E-BOOK

5 Gründe, warum Sie Ransomware nicht verhindern können

NetApp

Inhalt

Angesichts der Zahl bekannter Ransomware-Angriffe im Laufe der Jahre und der schwerwiegenden Konsequenzen einer Infektion sollte man meinen, dass Abwehrmechanismen früher oder später so weit entwickelt sein werden, dass Ransomware keine Chance mehr hat.

Denken Sie nur an die einst allgegenwärtige Bedrohung durch Exploit-Kits wie den berüchtigten Angler, damals eine große Herausforderung für jedes Sicherheitsteam. Diese Exploit-Kits gehören dank des unermüdlichen Einsatzes von Forschern, die scharf dagegen vorgingen, der Vergangenheit an.

Ransomware dagegen ist immer noch weit verbreitet, und ein zuverlässiger Schutz vor Ransomware ist praktisch unmöglich. Sehen wir uns die Gründe dafür an.

5

Ransomware lohnt sich

Angreifer sind motivierter als je zuvor, denn erfolgreiche Angriffe lohnen sich. Der Durchschnitt der Forderungen, die von Unternehmen in den USA, Kanada und Europa beglichen wurden, stieg von 115.123 US-Dollar im Jahr 2019 auf 312.493 US-Dollar im Jahr 2020 an. Das entspricht einer jährlichen Steigerung von 171 %. Der Durchschnitt für das erste Geschäftsquartal 2021 belief sich auf 850.000 US-Dollar. Seit 2019 haben Ransomware-Vorfälle um 65 % zugenommen. Die Häufigkeit dieser Angriffe wird weiter steigen. Derzeit kommt es alle 11 Sekunden zu einem Ransomware-Angriff. Experten gehen davon aus, dass sich im Jahr 2031 bereits alle 2 Sekunden ein solcher Angriff ereignen wird. Diese Angriffe werden immer mehr zur Normalität. Angesichts dieser Zahlen wird klar, warum Ransomware nach wie vor bei Kriminellen beliebt ist.

Obwohl Exekutivbehörden davon abraten, zahlen Unternehmen nach wie vor das Lösegeld. Es ist nur natürlich, dass Unternehmen ihre Daten schützen möchten, doch die Kosten für die entstehenden Geschäftsunterbrechungen übersteigen häufig die eigentliche Lösegeldsumme. Auf die Forderungen einzugehen, ist somit oft die kostengünstigste Option.

4

Ransomware ist günstig

Auf Angreiferseite sind die Kosten für eine Ransomware-Kampagne gering. Ein Angreifer kann heute ein fertiges Ransomware-Kit für kleines Geld erwerben. Das Kit enthält alles, was für einen gewinnbringenden Angriff nötig ist, darunter Verschlüsselungsservices, den Payload Dropper und Verschleierungstools. Ein typisches RaaS-Abonnement (Ransomware-as-a-Service) ist bereits für 100 US-Dollar pro Monat zu haben. Komplexere und leistungsstärkere Varianten können Tausende US-Dollar kosten, doch damit steigt auch der potenzielle Gewinn. Support-Tarife sind ebenso enthalten, damit Angreifer den Service maximal ausschöpfen können.

3

Ransomware ist effektiv

Ransomware ist ein profitables Geschäft. Vergessen Sie das Klischee vom Kapuzenpulli tragenden Übeltäter im dunklen Kämmerlein – das ist ein ausgeklügeltes Netzwerk, das mit jedem Unternehmenspartnerprogramm mithalten kann. Eines der jüngsten Beispiele für RaaS ist DarkSide. DarkSide trat erstmals im August 2020 in Erscheinung und wechselte im November zu einem RaaS-Vertriebsmodell. Aus den gemeldeten Vorfällen lässt sich ableiten, dass für die Schlüssel zur Freischaltung der Daten üblicherweise ein Betrag in Höhe von 200.000 US-Dollar bis hin zu 2 Millionen US-Dollar verlangt wird. Die Hintermänner von DarkSide-Ransomware-Angriffen kassieren nicht nur viel Geld, sie sehen sich auch als eine Art „Robin Hood“: Sie nehmen das Geld von großen profitablen Unternehmen und spenden einen Teil davon für wohltätige Zwecke. Unbestätigten Berichten zufolge waren mindestens 90 Unternehmen bereits Opfer eines DarkSide-Angriffs. Insgesamt befinden sich mittlerweile mehr als 2 TB an gestohlenen Daten in den Händen von DarkSide – ein weiterer Anreiz zur Zahlung des Lösegelds.

