zurückbleibt.

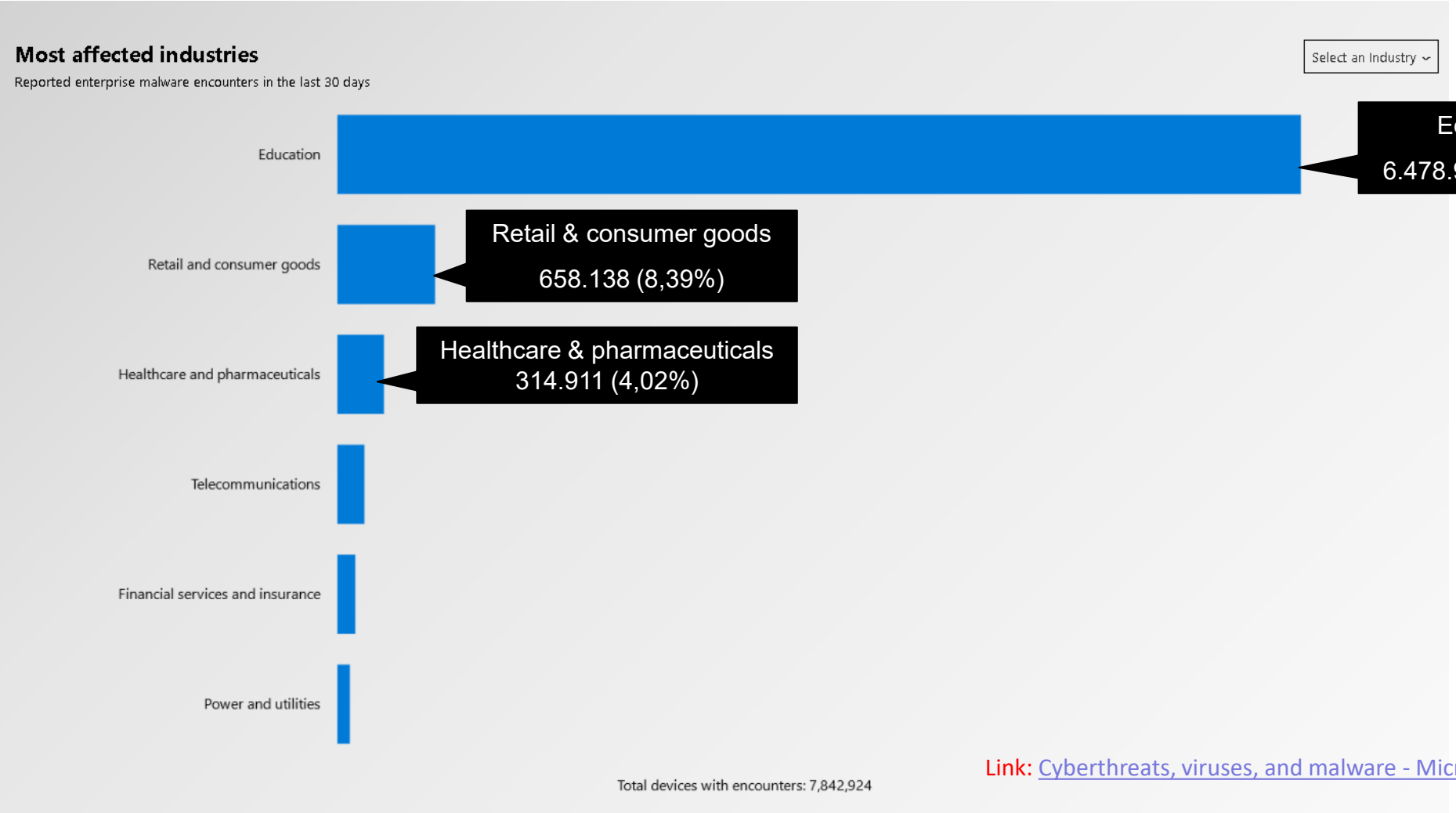
⇒ sie in zunehmendem Maße Ransomware-Angriffen ausgesetzt. Das kommt nicht überraschend: Zu Beginn des Umstiegs ging es vor allem darum sicherzustellen, dass die erforderliche Technologie zum Remote-Arbeiten überhaupt vorhanden ist. Der Unterricht sollte dabei so wenig wie möglich gestört werden.

⇒ Hackerangriffe auf Forschungs- und Bildungseinrichtungen werden weiter zunehmen

⇒ Laut dem Lagebild des Bundeskriminalamts wurden im vergangenen Jahr rund 100.000 Fälle von Cyberkriminalität gemeldet. Im Vergleich zu 2019 ist das ein Zuwachs von 15 Prozent.

