RANSOMWARE: HÄUFIG GESTELLTE FRAGEN

ABSCHNITT 1: RANSOMWARE – ÜBERSICHT

Was ist Ransomware?

Ransomware ist eine Form von schädlicher Software, die entwickelt wurde, um entweder den Zugriff auf ein Computersystem zu blockieren oder die Dateien oder andere Daten eines Benutzers zu verschlüsseln. Der Cyberkriminelle fordert dann Lösegeld (in der Regel in Form von virtueller Währung, z. B. Bitcoin, die schwer nachzuverfolgen ist), nach dessen Erhalt der Täter möglicherweise (es besteht keine Garantie!) Anweisungen zur Wiederherstellung des Zugriffs auf das System und die Dateien des Benutzers bereitstellt. Ransomware zielt häufig auf Personen ab; jedoch sind auch Unternehmen – einschließlich großer Konzerne – Ziel dieser Angriffe geworden.

Warum sollte ich mir wegen Ransomware Sorgen machen?

Bei Ransomware handelt es sich um eine wachsende Bedrohung; tatsächlich entstehen jedes Jahr buchstäblich Millionen von neuen Malwarevarianten. Sie benötigen einen Plan, um gegen diese Form der Cyberkriminalität vorzugehen.

Wie wird Ransomware weitergegeben?

Ransomware erhält über das schwächste Glied im Netzwerk Zugriff auf ein Computersystem, in der Regel ist das die E-Mail oder ein soziales Netzwerk des Benutzers. Nicht selten gehen Kriminelle informierte Benutzer über Phishing-E-Mails und zweifelhafte Weblinks an. Sobald ein Benutzer auf einen schädlichen Link klickt oder einen infizierten Anhang öffnet, verteilt sich die Malware im gesamten System. Nach dem Öffnen können mit Schadsoftware infizierte Dateien die Netzwerksicherheit eines Unternehmens schnell umgehen. Die Schadsoftware kann sich auch innerhalb von Dateien auf Anwendermaschinen befinden. Wenn diese Dateien mit einer Plattform für Zusammenarbeit synchronisiert oder darauf gespeichert werden und andere Benutzer darauf zugreifen können, kann sich die Schadsoftware auf andere Computer verbreiten.

Wie wird Ransomware erkannt?

Ein Angriff mit Ransomware bleibt in der Regel unerkannt, bis die Schadsoftware das System infiziert hat. Oft erscheint eine Meldung auf dem Computerbildschirm, die den Benutzer darüber informiert, dass sein Computer gesperrt wurde bzw. seine Dateien verschlüsselt wurden.

Was kann ich tun, um mich vor Ransomware zu schützen?

Sie können Whitelisting, Filterung, Isolierung, Virenschutz und Systemscans nutzen, um Ransomware zu verhindern. Allerdings sind Kriminelle sehr erfindungsreich und beharrlich. Nur ein Mausklick genügt, um infiziert zu werden. Die beste Möglichkeit, sich selbst vor Ransomware zu schützen, ist ein zuverlässiges Backup, von dem Sie Ihre nicht infizierten Dateien wiederherstellen können. Backups sollten häufig erstellt werden und zuverlässig sein, damit Sie Daten auf einen Point-in-Time vor dem Angriff wiederherstellen können.

Warum ist Synchronisierung keine gute Backupmethode?

Eine Synchronisierung ist kein Backup. Alle Änderungen an der Quelldatei, einschließlich der Ransomware, werden schnell mit der Cloud und allen anderen Benutzern, die auf die Datei zugreifen können, synchronisiert. Darüber hinaus müssen Benutzer von Synchronisierungsdiensten, die eine Versionierung oder einen Papierkorb anbieten, Dateien einzeln zur Wiederherstellung auswählen und können keinen Point-in-Time-Snapshot verwenden. Ein Backupservice hingegen ermöglicht es, bestimmte Dateien oder alle Dateien eines bestimmten Datums mit wenigen Mausklicks wiederherzustellen. Ein Synchronisierungsdienst bietet also bequemen Zugriff auf Dateien, ein Backupservice aber bietet viel leistungsfähigere Wiederherstellungsfunktionen im Katastrophenfall. Darüber hinaus kann über einen Synchronisierungsdienst unabsichtlich Malware auf viele andere Computer und Geräte weiterverbreitet werden.