2

Ransomware verspricht schnellen ROI

Ein weiterer Grund, der Ransomware so attraktiv macht: Nachdem sie in ein Unternehmen eingeschleust wurde – üblicherweise über E-Mail-Anhänge, schädliche URLs, unsichere Remote-Desktop-Protokolle oder schädliche Werbeanzeigen („Malvertising“) –, verbreitet sie sich schnell. Sie scannt das Netzwerk, um Dateien aufzuspüren, verschlüsselt dann den Inhalt und verlangt ein Lösegeld. Sobald die Verschlüsselung beginnt, lässt sie sich unglücklicherweise kaum mehr aufhalten. Als alarmierender Trend ist zudem eine neue Methode auf dem Vormarsch, bei der Angreifer Daten erst stehlen und danach verschlüsseln. Im Mai 2021 wurde Colonial Pipeline, der Betreiber einer großen Pipeline für Erdölderivate, über die große Teile der US-amerikanischen Ostküste mit Treibstoffen versorgt werden, zum Opfer eines Ransomware-Angriffs. Der Angriff wurde von der Hackergruppe DarkSide oder einem ihrer Partner ausgeführt. Dabei wurden nicht nur die Computersysteme von Colonial Pipeline gesperrt, sondern auch mehr als 100 GB an Unternehmensdaten gestohlen. Dieser Datendiebstahl zeigt, dass DarkSide seine Opfer auf doppelte Weise erpresst. Sie verlangen nicht nur Geld für die Freischaltung der befallenen Computer, sondern auch für die gestohlenen Daten. Sie drohen zudem mit der Veröffentlichung der gestohlenen Daten, falls die Opfer nicht zahlen.

1

Auf Menschen ist nicht immer Verlass

Bisher ging es um die Frage, warum Ransomware allgegenwärtig ist, aber nicht um die Antwort, wie wir sie stoppen können. Auch wenn viele Angriffe durch eine bessere Patching-Verwaltung verhindert werden könnten, gibt es nach wie vor einen vorrangigen Grund, der einen vollständigen Schutz unmöglich macht: der Mensch.

Sie vertrauen vielleicht darauf, dass Ihre Mitarbeiter Ihrem Unternehmen niemals vorsätzlich schaden würden. Dennoch kommen Ransomware-Infektionen vor, weil Mitarbeiter nicht zu jeder Zeit achtsam sind und geistesgegenwärtig auf schädliche Links und E-Mails oder Phishing-Angriffe reagieren.