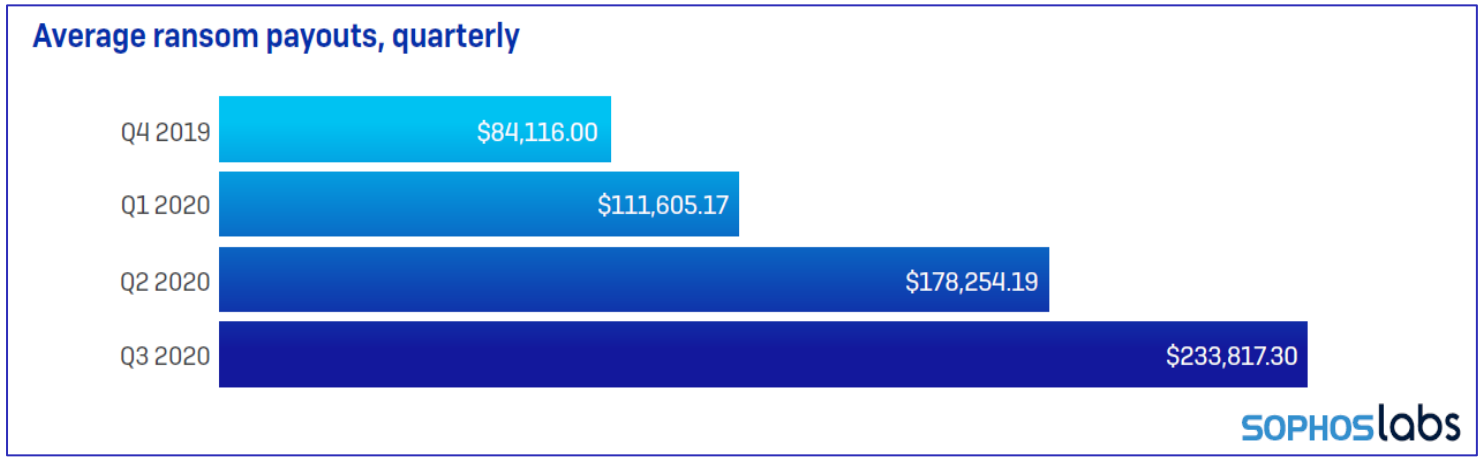
Bildung im Fadenkreuz

Warum sollte das Thema für Bildungseinrichtungen wichtiger sein als z.B. greifbare, „neue Endgeräte“ zu beschaffen?



Link: Cyberthreats, viruses, and malware - Microsoft Security Intelligence

Wachsende Auswirkungen von Ransomware auf IT und Unternehmen

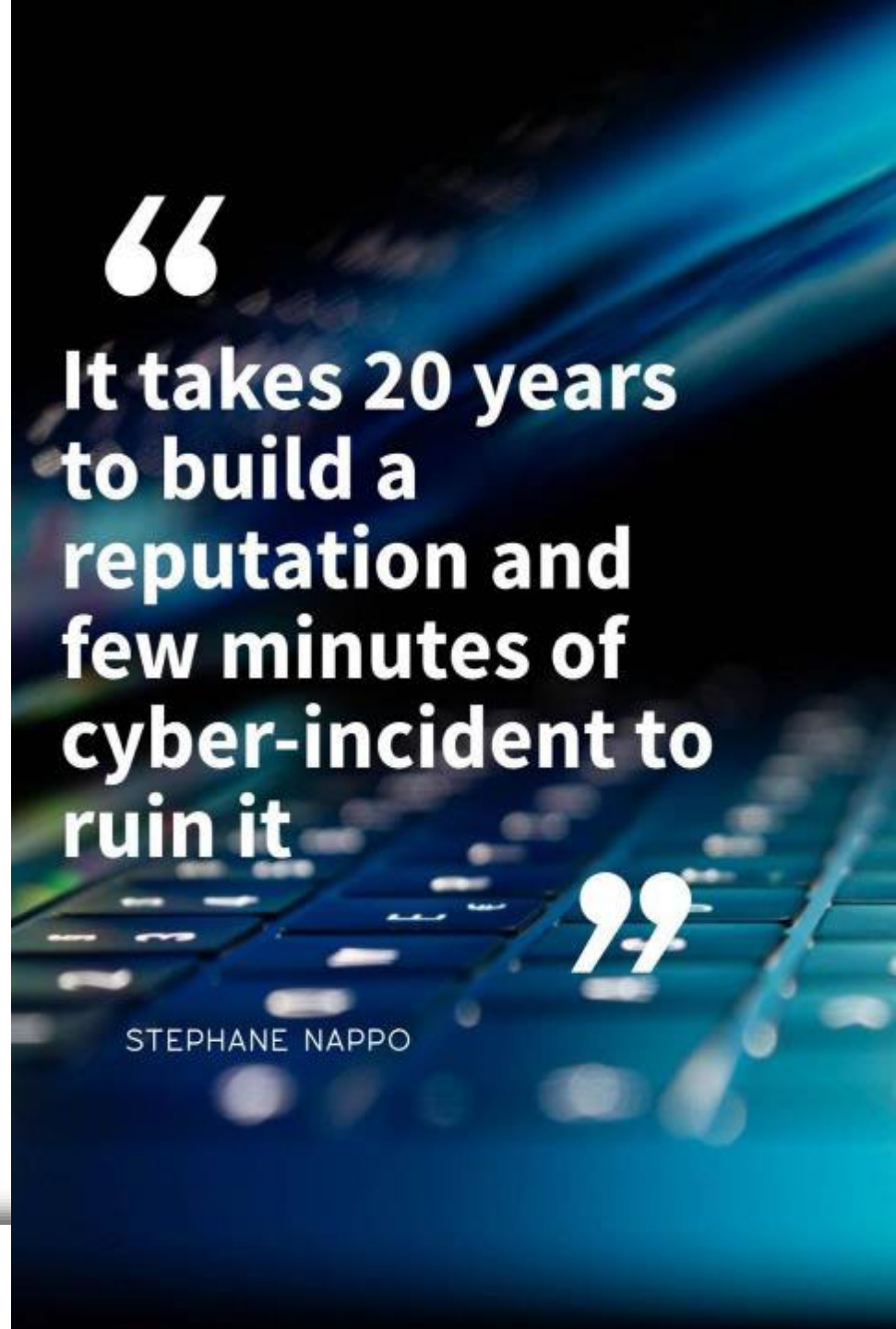


Neuste Ransomware Trends:

