Verbessern Sie Ihre Ransomware-Abwehr

Die Folgen von Ransomware im Gesundheitswesen

Mario Zimmermann

Regional Director Austria
Veeam Software

Markus Schober

Senior Systems Engineer
Veeam Software

Fakt ist:
Cybersicherheit **IST** Patientensicherheit

Das Gesundheitswesen befindet sich an einem Scheideweg. Wir behandeln Menschen, und die müssen uns vertrauen. Sie brauchen die Gewissheit, dass wir uns gut um sie kümmern, immer die besten Entscheidungen für sie treffen und ihre Daten genauso sorgsam behandeln wie ihre Krankheiten.

Führungskraft aus dem Gesundheitswesen

Der softwaredefinierte Ansatz von Veeam sorgt dafür, dass Sie sich nicht an einen Hardwareanbieter binden müssen. Unsere Lösungen funktionieren in Ihrer vorhandenen Architektur vor Ort oder in der Cloud.
Veeam unterstützt Sie dabei, Ausfallzeiten und Datenverlust zu minimieren, und bewahrt Sie vor Lösegeldzahlungen.

VEEAM

Agenda

1. Warum das Gesundheitswesen gefährdet ist
2. Ablauf eines Angriffs
3. Sofortmaßnahmen
4. Success Storys von Veeam
5. Veeam-Ressourcen und Marketingmaterial

Ransomware-Trends Gesundheitswesen & Biowissenschaften

Wichtige Trends, die einen anderen, besseren Datenschutz erfordern

Das Gesundheitswesen hat eine ungewöhnlich hohe Fragmentierung: 19,4 Systeme pro Nutzer.

Die steigende Nachfrage nach Telemedizin und remote durchgeführten klinischen Studien belastet die vorhandenen Infrastrukturen.

Mit dem IoT sind im Ökosystem des Gesundheitswesens Tausende ungesicherte Endpunkte entstanden.

Cloud-Workloads, MSP und Managed Services haben die Angriffsfläche vergrößert.

Ransomware-Trends

RaaS
(Ransomware-as-a-Service)

Die digitale Transformation im Gesundheitswesen und in den Biowissenschaften ist in vollem Gange. Doch das digitale Integrieren von Assets und Wissen über lokale und nationale Gesundheitssysteme hinweg steckt noch in den Kinderschuhen.

Double Extortion
(sensible medizinische Daten)

Bei der „doppelten Erpressung" werden die Daten auch an einen externen Speicherort ausgeschleust. Dort können sie für weitere Zwecke verwendet werden, z. B. um die Informationen öffentlich zu machen, wenn keine Zahlung erfolgt.

Supply Chain Attacks

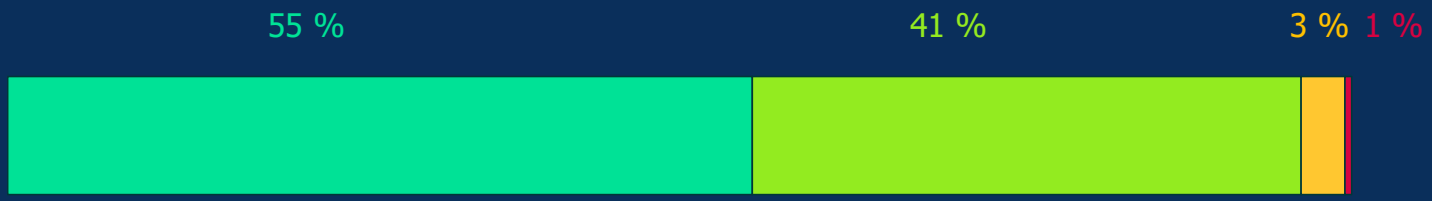
Statt nur ein einzelnes Opfer anzugreifen, wird bei Attacken auf die Lieferkette der Radius vergrößert. Beispielsweise wurde 2022 der MSP Kaseya mit Ransomware angegriffen, wobei mindestens 1.500 seiner Kunden in Mitleidenschaft gezogen wurden.

