Synology®

Schützen Sie sich vor Ransomware

Ransomware-Angriffe werden Unternehmen geschätzt allein im Jahr 2023 insgesamt 8 Billionen US-Dollar kosten.[1] Datensicherungspläne mit schneller Wiederherstellung sind daher entscheidend, um die Bedrohung durch Ransomware und andere Arten von Cyberkriminalität einzudämmen.

Date 13. Okt. 2023

Backups - der essentielle Bestandteil Ihrer Cyber-Security-Strategie

Wenn Daten durch böswillige Löschung oder Änderung verloren gehen, können Sie mit Hilfe von Backups geschäftskritische Daten wiederherstellen und kostspielige Ausfallzeiten vermeiden. Nutzen Sie die Backup-Lösungen von Synology, um eine Sicherungsstrategie für Ihre gesamte IT-Infrastruktur zu entwickeln.

Kompletter Schutz

Sichern Sie sowohl die Endpunkte als auch die primären Backups, um mehrere Sicherheitsnetze für Ihre Daten zu schaffen.

Schnelle Wiederherstellung

Mit sofortigen Wiederherstellungsoptionen reduzieren Sie die Ausfallzeiten auf ein Minimum, wenn eine Katastrophe eintritt.

Unveränderlicher Speicher

Verhindern Sie unbefugte Änderungen an Daten und Schnappschüssen.

Lizenzfreie Backups

Sichern Sie so viele Daten, wie Ihr Speicherplatz erlaubt, ohne Einschränkungen oder versteckte Gebühren.

Zentraler Schutz vor Ransomware

Konsolidieren Sie Backups von all Ihren Workstations, PCs, Servern, virtuellen Maschinen und Cloud-Anwendungen. Optimieren Sie den Speicherverbrauch und vermeiden Sie Bandbreitenengpässe mit Datendeduplizierung und inkrementellen Backup-Technologien. https://www.synology.com/dsm/solution/infrastructure

PC und Server

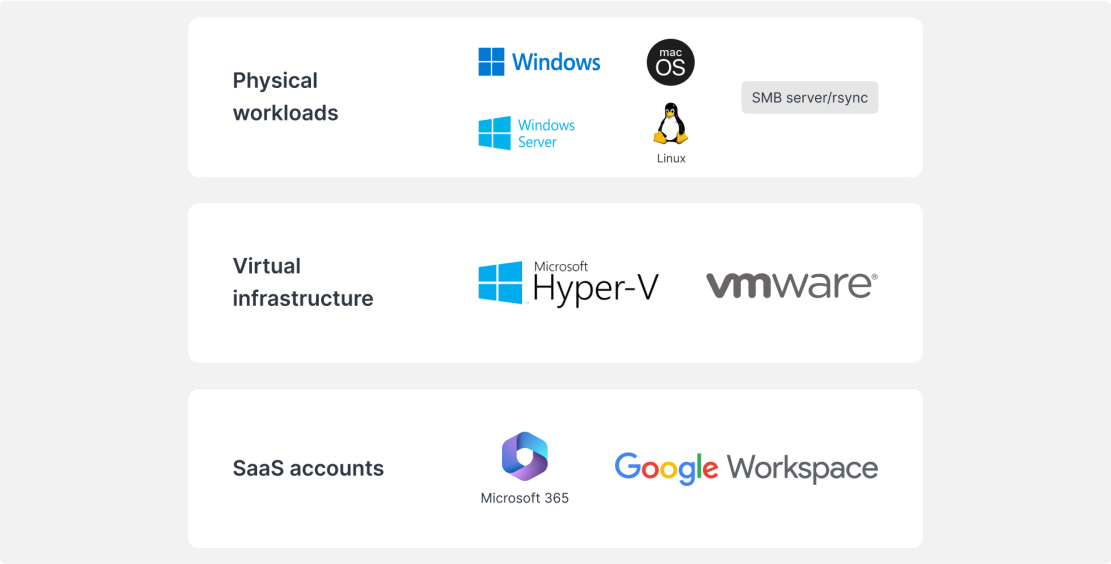
Schützen Sie Endgeräte im Falle von Cyber-Angriffen mit umfassenden Bare-Metal-Backups und flexibler Wiederherstellung auf Dateiebene.