- Ransomware-as-a-Service
- Kunden Support Hotlines
- Kaltakquise per Telefon

IT Wandlung erschwert die Verteidigung von Ransomware:

- Server, Endpoints, IoT, NAS, SAN, LAN, WAN, Cloud IaaS, Cloud SaaS, etc.



Sven Haubold (Sven.Haubold@arcserve.com)

Haben Sie einen Plan für eine Datenwiederherstellung im Notfall?

Obwohl die viele eine Katastrophe als etwas ansehen, das nicht eintreten wird, haben die Meisten konkrete Maßnahmen zur Risikominderung ergriffen.

Folgenden Möglichkeiten sind die Regel:

- ✓ Datensicherung / Kopie auf Band
- ✓ Standortübergreifende Datensicherungen / Replikation
- ✓ Datensicherung / Kopie in die Cloud
- ✓ Ein kleinerer Prozentsatz hat DRaaS

Eine Datensicherung & DR-Plan…

- ✓ …müssen den Anforderungen der **EUDSGVO** entsprechen und es ist immer der Prozess und nicht die Soft- & Hardware alleine
- ✓ …sind versicherungsrelevant und werden in einer Police gefordert / berücksichtigt.

Der Schutz vor Ransomware bei der Datensicherung wird häufig unterschätzt!

Im Falle eines Angriffs – *die Schüler freuen sich über Unterrichtsausfall*

- ✓ Die Wahrscheinlichkeit eines Ransomware-Angriffs ist wesentlich höher als die einer „normalen“ Katastrophe.
- ✓ Wenn ein Ransomware-Angriff auftritt.....
  - ✓ Die erste Frage lautet: "Können wir Daten und Dienste wiederherstellen?„
    - ✓ „JA!“ Wie aktuell ist die Datenwiederherstellung?
    - ✓ „NEIN“ => Beantworten Sie sich die Frage selber!
  - ✓ Die zweite Frage lautet: "Wie schnell können wir uns davon erholen?„
    - ✓ „Schnell !“ => Wann kann der Betrieb wieder aufgenommen werden.
    - ✓ „Langsam !“ => Welchen Einfluss hat der Ausfall auf den Geschäftsbetrieb.
- ✓ Eine Cloud oder ein zweiter Standort ist gut gegen Katastrophenfälle und schlecht für Ransomware (langsame Wiederherstellung)
- ✓ Immutable Storage => Unveränderbarer Speicher
  - ✓ Gut für die Wiederherstellung nach einem Ransomwarebefall,
  - ✓ Für ein reines OS Desaster Recovery nicht geeignet

Vollständige Ransomware-Präventionsstrategie

Ransomware-Prävention erfordert eine multimodale Strategie

Es gibt keine “Wunderwaffen"

Es ist möglich, die Wahrscheinlichkeit eines Ransomware-Angriffs mit Cybersicherheit zu reduzieren

Angriffe können passieren, und eine organisierte Wiederherstellung ist entscheidend