VEEAM

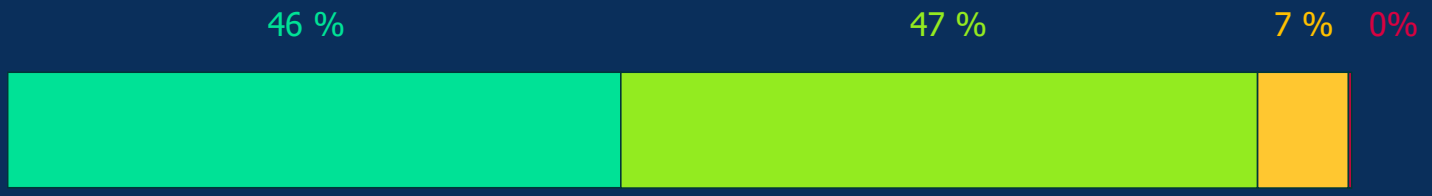
Die „Verfügbarkeitslücke“ im Gesundheitswesen

n = 399 Unternehmen im Gesundheitswesen

Verfügbarkeitslücke
In meinem Unternehmen gibt es eine Lücke zwischen der tatsächlichen Wiederherstellungsdauer und der notwendigen Geschwindigkeit, mit der Anwendungen und damit die Produktivität der Mitarbeiter wiederhergestellt werden müssten.



Sicherheitslücke
In meinem Unternehmen besteht eine Lücke zwischen der Häufigkeit der Datensicherung und dem tolerierbaren Datenverlust im Fall eines Ausfalls.



Stimme vollkommen zu | Stimme zu | Stimme nicht zu | Stimme überhaupt nicht zu

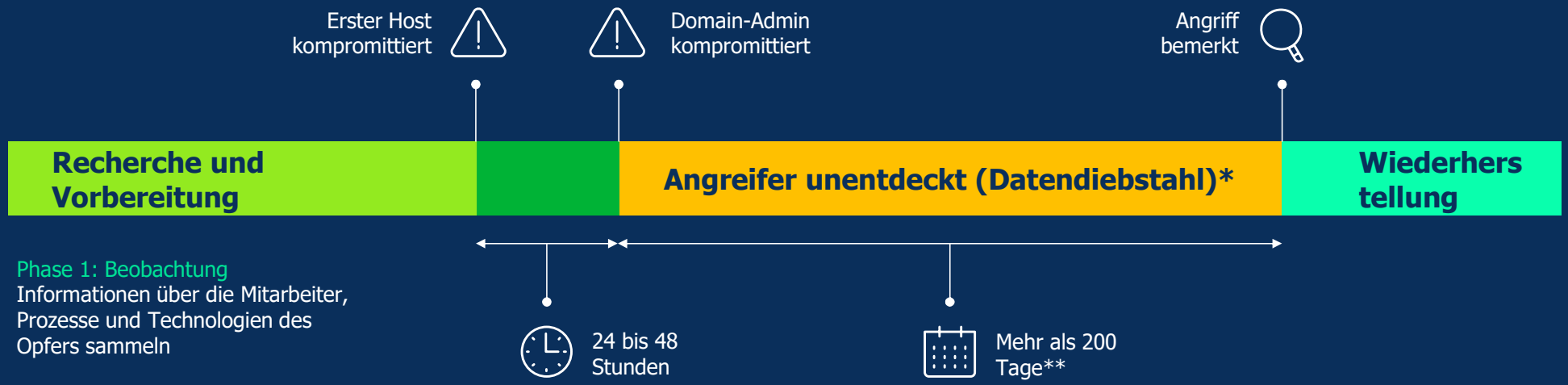
Quelle: **Data Protection Trends Report 2022**
https://vee.am/DPR22

Ablauf eines Angriffs

Phase 2: Einschleichen
Zugang zum Opfer erlangen, ein Klick reicht!