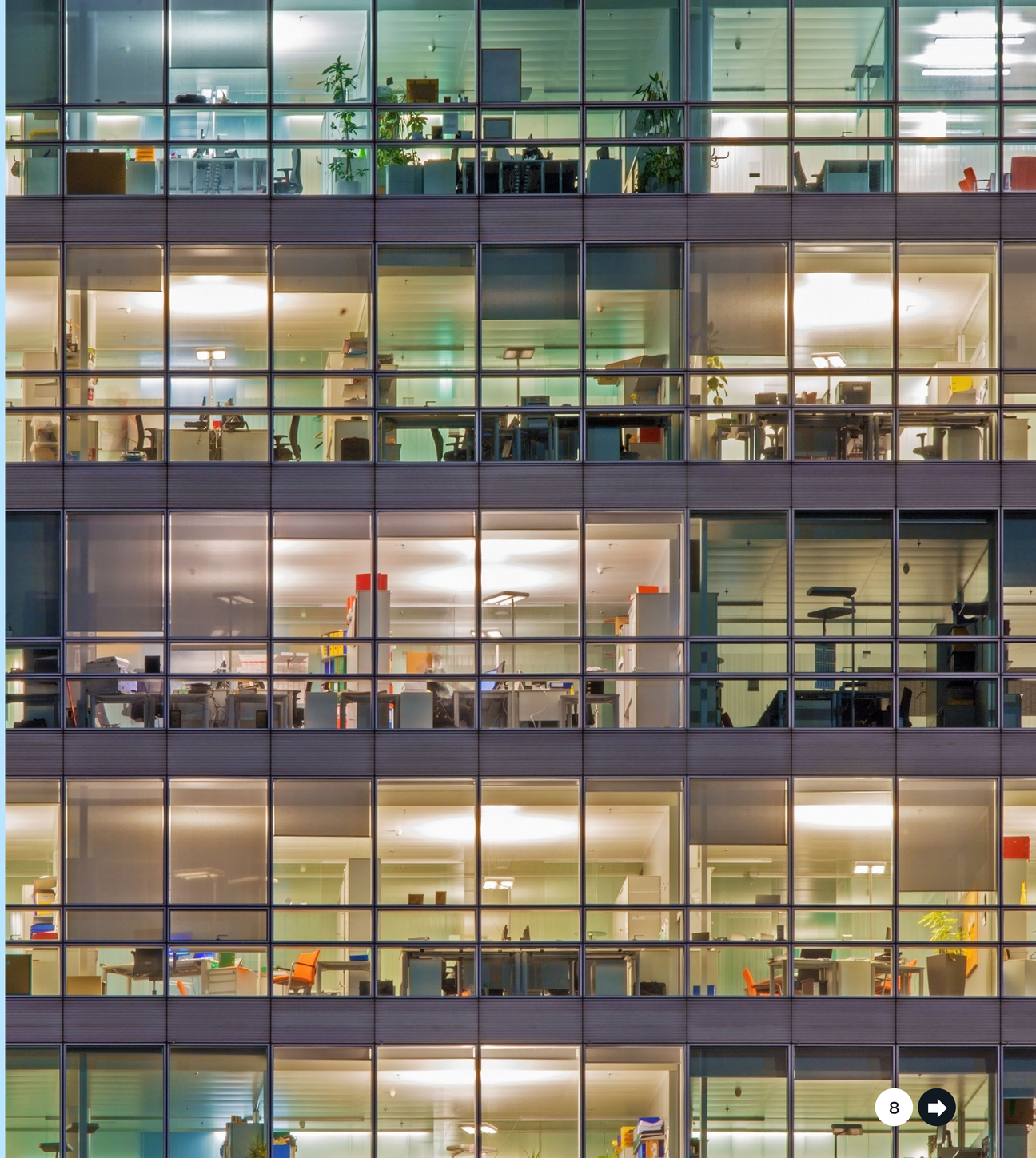
Viele Leser sind vermutlich mit regelmäßigen, verpflichtenden Computertrainings zur Erhöhung des Sicherheitsbewusstseins vertraut. Training schadet sicherlich nicht, doch selbst die vorsichtigsten Mitarbeiter können Fehlentscheidungen treffen und versehentlich einen Link anklicken oder eine E-Mail öffnen. Ohne extrem restriktive Sicherheitsrichtlinien, die die Mitarbeiter bei ihrer täglichen Arbeit extrem einschränken würden, reicht eine einzige solche Fehlentscheidung bereits aus. Die Erkennung darf nur wenige Sekunden dauern, keine Minuten, Stunden oder noch länger.

Vor Ransomware schützt nur ein Zero-Trust-Modell

Wenn Sie Ransomware nicht verhindern können, wie können Sie sich dann davor schützen?

Ihre Mitarbeiter müssen Zugriff auf Daten haben, um ihre Arbeit zu erledigen – genau wie Ransomware. Ihre Mitarbeiter werden also zum Angriffspunkt. Richtlinien und Rollen zur Einschränkung des Zugriffs auf Daten können hilfreich sein, häufig wirken sie sich jedoch negativ auf die Produktivität aus.

Die Antwort lautet Wachsamkeit: Früherkennung, Analysen des Benutzerverhaltens und automatisierte Maßnahmen beim Auftreten verdächtiger Muster – innerhalb von Sekunden.



NetApp Cloud Insights bietet mit der Funktion Cloud Secure genau diese Erkennung. Mit Cloud Secure können Sie Aktivitäten überwachen, Anomalien aufdecken und Reaktionen automatisieren.

- **Überwachen der Benutzeraktivität**
  Um Vorfälle korrekt zu identifizieren, werden alle Benutzeraktivitäten in lokalen und Hybrid-Cloud-Umgebungen erfasst und analysiert. Die Daten werden mit einem schlanken, statusfreien Datenerfassungs-Agenten gesammelt, der auf einer VM in der Umgebung des Unternehmens installiert wird. Zu diesen Daten gehören auch Benutzerdaten von Active-Directory- und LDAP-Servern und Benutzerdateiaktivitäten von NetApp ONTAP Storage (in Ihrem Datacenter oder in der Cloud).