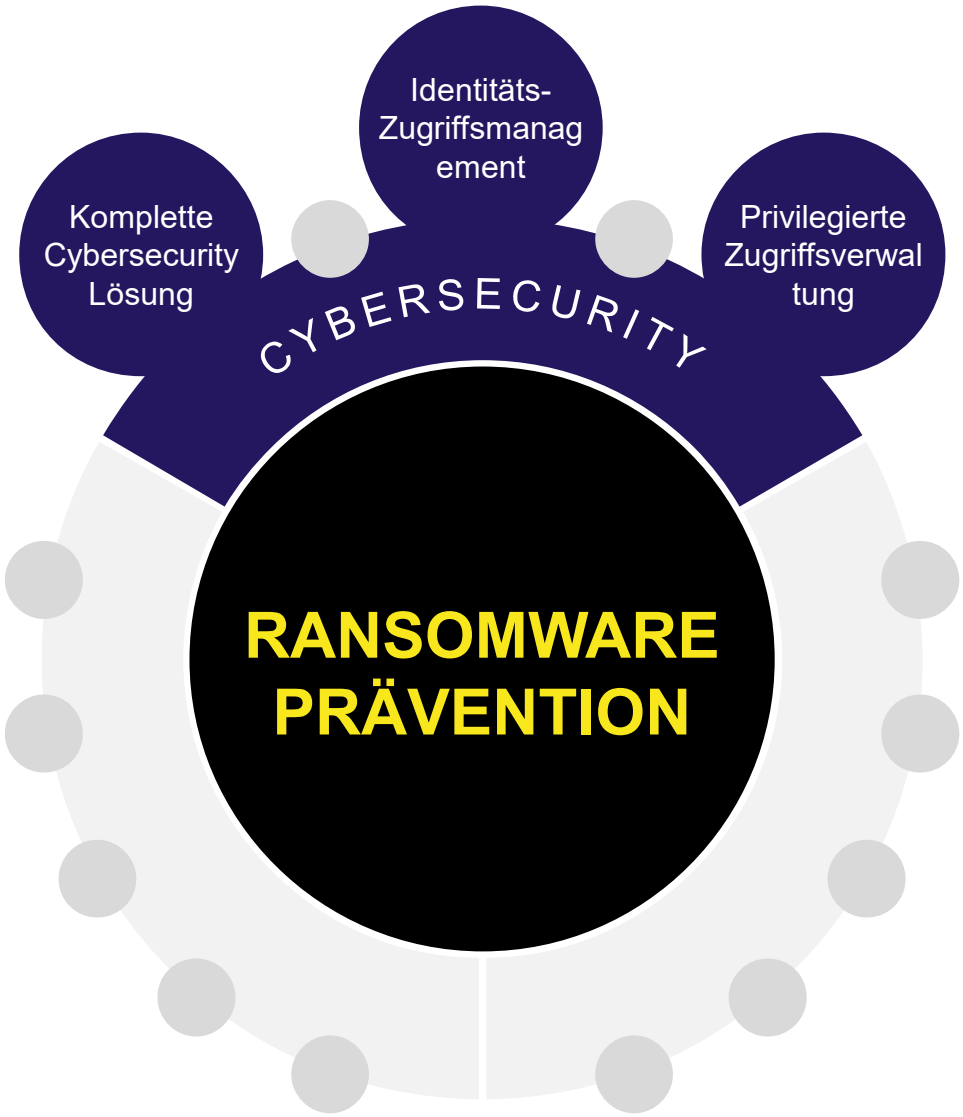
Vollständige Ransomware-Präventionsstrategie

Ransomware-Prävention erfordert eine multimodale Strategie

Es gibt keine “Wunderwaffen"

Es ist möglich, die Wahrscheinlichkeit eines Ransomware-Angriffs mit Cybersicherheit zu reduzieren

Angriffe können passieren, und eine organisierte Wiederherstellung ist entscheidend



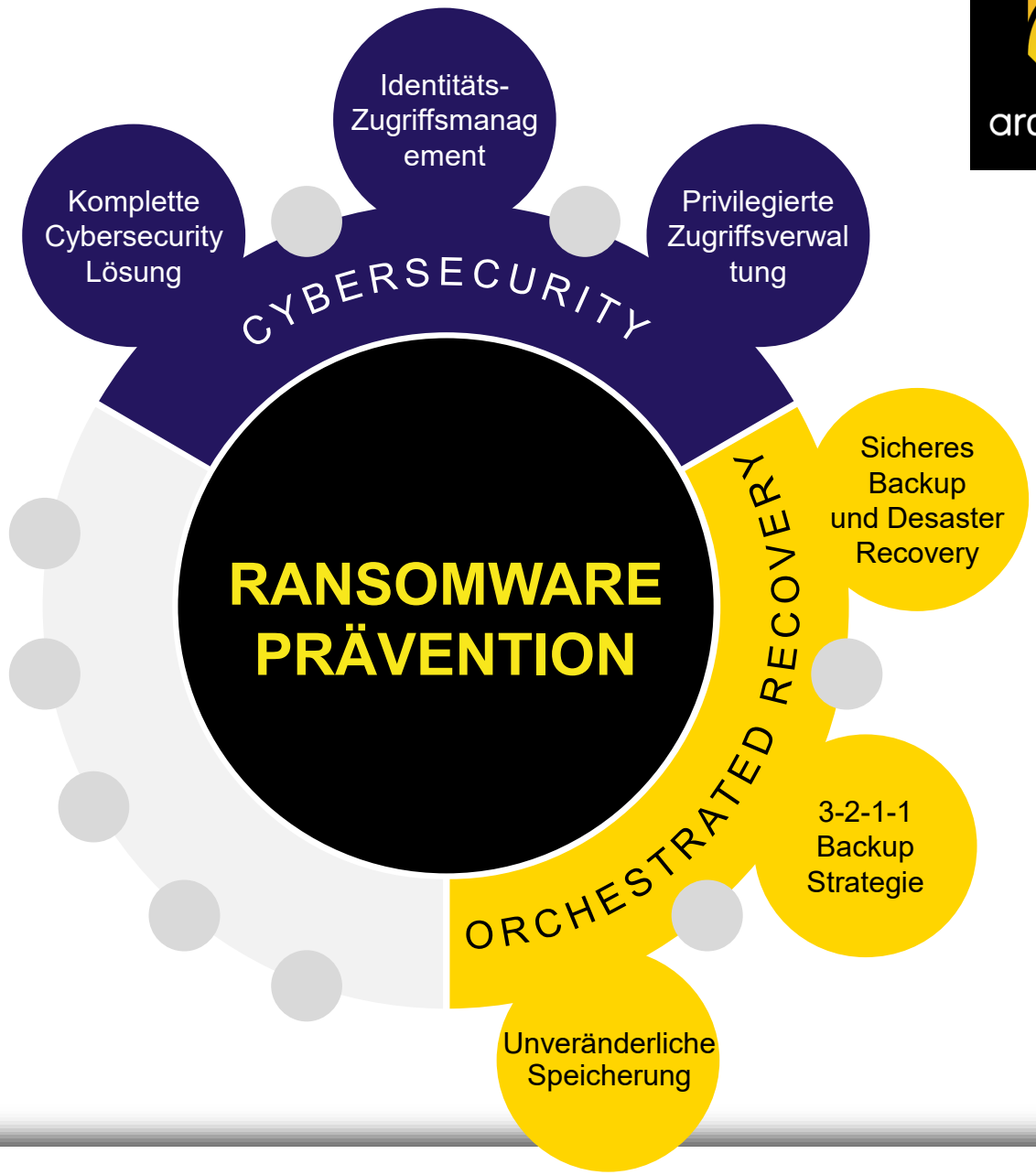
Vollständige Ransomware-Präventionsstrategie