ABSCHNITT 2: RANSOMWARE UND MOZY

Wie sind Mozy-Daten vor einem Ransomware-Angriff geschützt?

Mozy-Kundendaten werden in der EMC Cloud gespeichert, die von der Umgebung des Kunden isoliert wird. Darüber hinaus ist die EMC Cloud eine Non-Executing-Umgebung. Programme, einschließlich Viren, können also nicht in der Cloud ausgeführt werden und dort gespeicherte Dateien infizieren.

Wie werden nicht infizierte Daten mit Mozy wiederhergestellt?

Sobald Sie alle betroffenen Benutzer identifiziert, die Schadsoftware gelöscht und bei Auftreten der Infektion isoliert haben, können Sie Daten aus einem bestimmten Backup wiederherstellen, das vor der Infektion erstellt wurde.

Was geschieht, wenn in meinem Mozy-Backup die Malware enthalten ist?

Die Mozy-Cloud ist eine Non-Executing-Umgebung, was bedeutet, dass Programme, einschließlich Viren, in der Cloud nicht ausgeführt werden und dort gespeicherte Dateien nicht infizieren können. Außerdem speichert Mozy Dateiversionen bis zu 90 Tage lang, d. h., wenn Sie den Infektionsherd (Benutzer und Datei) und den Zeitpunkt, zu dem die Schadsoftware in die Maschine eingeschleust wurde, ermittelt haben, kann Mozy alle Dateien für den angegebenen Benutzer ab dem Point-in-Time vor Einschleusung der Schadsoftware wiederherstellen. Angenommen, die Schadsoftware wurde am 2. Juni eingeschleust, dann können Sie Dateien aus dem Backup vom 1. Juni wiederherstellen. Dies wird manchmal als Rollback bezeichnet.

ABSCHNITT 3: RANSOMWARE UND SPANNING

Wie können Daten in Google Drive oder OneDrive for Business mit Ransomware infiziert werden?

Die meisten Unternehmen, die Google Drive oder OneDrive for Business nutzen, verwenden auf den Endpunkten ihrer Anwender (Laptops) Synchronisierungsdienste, damit sie leichter auf Dateien zugreifen, diese bearbeiten und die Dateiänderungen anschließend zurück in die Cloud sowie mit allen anderen Benutzern, die gemeinsamen Zugriff auf diese Dateien haben, synchronisieren können. Wenn Ransomware einen Endpunkt wie einen Laptop angreift, werden die von der Ransomware verschlüsselten Dateien mit der Cloud synchronisiert und an andere Benutzer in Ihrem Unternehmen oder schlimmer, an externe Partner oder Kunden weiterverbreitet.

Wie sind die Daten in einem Spanning-Backup vor einem Ransomware-Angriff geschützt?

In einem Spanning-Backup gespeicherte Kundendaten sind von der Umgebung des Kunden isoliert. Alle Daten werden in der SSAE SOC 2-konformen Cloudumgebung von Spanning gespeichert und in einer Non-Executing-Umgebung isoliert, was bedeutet, dass Programme, einschließlich Viren und Schadsoftware, nicht ausgeführt werden und dort gespeicherte Dateien nicht infizieren können.

Wie werden nicht infizierte Daten mit Spanning wiederhergestellt?

Sobald Sie alle betroffenen Benutzer identifiziert, die Schadsoftware gelöscht und bei Auftreten der Infektion isoliert haben, können Sie Daten von jedem Point-in-Time-Backup in einem Spanning-Backup direkt in Office 365 oder Google Apps wiederherstellen. Nachdem die Daten wiederhergestellt wurden, können sie mit den Endpunkten synchronisiert werden. Unternehmen können die Synchronisierungsdienste während einer Infektion auch anhalten und Benutzer darauf beschränken, Dokumente in Clouddiensten wie Google Docs oder in den Onlineversionen von Word, Excel und PowerPoint von Office 365 zu bearbeiten.

KONTAKTIERE UNS

Wenn Sie mehr darüber erfahren möchten, wie Sie mithilfe von Endpunktdatensicherheit eine Ransomware-Katastrophe verhindern können, besuchen Sie Mozy. Für weitere Informationen über den Schutz Ihrer SaaS-Daten besuchen Sie Spanning.