Virtuelle Infrastruktur

Sichern Sie VMware® vSphere™, Microsoft® Hyper-V® VMs und LUNs mit leistungsstarken Technologien zur Datenreduzierung.

SaaS-Konten

Aktivieren Sie kontinuierlichen Schutz für in der Cloud gespeicherte Daten mit automatischer Erkennung neu hinzugefügter Konten.



Effiziente Wiederherstellung

Minimieren Sie Ausfallzeiten für kritische Produktionssysteme durch die schnelle Wiederherstellung von Backup von einem lokalen oder externen Synology System.

RTO nahe Null

Montieren Sie die Datensicherungs-Images auf VMware®, Hyper-V® oder Synology Virtual Machine Manager, um die Arbeit so schnell wie möglich wieder aufzunehmen. Stellen Sie VMs auf einem alternativen Hypervisor wieder her, um Serviceunterbrechungen zu vermeiden.

Minimales RPO

Konfigurieren Sie die Häufigkeit der Datensicherungen nach Ihren Bedürfnissen und minimieren Sie die Datenmenge, die bei einem Angriff betroffen sein könnte. Sichern Sie Systeme schnell dank inkrementellen Backups und Deduplizierungstechnologie.

Intuitiver Betrieb

Lassen Sie Ihre Mitarbeiter E-Mails, Kontakte und Dateien über ein praktisches Portal durchsuchen und in der Vorschau anzeigen, bevor sie sie wiederherstellen. Das entlastet die IT-Teams.

Fügen Sie eine zusätzliche Sicherheitsebene hinzu

Halten Sie sich an die 3-2-1-Backup-Strategie, indem Sie einen dritten Datensatz außerhalb des Standorts oder in der Cloud speichern. So schützen Sie Ihre Daten vor Feuer, Naturkatastrophen oder Diebstahl.

Zu externen Servern

Speichern Sie Sicherungen auf einem Synology-Server an einem zweiten Standort als Schutz vor physischen Schäden und replizieren Sie unveränderliche Schnappschüsse für zusätzlichen Schutz vor Ransomware.

In die Cloud

Erstellen Sie Backup-Kopien bei einem großen Cloud-Speicheranbietern Ihrer Wahl. So schützen Sie Ihre Daten durch client-seitige AES-256-Verschlüsselung vor unberechtigtem Zugriff. https://c2.synology.com/storage/nas

Unternehmen vertrauen branchenweit Synology

„Synology [...] ermöglichte es uns, die Ausgaben für Server-Hardware zu reduzieren [...] und gleichzeitig Infrastruktur- und Workstation-Backups, Systemprotokollierung und Dateiverwaltung viel einfacher zu gestalten.“
https://www.synology.com/company/case_study/Investortools

„Dank Active Backup for Business sind alle unsere Backups jetzt zentralisiert und rund um die Uhr verfügbar, was uns hilft, Ausfallzeiten zu minimieren und die FERPA-Vorschriften einzuhalten.“
https://www.synology.com/company/case_study/University_of_Washington

„[...] Active Backup for Business hat eine erstaunliche Datensicherungs-Geschwindigkeit und wirkt Wunder beim Löschen von doppelten Daten - es hat nur 28 TB der insgesamt 58 TB auf dem Server verbraucht. [...]“
https://www.synology.com/company/case_study/SHISEIDO_Taiwan_ABB

„[...] Active Backup for Business [...] ermöglicht uns die Zentralisierung und Verwaltung aller Sicherungsaufgaben über eine einzige Konsole. Die schnelle und zuverlässige Wiederherstellung stellt außerdem den unterbrechungsfreien Betrieb sicher.“
https://www.synology.com/company/case_study/UNESCO

Häufig gestellte Fragen

Was ist Ransomware?

