Cove
Data Protection

Ransomware-Fehltritte, die Sie teuer zu stehen kommen können

Whitepaper

N-ABLE™

Ransomware-Fehltritte, die Sie teuer zu stehen kommen können

Katastrophen gibt es in vielerlei Form, aber Cyberangriffe wie Ransomware machen immer wieder Schlagzeilen und entwickeln sich sehr schnell zur besorgniserregendsten Art von Katastrophe. IT-Experten und Anbieter von Managed Services müssen bereit sein, rechtzeitig und angemessen zu reagieren. Das beginnt damit, dass Sie sich über die größten Probleme und möglichen Fehltritte informieren, die den entscheidenden Unterschied machen können.

Cybersicherheitsforscher haben zwischen dem ersten und zweiten Quartal 2022 einen Anstieg der Ransomware-Angriffe um 21 Prozent festgestellt, was auf eine starke Zunahme der Aktivitäten bei drei der aktivsten Organisationen zurückzuführen ist.[1] Die Vereinigten Staaten waren mit fast 40 Prozent aller Vorfälle die am stärksten betroffene Region. Deutschland und das Vereinigte Königreich folgen auf den Plätzen zwei und drei.[1]

Um welche Art von Katastrophe handelt es sich?

Bei herkömmlichen Katastrophen wie Feuer, Überschwemmung oder Hardwareausfällen hat die sofortige Wiederherstellung Vorrang, um die Ausfallzeiten zu minimieren. Auch wenn dies in solchen Situationen immer noch der Fall ist, ist die sofortige Wiederherstellung der Produktionsumgebung im Falle eines Cyberangriffs nicht die beste Option. In diesem Szenario wird Ihr Netzwerk im Wesentlichen zu einem Tatort, was andere Anforderungen als die herkömmliche Notfallwiederherstellung mit sich bringt.

Überlegung	Herkömmliche Katastrophe	Cyberangriff
Datenvolumen	Umfassend, alle Daten	Selektiv, einschließlich grundlegender Dienstleistungen
Wiederherstellung	Standard DW/Failback	Iterativ, selektive Wiederherstellung als Teil der Reaktion auf einen Zwischenfall
Wiederherstellungszeit	Nahezu sofort	Zuverlässig und schnell
Wiederherstellungspunkt	Idealerweise kontinuierlich	Im Durchschnitt ein Tag
Art der Katastrophe	Überschwemmung, Stromausfall, Wetter	Gezielter Cyberangriff
Auswirkungen der Katastrophe	Regional, in der Regel örtlich begrenzt	Global, breitet sich schnell aus
Topologie	Verbunden, mehrere Ziele	Isoliert, zusätzlich zur DR

Die Risiko- und Compliance-Experten von Arcas Risk Management empfehlen mehrere wichtige Best Practices für die Cybersicherheit – in der Post-COVID-Ära mit vermehrter Telearbeit wurde die richtige Art der Datensicherung und des Datenschutzes neben Tools wie **Antivirus oder EDR, Firewalls, 24x7-Sicherheitsüberwachung und dem Einsatz von Multi-Faktor-Authentifizierung** auf die Liste der wesentlichen Maßnahmen gesetzt.

Diese Vorsichtsmaßnahmen sind besonders wichtig, wenn man bedenkt, in welchem Ausmaß Ransomware „kommerzialisiert" wurde. Dadurch hat sich die Zahl der Übeltäter, die Ransomware einsetzen können, über die hochtechnisierten Cyberkriminellen oder Staaten hinaus erweitert. Es wird immer deutlicher, dass sich diese Art von Kriminalität für die Täter auszahlt und dass die Zahlung des Lösegelds nicht immer eine sichere Rückgabe der Daten sicherstellt. Tatsächlich kann Ihre Zahlungsbereitschaft Tür und Tor zu weiteren Angriffen öffnen. Denn Untersuchungen zeigen, dass 80 Prozent der Unternehmen, die ein Lösegeld gezahlt haben, erneut angegriffen wurden – oft durch dieselben Angreifer.[2] Ein weiterer Aspekt, den es zu berücksichtigen gilt, ist, dass Ransomware zunehmend auf die Backup-Infrastruktur abzielt, um Unternehmen die Wiederherstellung zu erschweren und damit die Wahrscheinlichkeit zu erhöhen, dass das Lösegeld gezahlt wird.