Ransomware-Prävention erfordert eine multimodale Strategie

Es gibt keine “Wunderwaffen"

Es ist möglich, die Wahrscheinlichkeit eines Ransomware-Angriffs mit Cybersicherheit zu reduzieren

Angriffe können passieren, und eine organisierte Wiederherstellung ist entscheidend



Sven Haubold (Sven.Haubold@arcserve.com)

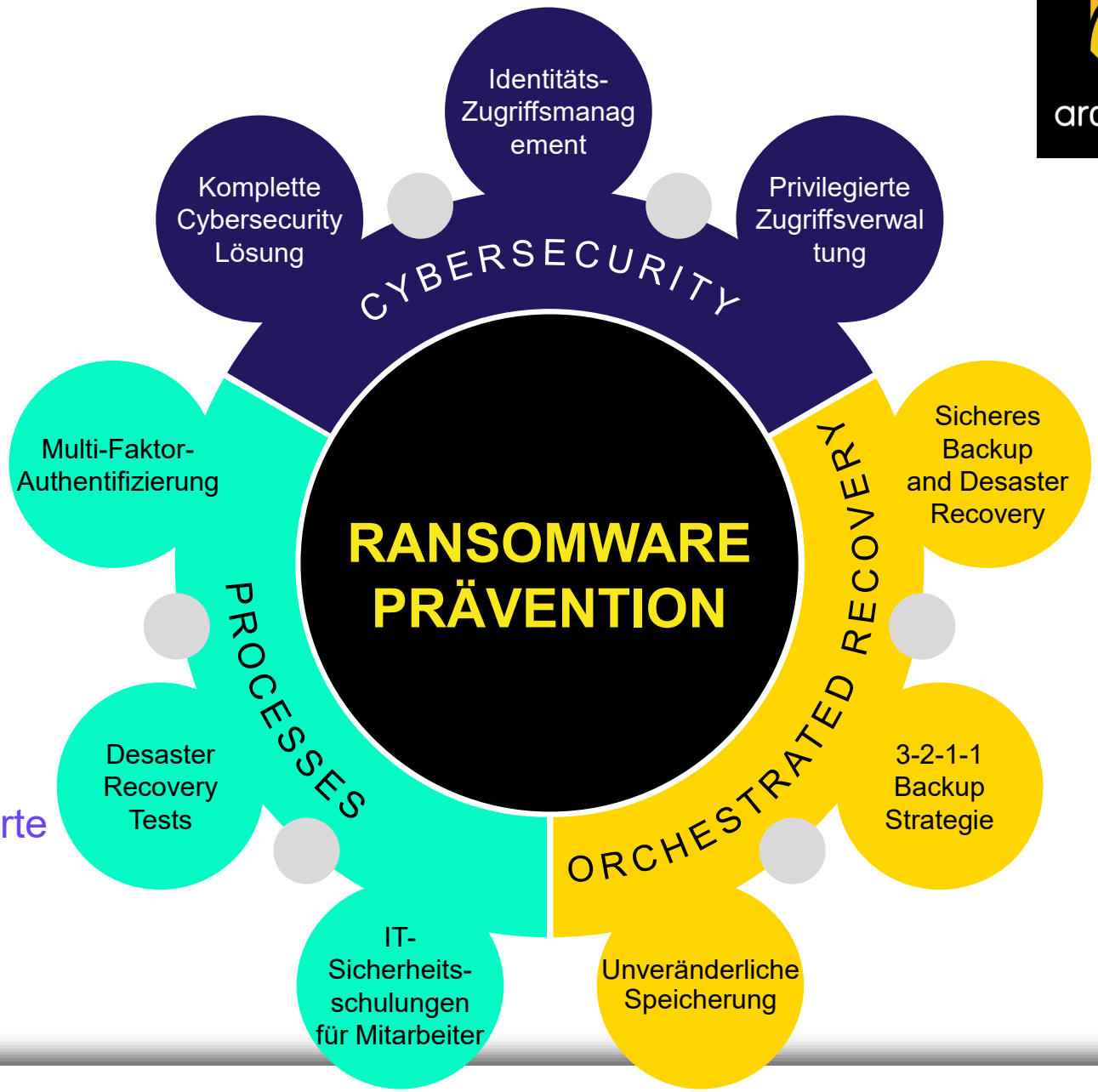
Vollständige Ransomware-Präventionsstrategie

Ransomware-Prävention erfordert eine multimodale Strategie

Es gibt keine “Wunderwaffen"