Phase 4: Zugang ausweiten
Unbemerkt herumspionieren und höherwertige Angriffsziele kompromittieren

Phase 6: Lösegeld gefordert!
Daten des Opfers verschlüsseln, Archive/Backups/Daten löschen, Lösegeld fordern



Phase 1: Beobachtung
Informationen über die Mitarbeiter, Prozesse und Technologien des Opfers sammeln

Phase 3: Etablieren
Stützpunkt einrichten, für Redundanz und Hochverfügbarkeit sorgen

Phase 5: Wiederherstellbarkeit vereiteln
Abläufe, Dokumentation und Systeme ändern, um Wiederherstellungsmöglichkeiten zu reduzieren/vereiteln

* Datendiebstahl bezeichnet die unzulässige Datenübertragung von einem Computer.
** Die genaue Dauer variiert je nach Region.

VEEAM

Ransomware in Zahlen

Studie 1200 Unternehmen mit mehr als 3000 Angriffen umfassend

- bei einer von sieben Organisationen werden fast alle Daten (> 80 %) von einem Ransomware-Angriff betroffen sein – ein Hinweis auf eine erhebliche Schutzlücke
- Cyber-Kriminelle zielen bei Cyber-Angriffen fast immer (> 93 %) zuerst auf Backups und in 75 % der Fälle schaffen sie es, die Wiederherstellungsfähigkeit ihrer Opfer zu beeinträchtigen
- 75 % der Unternehmen verlieren einen Teil der Repositories, 39% alle !!
- 80 % der befragten Unternehmen zahlen trotzdem Lösegeld, um einen Angriff zu beenden und Daten wiederherzustellen – ein Anstieg von 4 % im Vergleich zum Vorjahr – obwohl 41 % der Unternehmen eine Do-Not-Pay-Richtlinie zu Ransomware haben
- während 59 % das Lösegeld zahlten und dann ihre Daten wiederherstellen konnten, bekamen 21 % ihre Daten trotzdem nicht von den Cyber-Kriminellen zurück

es geht heute nicht mehr darum, OB ein Unternehmen das Ziel eines Cyber-Angriffs wird, sondern, WANN und WIE OFT !

VEEAM

Key „Take-Aways“

- **Cyber-Versicherungen werden zu teuer**: 21 % der Unternehmen gaben an, dass Ransomware jetzt ausdrücklich von ihren Polizzen ausgeschlossen ist

- **Leitfaden für die Reaktion auf Vorfälle hängen von der Sicherung ab**: 87 % der Unternehmen verfügen über ein Programm zum Risikomanagement, welches ihren Sicherheitsplan vorantreibt, doch nur 35 % sind der Meinung, dass ihr Programm gut funktioniert

- **Die organisatorische Ausrichtung leidet weiterhin:** Obwohl viele Unternehmen Ransomware als Katastrophe ansehen und daher Cyber-Angriffe in ihre Business-Continuity- oder Disaster-Recovery-Planung (BC/DR) einbeziehen, geben 60 % der Unternehmen an, dass sie ihre Backup- und Cyber-Teamaufstellungen noch erheblich verbessern oder komplett überarbeiten müssen, um auf dieses Szenario vorbereitet zu sein

https://www.veeam.com/ransomware-trends-report-2023

VEEAM

Was Sie HEUTE noch tun können

1

Ransomware-Schutz ausweiten

Entwickeln Sie eine umfassende Strategie zum Schutz der Datenverfügbarkeit, damit Sie Ihre Daten und Workloads zuverlässig wiederherstellen können, wenn Sie von Ransomware angegriffen werden.

2

Verbesserung der Repository-Strategie

Vaulting schützt Ihre Daten vor Verlust oder Beschädigung und bietet Versionskontrolle, sodass die Änderungen und unterschiedlichen Versionen der Daten nachverfolgt werden können. Mit Scale-out, Hardening und Air-Gapping realisieren Sie unterschiedliche Sicherheitsstufen.

3

Immutable Objektspeicher

Immutability ist eine leistungsstarke Technik, die Backups vor Ransomware und anderen Bedrohungen schützt, da die Daten dann nicht verändert, abgegriffen oder gelöscht werden können. Beginnen Sie mit Ihren kritischen Workloads.