Wiederherstellung als Teil der Reaktion auf einen Vorfall

Im Gegensatz zu herkömmlichen Natur- oder physischen Katastrophen sollte Ihr Plan zur Wiederherstellung nach einem Cyberangriff Teil einer umfassenderen Strategie zur Reaktion auf einen Vorfall sein, die viel breiter angelegt ist als nur die Wiederherstellung von einem funktionierenden letzten Backup. Arcas empfiehlt eine Vier-Punkte-Strategie:

Sichtbarkeit: Was Sie nicht sehen können, können Sie auch nicht effektiv bekämpfen. Mit den richtigen Tools können Sie erkennen, wo die Schadsoftware in Ihrer Umgebung lauert, wann sie eingedrungen ist und wie Sie vorgehen können. Eine Möglichkeit dazu sind Tools wie N-able EDR.

Schutz: Schon vor einem Angriff ist es ratsam, Ihre Netzwerkabgrenzung, Ihre widerstandsfähigen Systeme und Ihre gesamte mehrschichtige Sicherheitsstrategie zu überprüfen. Dies kann helfen, sich vor zukünftigen Angriffen zu schützen.

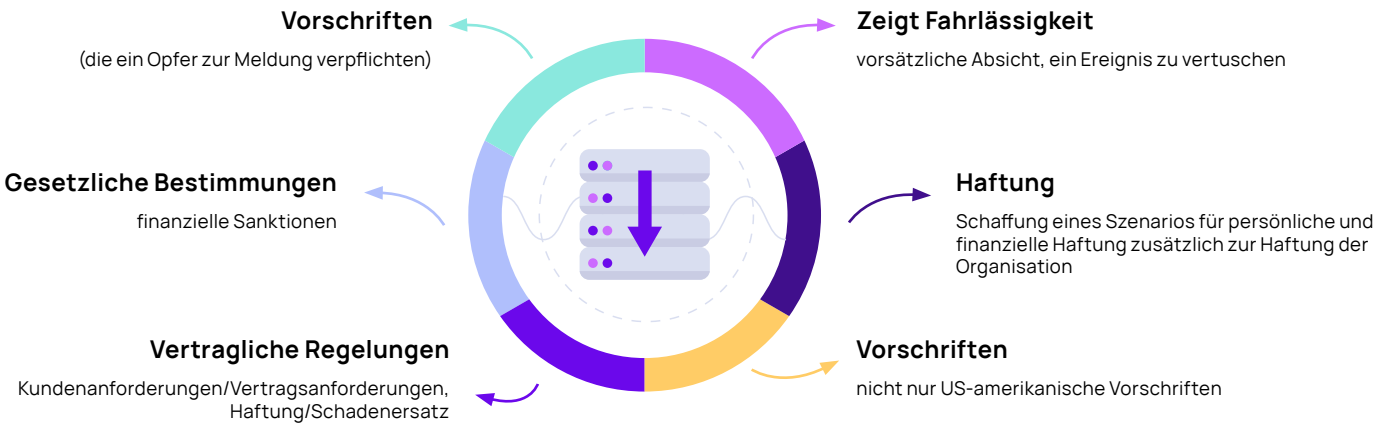
Kontrolle: Sichern Sie Ihre Umgebung mit praktischen Tools wie der Multi-Faktor-Authentifizierung und stellen Sie sicher, dass Sie die Deprovisionierung von ehemaligen Mitarbeitern, Login-Timeouts und ähnliche Maßnahmen durchführen, um offene Türen, die potenzielle Angreifer ausnutzen könnten, so weit wie möglich zu schließen. Außerdem sollten Sie auch die Anwendung des Prinzips des geringsten Privilegs in Erwägung ziehen, indem Sie die Anzahl der Super-User, Sicherheitsbeauftragten oder Administratoren mit API-Zugang begrenzen.

Korrektur: Sobald die unmittelbare Bedrohung bewältigt und neutralisiert ist, ist es wichtig, die Verantwortlichkeiten für die Wiederherstellung zuzuweisen und zu klären.