Es ist möglich, die Wahrscheinlichkeit eines Ransomware-Angriffs mit Cybersicherheit zu reduzieren

Angriffe können passieren, und eine organisierte Wiederherstellung ist entscheidend



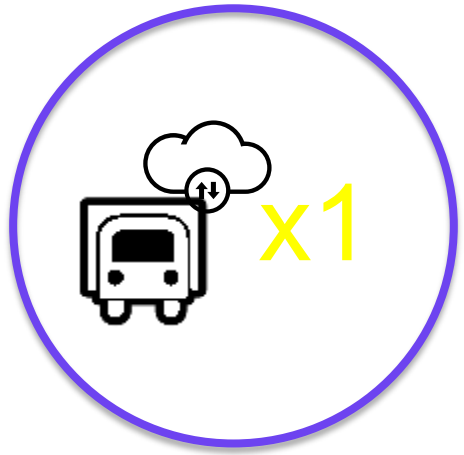
Sven Haubold (Sven.Haubold@arcserve.com)

Was kann/muss der Bildungsträger leisten? Wie sieht der minimale/optimale Schutz aus?

Die 3-2-1 Regel in der Datensicherung

Erstellen Sie mindestens 3 Sicherheitskopien Ihrer Daten. (regelmäßig, automatisiert, nachvollziehbar)

Sichern Sie diese Kopien auf mindestens 2 verschiedenen Datenträgern. (lokaler Speicher, NAS, SAN, Band etc.)

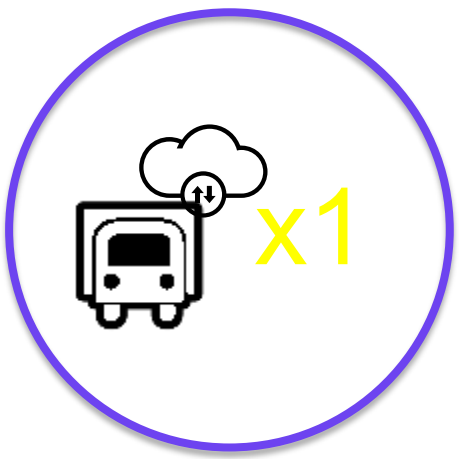


Speichern Sie mindestens 1 Kopie an einem separaten Standort (Cloud, Tresor, anderer Brandabschnitt etc.)

Die 3-2-1 Regel reicht nicht mehr aus und sollte durch 3-2-1-1 erweitert werden!

Erstellen Sie mindestens 3 Sicherheitskopien Ihrer Daten. (regelmäßig, automatisiert, nachvollziehbar)

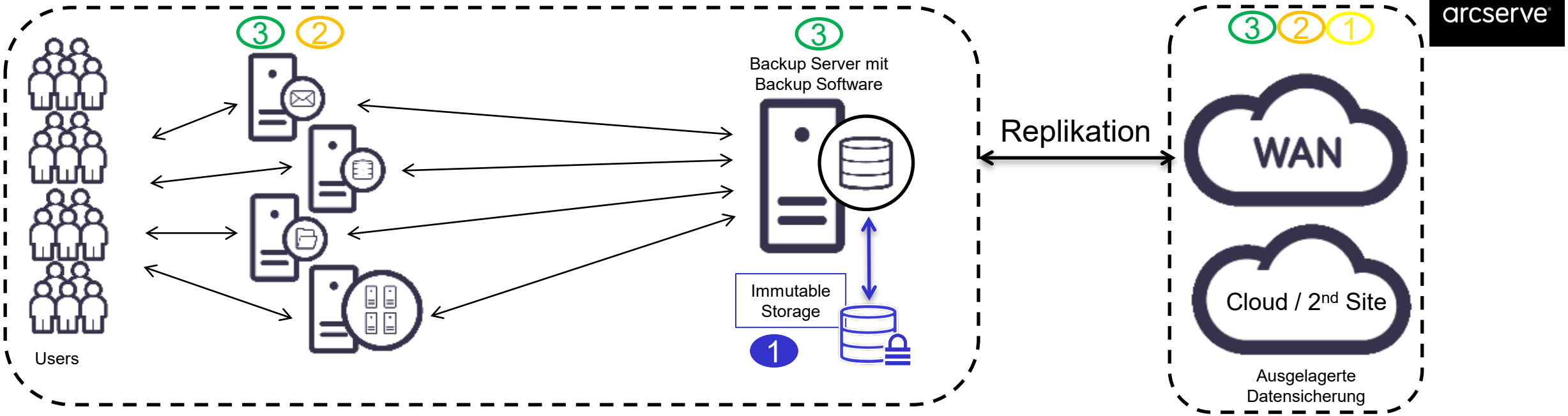
Sichern Sie diese Kopien auf mindestens 2 verschiedenen Datenträgern. (lokaler Speicher, NAS, SAN, Band etc.)



Speichern Sie mindestens 1 Kopie an einem separaten Standort (Cloud, Tresor, anderer Brandabschnitt etc.)