Ransomware ist eine Art von Malware, die die Dateien der Opfer verschlüsselt. Die Angreifer verlangen dann ein Lösegeld, um den Datenzugriff wiederherzustellen, und drohen oft damit, die Daten dauerhaft zu zerstören, wenn kein Lösegeld gezahlt wird. Ransomware-Angriffe können sehr störend sein und erhebliche finanzielle Verluste für Einzelpersonen und Unternehmen verursachen. Es ist wichtig, dass Sie sich und Ihre Geräte vor Ransomware schützen, indem Sie z. B. Ihre Software auf dem neuesten Stand halten und regelmäßig Sicherungskopien Ihrer Dateien erstellen.

Welche Arten von Ransomware gibt es?

Es gibt viele verschiedene Arten von Ransomware, und es werden ständig neue Stämme entwickelt. Zu den häufigsten Arten von Ransomware gehören:

- **Verschlüsselnde Ransomware** – Die häufigste Art von Ransomware verschlüsselt die Dateien des Opfers, so dass sie ohne den Entschlüsselungsschlüssel nicht zugänglich sind. Die Angreifer verlangen dann eine Lösegeldzahlung im Austausch für den Schlüssel
- **Locker-Ransomware** – Eine Art von Ransomware sperrt die Opfer von ihrem Computer aus, indem sie die Anmeldedaten ändert oder eine Nachricht anzeigt, die das Opfer am Zugriff auf sein System hindert. Die Angreifer verlangen dann eine Lösegeldzahlung, um den Computer freizuschalten.
- **Ransomware-as-a-Service (RaaS)** – Ein Geschäftsmodell, bei dem Angreifer anderen Personen oder Gruppen, die Angriffe durchführen wollen, Ransomware anbieten. Erstere stellen in der Regel die Ransomware bereit und wickeln die Zahlungen ab, während letztere einen Prozentsatz der Lösegeldzahlungen erhalten
- **Scareware** – Ransomware, die die Opfer zur Zahlung des Lösegelds zwingen soll. Dabei werden in der Regel gefälschte Sicherheitswarnungen oder Nachrichten angezeigt, die behaupten, der Computer des Opfers sei mit einem Virus infiziert. Der Angreifer verlangt dann die Zahlung eines Lösegelds, um die vermeintliche Infektion zu entfernen.

Wie verbreitet sich Ransomware?

Ransomware verbreitet sich in der Regel über Phishing-E-Mails oder durch Ausnutzung von Schwachstellen in einem Computersystem. Bei einem Phishing-Angriff sendet ein Angreifer eine E-Mail, die scheinbar von einer legitimen Quelle stammt, z. B. von einer Bank oder einem bekannten Unternehmen. Die E-Mail enthält oft einen Link oder einen Anhang, der, wenn er angeklickt wird, die Ransomware auf dem Computer des Opfers installiert. Das Ausnutzen von Schwachstellen in einem System ist ähnlich – mit dem Unterschied, dass der Angreifer eine Sicherheitslücke im System nutzt, um die Ransomware ohne das Wissen des Opfers zu installieren. In jedem Fall kann sich die Ransomware, sobald sie installiert ist, schnell auf andere Computer im selben Netzwerk ausbreiten.

Was ist der typische Ablauf eines Ransomware-Angriffs?

Ein Ransomware-Angriff läuft in der Regel in folgenden Schritten ab:

1. Der Angreifer verschafft sich Zugang zum Computer des Opfers, indem er entweder eine Phishing-E-Mail verschickt oder eine Sicherheitslücke im System ausnutzt
2. Sobald der Angreifer Zugriff auf den Computer des Opfers hat, installiert er die Ransomware auf dem System
3. Die Ransomware verschlüsselt dann die Dateien des Opfers und macht sie für den Benutzer unzugänglich
4. Der Angreifer fordert dann ein Lösegeld vom Opfer, normalerweise in Form einer digitalen Währung wie Bitcoin, im Austausch für den Entschlüsselungsschlüssel, der die verschlüsselten Dateien entsperrt
5. Wenn das Opfer das Lösegeld bezahlt, stellt der Angreifer den Entschlüsselungsschlüssel zur Verfügung und das Opfer kann wieder auf seine Dateien zugreifen. Es gibt jedoch keine Garantie dafür, dass der Angreifer den Schlüssel tatsächlich zur Verfügung stellt, und selbst wenn dies der Fall ist, können die Dateien des Opfers durch den Verschlüsselungsprozess beschädigt oder beschädigt werden.