4

Ransomware Simulation Lab

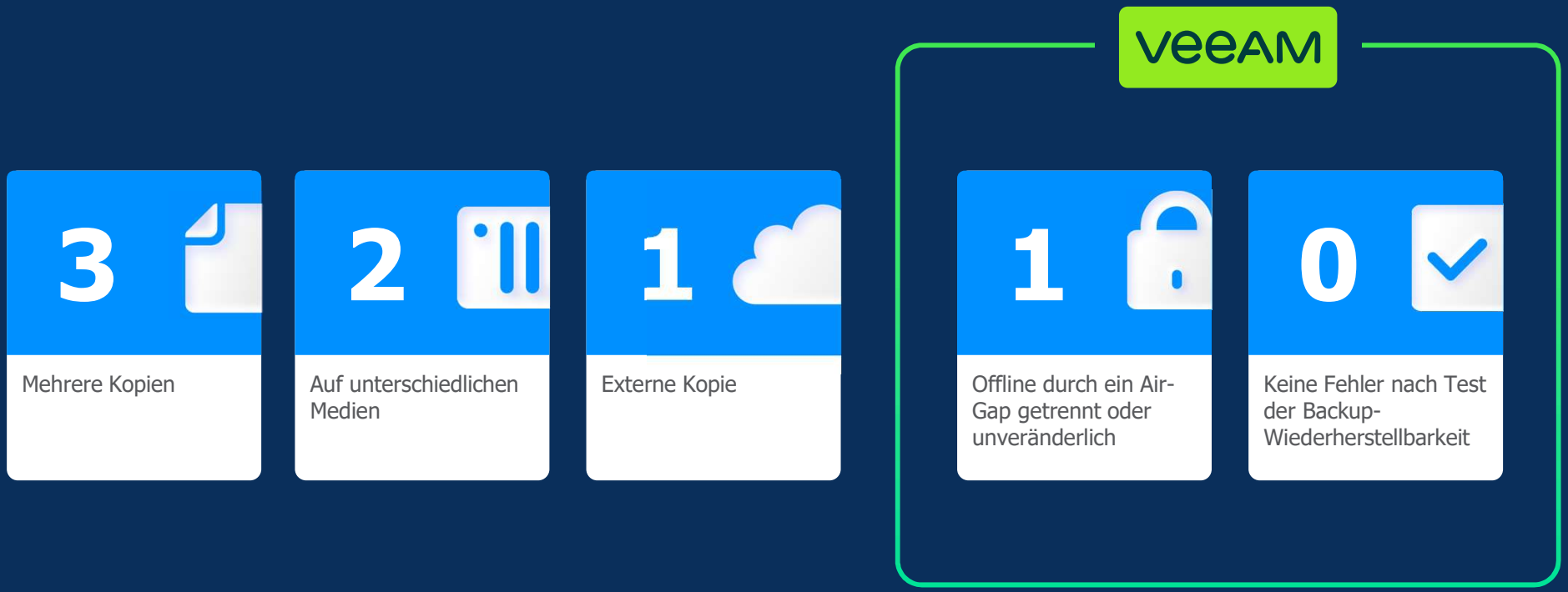
Gewinnen Sie wichtige Erkenntnisse, bevor Sie tatsächlich mit Ransomware angegriffen werden. Mit der Ransomware-Simulation von Veeam können Sie Ihre Verteidigungsplanung weiterentwickeln und schärfen.

VEEAM

1

Ransomware-Schutz ausweiten

Ransomware-Schutz ausweiten



VEEAM

2

Verbesserung Ihrer Repository-Strategie

Verbesserung Ihrer Repository-Strategie

Scale-out-Repository

Ermöglicht eine nahtlose Erweiterung der Kapazität für steigende Datenmengen

Bietet unbegrenzte Kapazität unabhängig vom Speichergerät und physischen Standort der Daten

Ermöglicht Block-, Datei- und Objektspeicherung

Hardened Repository

Bietet zuverlässige Sicherheitsmaßnahmen für die Vertraulichkeit, Integrität und Verfügbarkeit der gespeicherten Daten