Speichern Sie mindestens 1 Kopie auf einem Immutable Storage (Cloud oder vor Ort)

Die 3-2-1-1 Regel

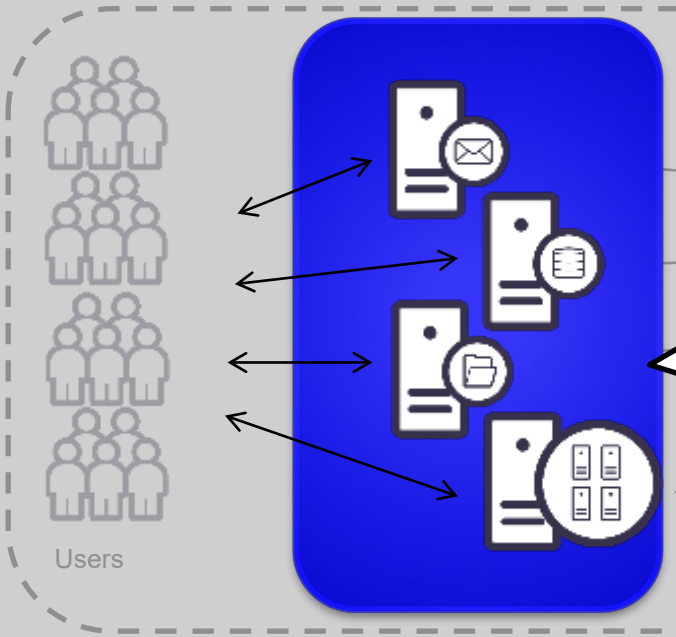


- 3 Kopien der Daten => Produktion, Backup & 3. Kopie
- 2 Mindestens 2 Kopien auf verschiedenen Datenträgern
- 1 Mindestens 1 Kopie an einem separaten Standort
- 1 Mindestens 1 Kopie auf einem Immutable Storage (WORM)

Herausforderungen

- ✓ Die Bandsicherung kann ein Teil der Lösung sein, die Wiederherstellung ist aber zeitaufwendig.
- ✓ Welches Band ist das Richtige für die Wiederherstellung nach einem Schadsoftwarebefall.
- ✓ Cloud- Kopien sind langsam bei der Wiederherstellung und können sehr teuer werden
- ✓ Immutable Storage ist als Ergänzung zur Datensicherung zu sehen.
- ✓ Mehrer Technologien ergeben eine ganzheitliche Lösung.

Die 3-2-1-1 Regel



3 3 Kopien der Daten– Produktion, Backup & 3. Ko

2 Mindestens 2 Kopien auf verschiedenen Datenträ

1 Mindestens 1 Kopie an einem separaten Standor

1 Mindestens 1 Kopie auf einem Immutable Storage

OneXafe Immutable Object Store

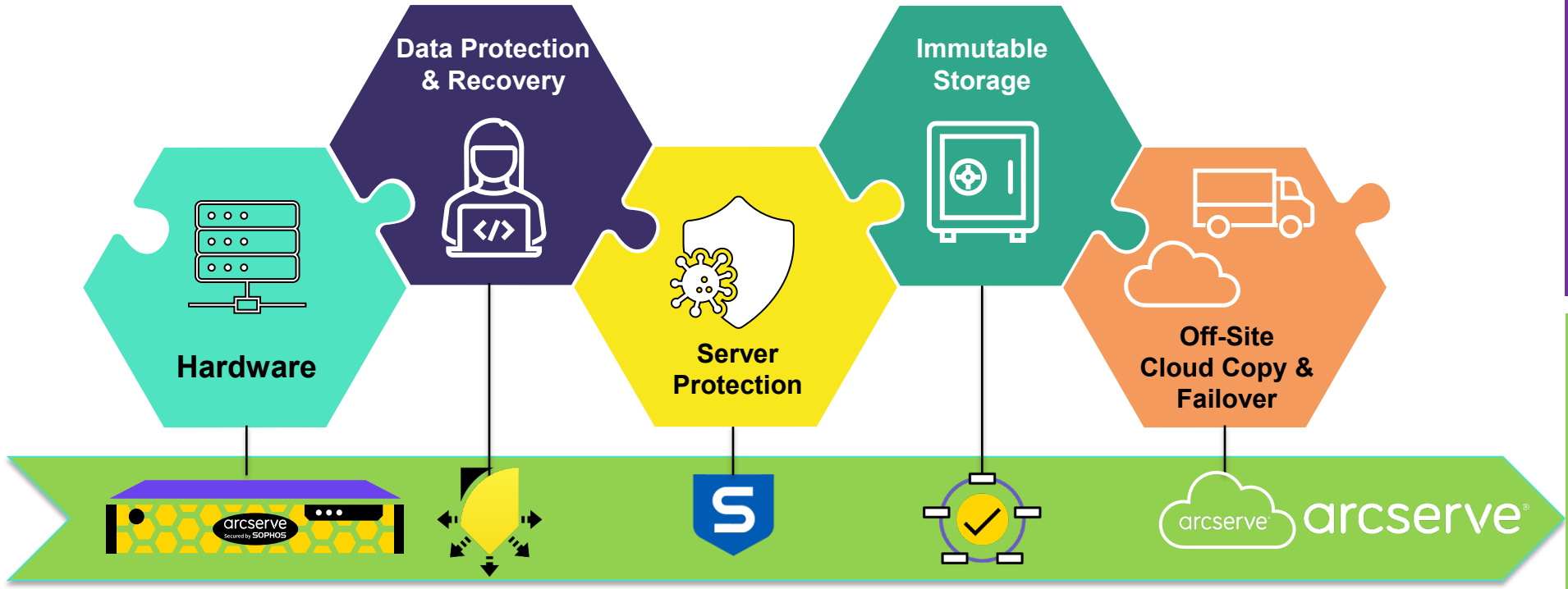
- Kosteneffektiv
- Immutable Snapshots – Point in Time Rollback zu einem früheren Zeitpunkt
- Sofortiger Zugriff auf alle Datensicherungen
- Multi Faktor Authentifikation (MFA Integration)
- Hohe Ausfallsicherheit (Cluster) und sehr schnelle Wiederherstellung nach einem Festplattenausfall
- Einfach skalierbar
- Schutz des gesamten UDP- Datenspeichers
- De-Duplizierung verbessert UDP weiter
- Zusätzlicher Schutz in Kombination mit Arcserve UDP durch Sophos Intercept X

