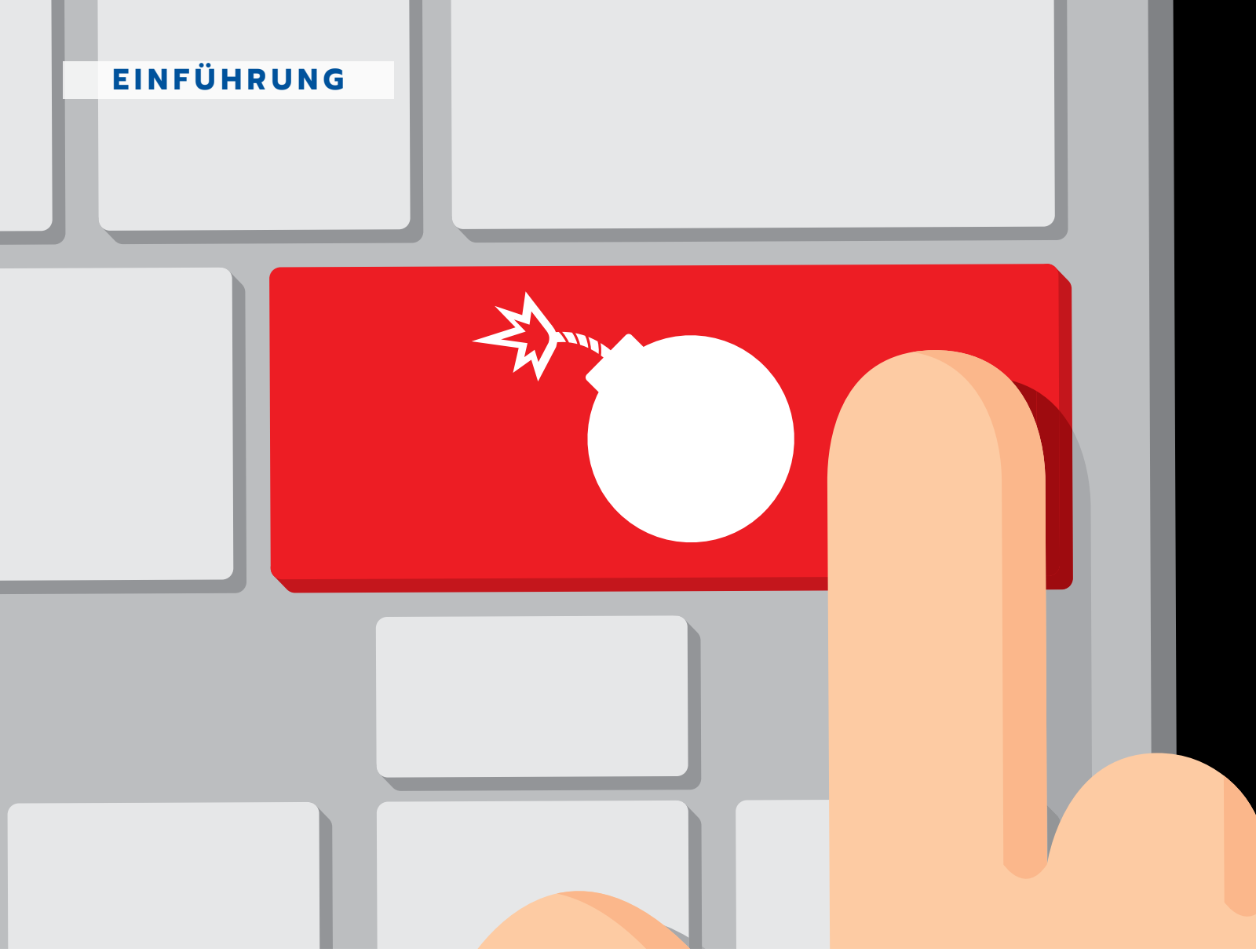
EFFEKTIVE DATENSICHERHEIT

mit einem mehrstufigen Ansatz für Ransomware-Schutz und -Recovery

Quantum®

EINFÜHRUNG



Kein Unternehmen, keine Branche ist heute mehr vor Ransomware sicher, und eine Trendwende ist nicht abzusehen. Die Malware verursacht heute (2021) Kosten in Milliardenhöhe. Am stärksten betroffen sind Organisationen aus dem Gesundheitswesen und dem öffentlichen Sektor, die durch die Attacken in ihrer Versorgungleistung erheblich beeinträchtigt sind. Die Leidtragenden sind nicht nur Patienten und Kunden, sondern wir alle. Laut einem Bericht von Health IT **„führen Ransomware-Attacken im Durchschnitt zu einem rund 15-tägigen Ausfall der elektronischen Patientenakten."** In einigen Fällen, so etwa beim University of Vermont Health Network und den Universal Health Services (UHS), dauerten die Angriffe über einen Monat. **„Die UHS-Attacke betraf alle 400 US-Standorte und führt zu einem dreiwöchigen Stillstand. Die Kosten für Wiederherstellung und Umsatzverluste beliefen sich auf insgesamt 67 Mio. US-Dollar."** Beim UVM-Angriff im Oktober lagen die Umsatzverluste und die Wiederherstellungskosten für die Computersysteme bei rund 1,5 Mio. US-Dollar pro Tag.

Vielfältige Einfallstore durch lückenhafte Security

Sie müssen nicht nur Ihr Netzwerk sichern, sondern auch alle denkbaren Eintrittspunkte – Edge-Anwendungen, IoT, Phishing und natürlich die Vorder- und offenen Hintertüren zum Netzwerk. Viele Unternehmen haben aber nur mangelhafte Sicherheitsmaßnahmen. So konnten die kriminellen Aktivitäten und Zugriffe auf wichtige Assets kontinuierlich ausgebaut und verfeinert werden.