  Cloud Secure erkennt Anomalien im Benutzerverhalten, indem für jeden Benutzer ein Verhaltensmodell erstellt wird. Dieses Verhaltensmodell erkennt abnorme Veränderungen der Benutzeraktivität und analysiert, ob es sich bei der Bedrohung um Ransomware oder einen böswilligen Benutzer handelt. Ein solches Verhaltensmodell reduziert die Menge an falsch positiven Ergebnissen.

- **Erkennen von Anomalien und potenziellen Angriffen**
  Ransomware und Malware sind heute sehr ausgeklügelt. Sie nutzen zufällige Endungen und Dateinamen, wodurch die Erkennung durch signaturbasierte Lösungen (Blockierliste) nicht mehr funktioniert. Cloud Secure setzt innovative Machine-Learning-Algorithmen ein, um ungewöhnliche Datenaktivitäten aufzudecken und einen potenziellen Angriff zu erkennen. Dieser Ansatz macht eine dynamische und korrekte Erkennung möglich und reduziert die Anzahl falsch positiver Ergebnisse.

- **Richtlinien für die automatisierte Reaktion**
  Cloud Secure warnt Sie bei möglichen Ransomware-Angriffen und schützt Ihre Daten mit diversen Richtlinien für automatisierte Reaktionen.

  Bei verdächtigen Verhaltensmustern wird automatisch eine NetApp Snapshot Kopie erstellt, damit Ihre Daten gesichert sind und schnell wiederhergestellt werden können. Mögliche Ausfälle durch falsch positive Ergebnisse werden auf ein Minimum reduziert.

Der Datenzugriff eines Benutzers wird gesperrt:
- wenn verdächtige Schreib-/Lesevorgänge erkannt werden
- wenn auffällige Löschvorgänge erkannt werden

Dank der detaillierten Dateizugriffsüberwachung von Cloud Secure können Administratoren kompromittierte Daten sowie die Quelle des Angriffs schnell identifizieren. So können Vorfälle schnell behoben und sämtliche Daten wiederhergestellt werden.

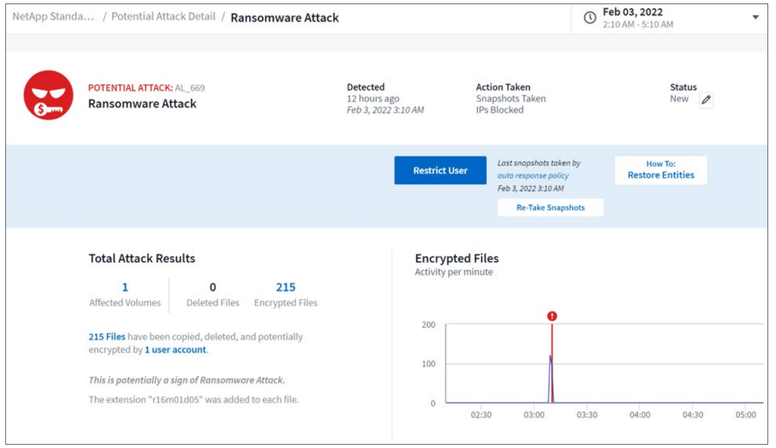


Abbildung 1) Das Cloud Secure Dashboard meldet einen Ransomware-Angriff

Sollte Cloud Secure Ihr Interesse geweckt haben, können Sie dieses Tool 30 Tage kostenlos testen.
Mehr erfahren und kostenlose Testphase starten.

NetApp

Über NetApp

In einer Welt voller Generalisten beweist sich NetApp als Spezialist. Wir haben ein Ziel fest im Blick: Ihr Unternehmen darin zu unterstützen, Ihre Daten optimal zu nutzen. NetApp bringt die Datenservices, denen Sie vertrauen, in die Cloud und die Einfachheit und Flexibilität der Cloud in Ihr Datacenter. Selbst bei höchsten Ansprüchen lassen sich die branchenführenden NetApp Lösungen in unterschiedlichsten Kundenumgebungen und den weltweit führenden Public Clouds einsetzen.

Als Cloud- und Daten-orientierter Softwareanbieter stellt nur NetApp alle Technologien bereit, mit denen Sie Ihre eigene maßgeschneiderte Data Fabric aufbauen, Ihre Clouds vereinfachen, Ihre Public Clouds anbinden und so die richtigen Daten, Services und Applikationen sicher bereitstellen können – immer und überall.