Daten werden verschlüsselt gespeichert und übertragen, Multifaktorauthentifizierung wird eingesetzt

Bietet Auditing und Protokollierung für Einhaltung der Compliance und Zuverlässigkeit

Air-Gap-Repository

Wird eingesetzt für vertrauliche Unternehmensdaten oder persönliche Gesundheitsdaten, wenn das Risiko von Datenpannen oder Datendiebstahl hoch ist

Schutzarchitektur, die physisch von allen Netzwerken und sonstigen externen Verbindungen getrennt ist

Häufig Durchführung automatisierter Prozesse für die Datenübertragung in das und aus dem Repository

VEEAM

3

Immutable Objektspeicher

Immutable Objektspeicher

Immutable Objektspeicher gegen Ransomware

Die Unveränderlichkeit der Daten ist ein Muss für die Cybersicherheit und die Business Continuity. Immutable Storage bildet ein „Air-Gap" und sorgt dafür, dass die Daten nur genau einmal geschrieben werden. Das gewährleistet die Integrität der Backups. Da vom Immutable Storage mehrere Kopien vorgehalten werden, ist der Objektspeicher das Repository-Ziel der Wahl für eine kosteneffiziente Speicherung.

- Veeam mit S3-kompatiblem Objektspeicher garantiert die Unveränderlichkeit Ihrer Daten
- Verhindert Verschlüsselung oder Löschung durch Hacker, damit für die Wiederherstellung eine saubere Datenkopie vorhanden ist

VEEAM

4

Ransomware Simulation Lab

Ransomware Simulation Laboratory

Schutz vor Ransomware im Praxistest

Kaum hat die Ransomware zugeschlagen, gleichen Ihre Rechenzentren einem Schlachtfeld. Um sich davor zu schützen, müssen Sie die Verteidigung gegen Ransomware gut trainieren, die Wiederherstellbarkeit umfassend testen und Ihre Business Continuity analysieren.

Bei einem simulierten Ransomware-Angriff sammeln Sie und Ihr Team wertvolle praktische Erfahrungen.

- Echte Angriffs- und Wiederherstellungsszenarien
- Entwicklung umfassender Maßnahmen zum Umgang mit Ransomware-Angriffen
- Empfehlungen für workloadspezifische Schutzmaßnahmen in Multi-Site- und Cloudumgebungen und Informationen zu deren Auswirkungen auf den Angriff
- Informationen zu Ransomware-Benachrichtigungen und deren Einfluss auf Backup-Überprüfungs- und Wiederherstellungsstrategien
- Training für schnelle, zuverlässige Wiederherstellung bei jeglicher Cyberbedrohung

VEEAM

Veeam-Lösungen gegen Ransomware

Schutz vor Ransomware

Sichere **Backups** sind Ihr **Rettungsanker**.

Backup

- Zuverlässige Immutability
- Backup-Überprüfung
- 3-2-1-1-0-Regel

Wiederherstellung

- Skalierbare Sofortwiederherstellung
- Secure Restore
- DR-Orchestrierung

Softwaredefiniert. Keine Festlegung auf proprietäre Hardware.

Veeam Backup & Replication™

AWS AZURE GCP

Veeam ONE™

Veeam Disaster Recovery Orchestrator

VEEAM

Ressourcen zum Schutz vor Ransomware

Ransomware Assessment Kit

Allgemeine Informationen zu Ransomware

Content Library (Executive und Technical)

DOWNLOAD:

Ransomware Trends Report 2023

Der Ransomware Trends Report 2023 ist der aktuellste und umfassendste Forschungsbericht in der Geschichte von Datensicherung und -verfügbarkeit und basiert auf den Erfahrungen von Opfern von Cyberangriffen. Die Befragung, die von einem unabhängigen Marktforschungsunternehmen durchgeführt wurde, umfasst 1.200 Unternehmen aus 14 Ländern und damit Informationen zu fast 3.000 Cyberangriffen.

VEEAM

VEEAM ON TOUR
EXPAND

13. Juni | Linz
14. Juni | Wien

Das Community-Event für Wiederherstellungsexperten

JETZT ANMELDEN