Formulierung einer Strategie zur Bekämpfung von Ransomware

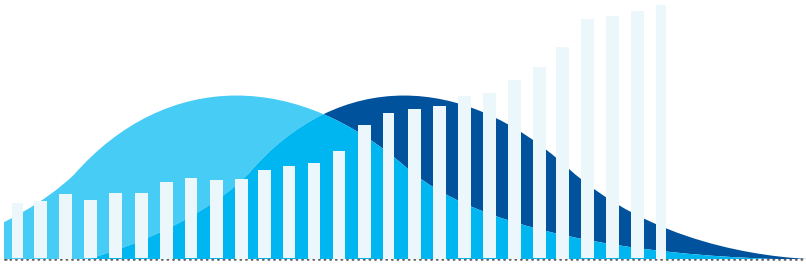
Organisationen müssen proaktiv vorgehen und einen robusten Datenschutzplan erstellen. Einfach auf eine vorhandene Backup-Infrastruktur zu vertrauen, reicht nicht mehr aus. Sie brauchen einen Backup- und Recovery-Plan, der regelmäßig aktualisiert wird, wenn neue Bedrohungen auftreten und Ihre Technologie auf den neuesten Stand gebracht wird.

Ein proaktiver Sicherheitsansatz

Backups werden zunehmend zum Hauptangriffsziel. Sie benötigen daher dringend Sicherheitsmaßnahmen zum Schutz Ihrer Backup-Infrastruktur. Ein mehrstufiger Ansatz, der Ihre Systeme vor Ransomware schützt und sie im Ernstfall wiederherstellt, gehört zu den kosteneffizientesten Methoden, um Daten wirksam zu sichern und gleichzeitig die Kosten im Griff zu behalten. Das folgende Zitat von Sunzi aus „Die Kunst des Krieges“ lässt sich gut auf die aktuelle Situation bei der Abwehr von Ransomware übertragen: **„Wenn du dich und den Feind kennst, brauchst du den Ausgang von hundert Schlachten nicht zu fürchten. Wenn du dich selbst kennst, doch nicht den Feind, wirst du für jeden Sieg, den du erringst, auch eine Niederlage erleiden. Wenn du weder den Feind noch dich selbst kennst, wirst du in jeder Schlacht unterliegen.“** Finden Sie sich nicht schon vor dem Kampf mit einer Niederlage ab, sondern setzen Sie mit einem proaktiven Sicherheitsansatz auf Sieg.