Es ist wichtig zu wissen, dass es viele Variationen dieses Prozesses gibt und dass nicht alle Ransomware-Angriffe genau diese Schritte befolgen. Bei einigen Angriffen geht es beispielsweise gar nicht um die Verschlüsselung von Dateien, bei anderen um andere Formen der Erpressung.

Wie kann ich Ransomware bekommen?

Es gibt mehrere Möglichkeiten, wie Sie Ransomware bekommen können. Eine der häufigsten Methoden ist das Klicken auf einen bösartigen Link oder Anhang in einer Phishing-E-Mail. Diese Art von E-Mail ist so gestaltet, dass sie legitim aussieht und oft den Anschein erweckt, von einem bekannten Unternehmen oder einer Organisation zu stammen. Wenn Sie auf den Link oder die Anlage klicken, wird die Ransomware auf Ihrem Computer installiert. Eine weitere Möglichkeit, Ransomware zu erhalten, ist der Besuch einer kompromittierten Website. Diese Websites wurden von Angreifern gehackt, die einen Code eingefügt haben, der die Ransomware automatisch auf Ihrem Computer installiert, wenn Sie die Website besuchen. Sie können Ransomware auch erhalten, indem Sie infizierte Dateien aus dem Internet herunterladen. Dies kann passieren, wenn Sie eine Datei von einer verdächtigen Website herunterladen oder wenn Sie eine Datei herunterladen, die von jemandem freigegeben wurde, den Sie nicht kennen. Kurz gesagt, es ist wichtig, beim Surfen im Internet vorsichtig zu sein und es zu vermeiden, auf Links zu klicken oder Dateien von unbekannten Quellen herunterzuladen. Dies kann Sie vor Ransomware und anderen Arten von Malware schützen.

Wer sind die Ziele von Ransomware?

Ransomware-Angriffe können jeden treffen, der einen Computer oder ein anderes mit dem Internet verbundenes Gerät benutzt. Einige Gruppen werden jedoch eher zur Zielscheibe als andere. Ransomware-Angriffe zielen beispielsweise häufig auf Unternehmen ab, da diese oft über wertvollere Daten verfügen und eher bereit sind, Lösegeld zu zahlen, um sie wiederzuerlangen. Krankenhäuser, Schulen und andere Organisationen, die wichtige Dienste anbieten, sind ebenfalls häufige Ziele, da ein Ransomware-Angriff ihren Betrieb stören und das Leben von Menschen gefährden kann. Auch Einzelpersonen können Ziel von Ransomware-Angriffen sein. In diesen Fällen versuchen die Angreifer möglicherweise, Geld von den Opfern zu erpressen, indem sie drohen, ihre persönlichen Dateien zu löschen oder sensible Informationen zu veröffentlichen, wenn kein Lösegeld gezahlt wird. Die Ziele von Ransomware-Angriffen werden oft nach dem Wert ihrer Daten und ihrer Bereitschaft ausgewählt, ein Lösegeld zu zahlen, um sie zurückzubekommen.

Welche Risiken birgt die Bezahlung von Ransomware?

Die Zahlung eines Lösegelds an einen Ransomware-Angreifer scheint der einfachste Weg zu sein, um Ihre Dateien zurückzubekommen, aber es kann tatsächlich eine sehr riskante Entscheidung sein. Die Zahlung eines Lösegelds birgt mehrere Risiken, unter anderem:

- Es gibt keine Garantie dafür, dass der Angreifer den Entschlüsselungsschlüssel tatsächlich bereitstellt. In vielen Fällen erhalten die Opfer, die das Lösegeld zahlen, den Schlüssel nie und können nicht auf ihre Dateien zugreifen
- Die Zahlung des Lösegelds kann die Angreifer ermutigen, ihre Angriffskampagne fortzusetzen. Wenn die Angreifer wissen, dass die Opfer bereit sind, das Lösegeld zu zahlen, ist die Wahrscheinlichkeit größer, dass sie in Zukunft weitere Angriffe durchführen
- Durch die Zahlung des Lösegelds werden Sie möglicherweise zum Ziel künftiger Angriffe. Wenn der Angreifer weiß, dass Sie bereit sind, ein Lösegeld zu zahlen, ist es wahrscheinlicher, dass er es in Zukunft auf Sie abgesehen hat.
- Die Zahlung des Lösegelds kann illegal sein. In einigen Fällen kann die Zahlung eines Lösegelds an eine kriminelle Organisation als eine Form der Finanzierung von Terrorismus oder anderen illegalen Aktivitäten angesehen werden