Allzu oft übersehen IT-Experten, die sich auf die traditionelle Notfallwiederherstellung konzentrieren, die umfassenderen Anforderungen an die Reaktion auf Vorfälle und versäumen es, sich mit Kollegen in anderen Teams abzustimmen. Tabletop-Übungen können bei der Planung helfen und Ihre gesamte Organisation besser auf die praktisch unvermeidlichen Angriffe vorbereiten.

Wie bereits erwähnt, kann eine übereilte „Sofortwiederherstellung“ in der Produktionsumgebung dazu führen, dass erneut Malware in Ihre Umgebung eingeschleust wird. Eine bessere Strategie ist die Wiederherstellung an einem separaten, sekundären Ort, sodass der Betrieb wieder aufgenommen werden kann, ohne die forensische Untersuchung zu beeinträchtigen, indem der „Tatort“ der Ransomware kontaminiert wird.

Sofortige Wiederherstellung kann kostspielig sein
(und kann ein Unternehmen sprichwörtlich Millionen kosten)



Versicherungstechnische Überlegungen

Eine andere Art, Ransomware zu betrachten, ist die Erkenntnis, dass es sich im Grunde um eine Frage des Risikomanagements handelt, nicht nur um eine technische Herausforderung. Diese Erkenntnis hat dazu geführt, dass der Abschluss von Cyber-Versicherungen zunimmt, aber die Qualifizierung für eine Cyber-Versicherung bringt neben den Vorteilen auch zusätzliche Fragen und Anforderungen mit sich.

Ein Cyber-Versicherer wird wahrscheinlich Informationen über Ihre allgemeine Cyber-Hygiene verlangen, einschließlich Sicherheitsrichtlinien, Backups, Zugangskontrolle und Ereignisprotokolle. Er kann Ihnen auch dazu raten, in wichtige Management-Tools zu investieren und ein Krisenreaktionsteam zu gründen, wenn Sie noch keins haben. Außerdem kann er Ressourcen zur Verfügung stellen, um die Mitarbeiter über Phishing und andere Bedrohungen aufzuklären.

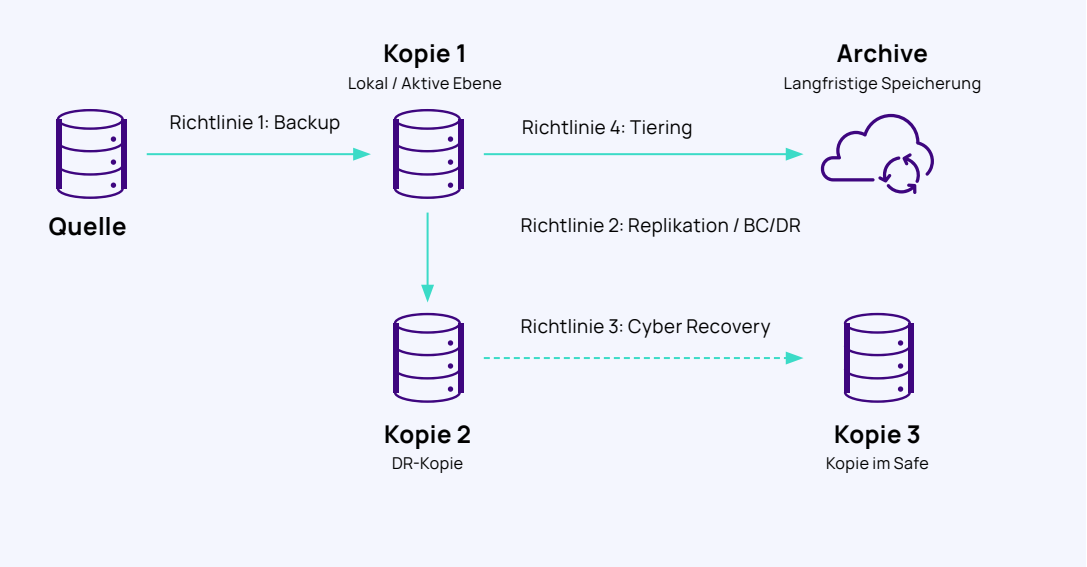
Die Qualifizierung für eine Cyber-Versicherungspolice kann an sich schon Ihre Sicherheitslage verbessern.