✓ Immutable Storage ist als Ergänzung zur Datensicherung zu sehen.

✓ Mehrer Technologien ergeben eine ganzheitliche Lösung.

Arcserve® - Eine Lösung für Datensicherung und Datenschutz

Risikominimierung | Zuverlässiger Datenschutz mit Cybersicherheit und unveränderlichem Speicher (Immutable Storage)



First Line of Defense

Cybersicherheit

Proaktiver Schutz vor bekannten & unbekannten Bedrohungen

Kombination fortschrittlicher KI-gesteuerter und verhaltensbasierter Technologien und Mechanismen zur Verhinderung von Angriffen

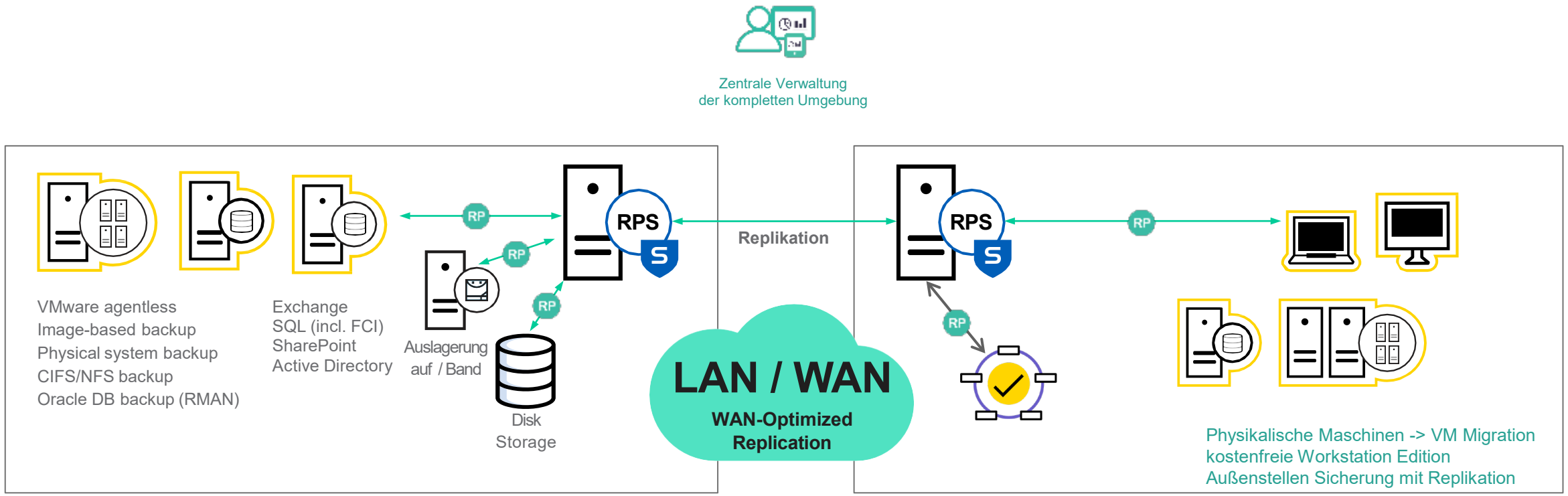
Last Line of Defense

Data Protection *mit Immutable Storage*

Schnelle & plattformübergreifende Datenwiederherstellung

Integration von Backup, Disaster Recovery und Betriebskontinuität, einschließlich Automatisierung und Ochestrierung.

Arcserve® beim Landkreis Leipzig

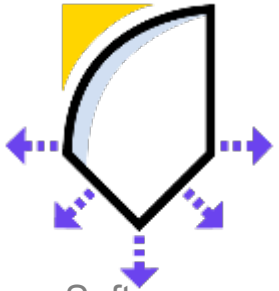


Protecting IT and Businesses from Ransomware

arcserve®

Arcserve Solutions – Multilayered Ransomware Protection

Arcserve® UDP
Geschützt durch Sophos



Software

Arcserve® Appliances
Geschützt durch Sophos

Backup Server

OneXafe Immutable Datastore

Daten unveränderbar speichern

Optional Tape or Cloud Offsite Protection

Integrated Tape / Cloud Protection

Lösungswort = Sophos

Lösungen sprechen für sich....
Sprechen Sie mit uns!

Sven Haubold
Territory Account Director
Tel.: +49 170 8538076
Sven.Haubold@Arcserve.com