Auch wenn die Zahlung des Lösegelds der einfachste Weg zu sein scheint, um Ihre Dateien wiederherzustellen, kann dies eine sehr riskante Entscheidung sein. Es ist wichtig, dass Sie die Risiken sorgfältig abwägen, bevor Sie eine Entscheidung treffen.

Welche Kosten entstehen durch Ransomware?

Die Kosten eines Ransomware-Angriffs können je nach Art der verwendeten Ransomware, der Anzahl der verschlüsselten Dateien und der Effektivität des Angriffs stark variieren. In einigen Fällen können die Kosten eines Ransomware-Angriffs relativ gering sein, da die Angreifer nur ein paar hundert Dollar Lösegeld verlangen. In anderen Fällen können die Kosten sehr viel höher sein, da die Angreifer Tausende von Dollar oder sogar mehr für die Wiederherstellung des Zugriffs auf die Dateien des Opfers verlangen. Zusätzlich zu den direkten Kosten, die mit der Zahlung eines Lösegelds verbunden sind, können Ransomware-Angriffe auch erhebliche indirekte Kosten verursachen. So kann beispielsweise ein Ransomware-Angriff zu Ausfallzeiten und Produktivitätsverlusten führen, was wiederum Umsatz- und Einkommensverluste zur Folge haben kann. Sie können auch den Ruf eines Unternehmens und das Vertrauen der Kunden schädigen, was sich langfristig negativ auf das Geschäft auswirken kann. Diese indirekten Kosten sind oft viel höher als das Lösegeld selbst.

Welches sind die Symptome von Ransomware?

Die Symptome eines Ransomware-Angriffs können je nach der Art der verwendeten Ransomware variieren. Zu den häufigsten Symptomen gehören jedoch:

- Ihre Dateien sind verschlüsselt und Sie können nicht auf sie zugreifen
- Sie erhalten eine Nachricht vom Angreifer, in der er ein Lösegeld für den Entschlüsselungsschlüssel fordert
- Sie sehen unbekannte Programme oder Prozesse auf Ihrem Computer laufen
- Ihr Computer wird langsam oder reagiert nicht mehr
- Ihr Computer zeigt ungewöhnliche Fehlermeldungen oder Pop-up-Fenster an

Wenn Sie den Verdacht haben, dass Ihr Computer mit Ransomware infiziert wurde, müssen Sie schnell handeln. Trennen Sie Ihren Computer vom Internet, um die Ausbreitung der Ransomware zu verhindern.

Wie kann man Ransomware-Angriffen vorbeugen?

Es gibt mehrere Maßnahmen, die Sie ergreifen können, um Ransomware-Angriffe zu verhindern, darunter:

- Verwenden Sie seriöse Antiviren- oder Sicherheitssoftware und halten Sie sie auf dem neuesten Stand. Dies kann dazu beitragen, Ihren Computer vor Ransomware und anderen Arten von Malware zu schützen
- Seien Sie vorsichtig beim Öffnen von E-Mail-Anhängen oder Links. Ransomware wird oft über Phishing-E-Mails verbreitet, daher ist es wichtig, dass Sie vorsichtig sind, worauf Sie klicken
- Halten Sie Ihr Betriebssystem und andere Software auf dem neuesten Stand. Software-Updates enthalten oft Sicherheits-Patches, die Ihren Computer vor Ransomware und anderen Bedrohungen schützen können
- Sichern Sie Ihre Dateien regelmäßig. Dies kann zum Schutz Ihrer Daten beitragen, wenn Ihr Computer mit Ransomware infiziert ist. Stellen Sie sicher, dass Sie eine der empfohlenen Datensicherungs-Strategien einhalten, wie z. B. die 3-2-1 Datensicherungs-Strategie
- Seien Sie sich der Risiken von Ransomware bewusst und klären Sie andere in Ihrem Unternehmen über diese Bedrohungen auf. Dies kann dazu beitragen, Ransomware-Angriffe zu verhindern und es einfacher machen, sie zu erkennen und auf sie zu reagieren, wenn sie doch auftreten