IT-Experten müssen das Thema Cybersecurity proaktiv angehen und die Verteidigungsmechanismen stufenweise betrachten und analysieren.

10 RICHTLINIEN ZUR VORBEREITUNG AUF EINE RANSOMWARE-ATTACKE



1. **Formulieren Sie eine sorgfältig durchdachte Datensicherungsstrategie, um die Unterstützung der Geschäftsleitung einzuholen. Ohne grünes Licht von oben kommen Sie nicht weit.**

2. **Erstellen Sie in Absprache mit dem Hersteller Ihres Vertrauens einen Plan, der den Nutzen des Angebots und die Vorteile für das Unternehmen insgesamt aufzeigt.**

3. **Installieren Sie eine Antivirussoftware, um die Vordertür zum Netzwerk zu schließen.**

4. **Nutzen Sie Verschlüsselungstechnologie in jeder Phase des Datenlebenszyklus – bei der Speicherung, während der Übertragung und bei der aktiven Nutzung.**

5. **Setzen Sie Schulungen an, um die Mitarbeiter über die häufigsten Methoden aufzuklären, mit denen sich Kriminelle Zugang zu Netzwerken und Systemen verschaffen, vor allem Phishing-Techniken.**

6. **Implementieren Sie unveränderbare Funktionen zur Erstellung von Snapshots Ihrer Daten, mit denen Sie Ihre Systeme unmittelbar wiederherstellen und die RPO/RTO-Vorgaben aus Ihren SLAs erfüllen oder übertreffen.**

7. **Implementieren Sie Lösungen mit „Air Gap"-Schutz (z. B. Tape-Speichersysteme) zur zeitlich unbefristeten Sicherung Ihrer Daten.**

8. **Replizieren Sie die Daten an einem externen Standort. Für DR-Zwecke können Sie auch eine Cloud- oder Object Storage-basierte Lösung nutzen.**

9. **Segmentieren Sie Ihr Netzwerk, um die Ausbreitung einer Attacke einzugrenzen. Dies ist eine der besten Methoden, um die potenziellen Folgen von Datensicherheitsverstößen, Ransomware und anderer Malware abzumildern.**

10. **Eine Cyberversicherung ist ein Muss, sollte aber immer nur den allerletzten Ausweg darstellen.**

GUTE VORBEREITUNG IST NUR EIN TEIL DER GLEICHUNG.

Angreifer nehmen Ihre Backup-Infrastruktur ins Visier.

Mit den folgenden einfachen Maßnahmen sichern Sie Ihre Datenplattformen und implementieren eine solide Backup-Strategie.

6 SCHRITTE ZUR AUSWAHL SICHERER DATENPLATTFORMEN UND DER IMPLEMENTIERUNG EINER BACKUP-STRATEGIE

Die Sicherheit gehört zu den wichtigsten Aspekten bei der Auswahl einer Datenspeicherplattform. Wenn Sie die Public Cloud nutzen oder Ihre Workloads über mehrere Clouds und Rechenumgebungen verteilt sind, benötigen Sie über die Schutzeinstellungen in Ihrem eigenen Netzwerk hinaus zusätzliche Datenschutz- und Sicherheitsmaßnahmen. Sie brauchen einen umfassenden Ansatz, an dem mehrere Abteilungen, einschließlich Sicherheitsexperten, Netzwerkadministratoren und deren Vorgesetzte, mitwirken. Schulen Sie sich und Ihre Anwender, insbesondere, wenn die Belegschaft remote arbeitet.

1 Identifizieren Sie potenzielle Schwachstellen.

2 Implementieren Sie eine renommierte Antivirussoftware. Dieser Punkt sollte nicht verhandelbar sein.

3 Erstellen Sie regelmäßige Backups nach der bewährten 3-2-1-1-Methode. So können Sie im Ernstfall z.B. bei einem Ransomware-Angriff auf geeignete Sicherheitsprotokolle zurückgreifen.