Cyber-Resilienz muss nicht komplex sein

Die meisten herkömmlichen Backup-Produkte wurden für physische und natürliche Katastrophen entwickelt, und die Versuche, sie für die moderne Cyber-Recovery-Welt nachzurüsten, haben die Komplexität zusätzlich verstärkt und dazu geführt, dass noch mehr Kopien von Backup-Daten an mehr Orten gespeichert werden. In Wirklichkeit brauchen Sie nicht mehr Kopien oder mehr Komplexität, um auf die Wiederherstellung nach einem Ransomware-Angriff vorbereitet zu sein. Wenn Sie sich für eine Cloud-first-Architektur für die Datensicherheit entscheiden, können Sie Ihre Anfälligkeit verringern, indem Sie die Angriffsfläche des Netzwerks verkleinern und gleichzeitig Ihren Wiederherstellungsprozess vereinfachen.

Ältere Backup-Produkte wurden für die lokale Sicherung entwickelt, d. h. sie speichern die primären Sicherungskopien im lokalen Netzwerk. Die beliebte „3-2-1"-Datensicherheitsstrategie führte zur Replikation oder zum Tiering auf einen zweiten Speicherort. Als nächstes wurden Standby-Kopien an einem besonders gesicherten Ort gelegt, um eine Cyber-Recovery vorzubereiten. Als dann die Vorteile der Cloud-Speicherung für die Ausfallsicherheit erkannt wurden, fügten viele Backup-Anbieter die Möglichkeit hinzu, eine nachgelagerte Kopie in der Cloud zu speichern. Diese Verkettung von Ereignissen hat zu einer komplexen Mischung von Richtlinien geführt, die eine Koordinierung und einen beträchtlichen Zeitaufwand seitens der Mitarbeiter erfordern, um alle beweglichen Teile zu verwalten.

Der traditionelle Ansatz – und was er für DR bedeutet



Erwägungen zum Schutz:

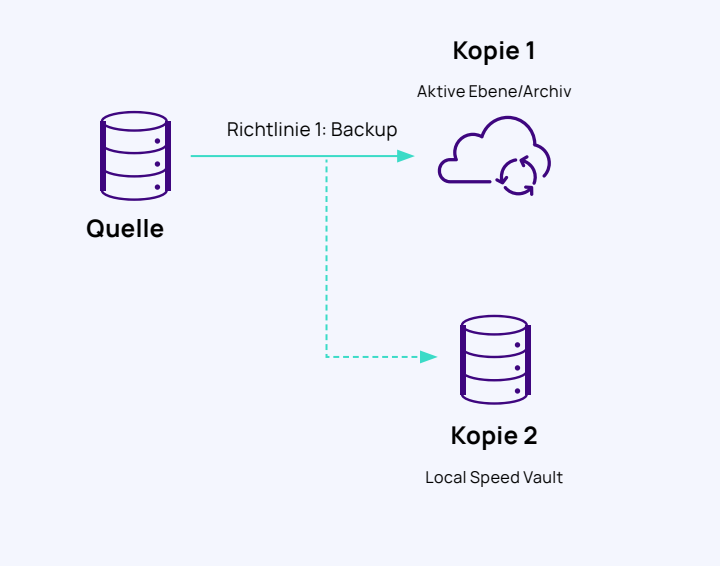
- Wie koordiniere ich die vier Richtlinien?
- Wer verwaltet das und wie viele Leute brauche ich?
- Benötige ich bis zu vier Zielorte?
- Koordinierung von Patches?
- Welche Kopien sollten unveränderlich sein?
- Wie schütze ich die Backup-Infrastruktur im primären Netzwerk?

Erwägungen zur Wiederherstellung:

- Wie kann ich ein DR/IR-Runbook erstellen, das dies abdeckt?
- Eine Tabletop-Übung in Erwägung ziehen.
- Wiederherstellung des Backup-Katalogs im Falle einer Kompromittierung in der Produktion?