Der beste Weg, Ransomware-Angriffe zu verhindern, besteht darin, wachsam zu sein und Maßnahmen zum Schutz Ihres Computers und Ihrer Daten zu ergreifen. Dies kann dazu beitragen, das Risiko eines Ransomware-Angriffs zu verringern und die Wiederherstellung nach einem solchen Angriff zu erleichtern.

Wie kann Synology mich vor Ransomware schützen?

Präventive Maßnahmen sind unerlässlich, um sich vor Ransomware zu schützen. Nutzen Sie dazu zusätzlich zu Ihrer Antivirensoftware folgende Synology Lösungen.

- **Zugriff verhindern** – Reduzieren Sie die Verbreitung von Ransomware, indem Sie Datei-, Anwendungs- und Zugriffsberechtigungen festlegen und sichere Anmeldedaten mit Secure SignIn und C2 Password konfigurieren.
- **Geräte schützen** – Veraltete Systeme sind einem größeren Risiko ausgesetzt. Aktualisieren Sie alle Ihre NAS auf einmal mit dem Synology Central Management System (CMS) und schützen Sie andere Geräte mit Gruppenrichtlinien im Synology Directory Server und mit C2 Identity
- **Finger weg von verdächtigen Dateien** – Spam- und Phishing-E-Mails mit verdächtigen Dateien sind gängige Methoden zur Verbreitung von Ransomware. Synology MailPlus bietet starken Anti-Malware-Schutz und Spam-Abwehr
- **Auf Sicherheitslücken prüfen** – Verwenden Sie den Synology Security Advisor, um routinemäßig nach Malware, Schwachstellen und anormalen Anmeldeaktivitäten zu suchen. Setzen Sie die Vorschläge des Beraters um und erhöhen Sie die Sicherheit Ihres NAS. https://www.synology.com/dsm/overview/security

Mehr Möglichkeiten, um Ihre Daten zu schützen

Zentrale Verwaltung Ihres gesamten Systems

Nutzen Sie die umfangreichen Funktionen zur zentralen Verwaltung von Datenzugriffsberechtigungen, Softwarestatus, Systemzustand und vielem mehr.
https://www.synology.com/dsm/overview/administration

Globale Überwachung all Ihrer Systeme

Erkennen Sie verdächtige Anmeldeaktivitäten, verwalten Sie Updates und überwachen Sie den Zustand Ihrer Geräte, egal wo sie sich befinden.
https://www.synology.com/dsm/feature/active-insight

Sicheres Backup für all Ihre Geräte

Befolgen Sie die 3-2-1-Backup-Regel, um Ihre Daten vor versehentlichen und böswilligen Änderungen oder Löschungen zu schützen.
https://www.synology.com/dsm/solution/data_backup

Jetzt starten

Beratung

Lassen Sie sich von unseren Experten beraten.
https://www.synology.com/services/business-consulting

Hier erhältlich

Finden Sie einen Synology Partner in Ihrer Region
https://www.synology.com/wheretobuy

Kundenberichte

Lesen Sie, wie andere Unternehmen von Synology profitieren
https://www.synology.com/company/case_study

Hinweise:

1. eSentire, Official Cybercrime Report 2022
   https://www.esentire.com/resources/library/2022-official-cybercrime-report

Schützen Sie sich vor Ransomware

https://www.synology.com/de-de/dsm/solution/ransomware

Synology Webseite

https://www.synology.com/

Kontakt

https://www.synology.com/company/contact_us

SYNOLOGY INC.

© 2023, Synology Inc. All rights reserved. Synology, the Synology logo are trademarks or registered trademarks of Synology Inc. Other product and company names mentioned herein may be trademarks of their respective companies. Synology may make changes to specification and product descriptions at anytime, without notice.