4 Erwägen Sie den Einsatz von Technologien zur Verhaltensanalyse, um verdächtige Aktivitäten an den Endpunkten zu erkennen.

5 Bewahren Sie Offline-Kopien der Daten auf (wie vom FBI, der CISA und dem NCSC UK empfohlen).

6 Prüfen Sie, ob Disk, Tape (lokal oder als Cold Storage in der Cloud) bzw. Cloud/Object Storage die beste Recovery-Methode gemäß Ihren SLAs darstellt.

In den nächsten fünf bis zehn Jahren müssen wir uns gemeinsam dafür engagieren, die Cyberwelt zu schützen, und Unternehmen jeder Größe die Möglichkeit geben, solide proaktive (und möglichst auch kosteneffiziente) Strategien und Richtlinien zu implementieren. Je raffinierter Kriminelle ihre Angriffe gestalten, desto dringender benötigen wir Technologien wie maschinelles Lernen (ML) oder künstliche Intelligenz (KI), um ihnen mithilfe fortschrittlicher Sicherheitsanalysen den entscheidenden Schritt voraus zu bleiben. Natürlich erfordert eine solche Risikominderung den Einsatz mehrerer Technologien.

Es gibt keine einzelne Lösung, die einen ausreichenden Schutz gegen die Wucht der Attacken bieten kann. Eine Absicherung gegen Ransomware muss aus mehreren Ebenen bestehen. Parallel dazu brauchen wir zur Eindämmung dieser Machenschaften andere Prozesse, Technologien, Backup-Methoden und Einstellungen.

Auch Investitionen in Schulungen sind unumgänglich. Und weil es sich bei diesen Angriffen längst nicht mehr um isolierte Einzelfälle handelt, kann nicht länger jeder für sich allein dagegen ankämpfen. Wir müssen das Wissen über unsere unerfreulichen Ransomware-Erfahrungen dokumentieren und weitergeben, um gemeinsam den Ausweg aus dieser Cyberkrise zu finden.

Risikominderung setzt mehrere Technologien voraus. Eine Absicherung gegen Ransomware muss aus mehreren Ebenen bestehen.

Ein mehrstufiger Ansatz bietet die Möglichkeit, Daten je nach Anforderung und Abschnitt des Lebenszyklus auf verschiedene Ebenen zu verschieben. Dies ist die kosteneffizienteste Methode zur Implementierung einer Strategie, mit der Sie Ihre Daten vor Ransomware schützen und nach einem Angriff wiederherstellen. Als Experte für Datensicherung verfügt Quantum über einzigartige Lösungen, mit denen Sie die Kosten im Griff behalten und gleichzeitig sicherstellen, dass Ihre Daten umfassend isoliert und gesichert sind oder sich hinter einer physischen „Air-Gap" befinden, die sie wirksam vor Angriffen schützt. Ransomware kann keine Daten infiltrieren, die sie nicht erreichen kann.

Weitere Informationen zu den Quantum Lösungen für das Recovery nach einem Ransomware-Angriff erhalten Sie unter: https://www.quantum.com/de/solution/ransomware-recovery/

Quantum®

ÜBER QUANTUM

Quantum Technologien und Services helfen Kunden bei der Erfassung, Erstellung und gemeinsamen Nutzung von digitalen Inhalten – sowie deren Vorhaltung und Sicherung für Jahrzehnte bei minimalen Kosten. Die Plattformen von Quantum liefern die schnellste Performance für hochauflösende Videos, Bilder und industrielles IoT und umfassen Lösungen für jede Phase im Datenlebenszyklus – vom hochperformanten Ingest über Echtzeit-Zusammenarbeit und -Analyse bis zur kostengünstigen Archivierung. Führende Unterhaltungskonzerne, Wissenschaftler, Behörden, Unternehmen und Cloud-Anbieter aus aller Welt setzen täglich auf Quantum, um die Welt zu einem freundlicheren, sichereren und intelligenteren Ort zu machen. Weitere Informationen erhalten Sie unter **www.quantum.com/de**.

www.quantum.com/de • + 49 (0)89 94303-0

ST02349G-v01 Mär 2021