Im Gegensatz dazu sendet eine moderne Cloud-first-Architektur jede Sicherung standardmäßig direkt in die Cloud und speichert die primären Sicherungskopien außerhalb des lokalen Netzwerks, sodass sie für Ransomware unerreichbar sind. Sie können eine sekundäre lokale Kopie für eine schnellere Wiederherstellung aufbewahren, aber selbst mit diesem Zusatz vereinfacht diese Methode Ihre Richtlinien drastisch und reduziert die Betriebskosten.

Ein anderer Ansatz ... und was er für DR bedeutet



Erwägungen zum Schutz:

- Vereinfachte Richtlinien
- Reduzierte Komplexität und geringerer Verwaltungsaufwand
- Verlagerung des Schwerpunkts auf echte DR/IR-Bereitschaft
- Verringerung der Anzahl von Kopien ››› Kostenreduzierung
- Vorteile von Patching als Service
- Standardmäßige Offsite-Kopien

Erwägungen zur Wiederherstellung:

- Vereinfachen Sie Ihre DR-Topologie und Ihren Prozess ››› Vereinfachen Sie Ihr DR/IR-Runbook
- Flexible Wiederherstellungsoptionen für eine große Bandbreite von Katastrophen
- Reduzierte Angriffsfläche, um die Wahrscheinlichkeit zu verringern, Ihren Backup-Katalog neu erstellen zu müssen

Verringern Sie die Größe Ihrer Angriffsfläche

Cyberkriminelle versuchen, sich über eine Vielzahl von Methoden Zugang zu Ihrem Netzwerk zu verschaffen. Es gibt mehrere häufig genutzte Angriffsvektoren, für die sich traditionelle Backup-Anwendungen vor Ort als anfällig erwiesen haben. Einige Gruppen und Techniken durchsuchen das lokale Netzwerk gezielt nach Backup-Dateien bekannter Hersteller und löschen oder verschlüsseln diese, wodurch ein wichtiger Weg zur Wiederherstellung abgeschnitten wird[3]. Alternativ können sie auch den Backup-Anwendungsserver löschen oder deaktivieren.

Wenn Sie sich für Cloud-first-Datensicherheit als Service entscheiden, können Sie Ihre Anfälligkeit für Ransomware-Angriffe auf drei wichtige Arten verringern:

- Indem Sie Ihre primären Sicherungskopien in unserer privaten Cloud speichern, außerhalb des lokalen Netzwerks und weit außerhalb der Reichweite von Ransomware.
- Da es sich um eine SaaS-Anwendung handelt, gibt es keinen lokalen Backup-Server im Netzwerk.
- Die obligatorische Zwei-Faktor-Authentifizierung schränkt den unbefugten Zugriff auf Ihre Backups ein.

››› **Wenn Sie mehr über die Empfehlungen von Arcas Risk Management** zur Vorbereitung auf Ransomware erfahren möchten, sehen Sie sich dieses On-Demand-Webinar an: https://youtu.be/ON28_27swlo.

››› **Wenn Sie mehr darüber erfahren möchten, wie die Cloud-first-Datensicherheitsarchitektur als Service von Cove Data Protection** Ihre Angriffsfläche reduziert, sehen Sie sich dieses kurze Video an: https://youtu.be/c-rHzx-qqTM.

Über N-able

N-able bietet MSPs und IT-Serviceanbietern leistungsstarke Software zur Überwachung, Verwaltung und Absicherung von IT-Infrastrukturen und Netzwerken. Unser Angebot umfasst eine skalierbare Plattform, eine sichere Infrastruktur, Tools für die einfachere Verwaltung komplexer IT-Umgebungen und Ressourcen für die digitale Transformation. Wir unterstützen unsere Partner in jeder Wachstumsphase beim Schutz ihrer Kunden sowie beim Ausbau ihres Angebots – durch das ständig wachsende flexible Portfolio an Integrationen führender Anbieter. n-able.com/de

[1]https://www.digitalshadows.com/blog-and-research/ransomware-in-q2-2022-ransomware-is-back-in-business

[2]https://www.infosecurity-magazine.com/news/most-ransomware-victims-hit-again/

[3]https://threatpost.com/conti-ransomware-backups/175114/