Die ultimative Checkliste: So verhindern und bekämpfen Sie Ransomware-Angriffe

Einem aktuellen Bericht des Institute for Critical Infrastructure Technology, einer Denkfabrik aus der Branche, zufolge steht das Jahr 2016 ganz im Zeichen von Ransomware. Gegen Ransomware-Attacken ist Angriff die beste Verteidigung. Ist Ihr Unternehmen entsprechend vorbereitet? Jetzt brauchen Sie nicht mehr lange überlegen, wie Ihre Verteidigungsstrategie aussehen soll. Mit dieser Checkliste schirmen Sie Ihr Unternehmen gegen raffinierte Cyber-Angriffe ab.

☐ 1. Alle Daten gründlich sichern

Ihr wirksamstes Mittel in der Abwehr von Ransomware sind regelmäßige Backups nach einem festgelegten Zeitplan. Im Falle eines Angriffs können sie dann das Endgerät herunterfahren, das Image neu laden und ein aktuelles Backup aufspielen, um zu verhindern, dass sich die Ransomware auf andere Systeme in Ihrem Netzwerk ausbreitet.

Ransomware kann nur durch eine komplette Löschung des betroffenen Systems entfernt werden. Systemstatus-Backups oder -Snapshots sind daher unerlässlich, um nach einem Angriff schnellstmöglich den Normalzustand wiederherstellen zu können. Je häufiger die Backups durchgeführt werden, desto weniger Daten gehen verloren. Der Turnus der Datensicherungen sollte sich dabei danach richten, inwiefern die Daten von strategischer Bedeutung sind und welches Ausmaß an Datenverlust für das Unternehmen noch akzeptabel ist. Da jedes an das betroffene System angeschlossene Gerät von der Ransomware verschlüsselt wird, muss ein externer Speicher verwendet werden, der nach Abschluss des Backups weder dem System zugeordnet noch damit verbunden ist.

☐ 2. Patches konsequent installieren

Ransomware findet ihren Weg ins Netzwerk häufig über bekannte Sicherheitslücken in veralteter Software. Unternehmen, in denen Patches nicht konsequent installiert und veraltete Software verwendet wird, sind anfällig gegenüber Angriffen. Aktualisieren Sie Ihre Software daher regelmäßig, insbesondere auch solche von Drittanbietern (z. B. Java und Flash), in denen Sicherheitslücken häufig ausgenutzt werden.

☐ 3. Nutzer über Gefahrenquellen aufklären

Das schwächste Glied in der Sicherheitskette ist in der Regel der Nutzer. Fällt ein Mitarbeiter etwa auf eine Phishing-E-Mail oder andere Social-Engineering-Taktiken herein, könnte er sich Malware einfangen und Ihr Unternehmen gefährden. Klären Sie die Nutzer daher umfassend darüber auf, wie sie Social-Engineering erkennen können. Cyberkriminelle nutzen diese Taktik, da es in der Regel einfacher für sie ist, das natürliche Vertrauen des Menschen auszunutzen, als sich in Ihre Software zu hacken.

Die Nutzer müssen daher wissen, wem und was sie trauen können. Machen Sie Ihnen klar, dass sie sich immer die folgenden Fragen stellen müssen, wenn sie ihre E-Mails lesen:

1. Kenne ich den Absender?
2. Muss ich den Anhang der E-Mail wirklich öffnen oder auf die darin enthaltenen Links klicken?
3. Habe ich tatsächlich etwas von dieser Firma bestellt?

☐ 4. Das Netzwerk schützen

Setzen Sie auf einen mehrschichtigen Ansatz für den Schutz Ihres Netzwerks, der Technologien wie eine Next-Generation Firewall (NGFW) und ein Intrusion Prevention System (IPS) beinhaltet. Eine mehrschichtige Verteidigung ermöglicht die Implementierung von Sicherheitsmaßnahmen in zahlreichen Bereichen Ihres Netzwerks. Indem Sie Single-Points-of-Failure beseitigen, schützen Sie Ihr Netzwerk und Ihre Daten effektiver.

☐ 5. Netzwerkzugriff segmentieren

Durch die Segmentierung Ihres Netzwerks begrenzen Sie die Zahl der Ressourcen, auf die ein Angreifer ggf. zugreifen kann. Dabei werden Netzwerk- und andere Ressourcen sowie Anwendungen in voneinander getrennte Bereiche gruppiert und mittels dynamischer Zugriffskontrolle verhindert, dass durch einen einzigen Angriff bereits das gesamte Netzwerk kompromittiert wird.

Die meisten Unternehmensnetzwerke sind „flach“, d. h. es besteht kaum oder keinerlei Segmentierung zwischen Geschäftsbereichen, Nutzern und Daten bzw. zwischen für bestimmte Geschäftsbereiche relevanten Daten usw. Indem Sie Ihr Netzwerk segmentieren, können Sie die Ausbreitung von Malware unterbinden oder verlangsamen und Bedrohungen eingrenzen.

☐ 6. Alle Aktivitäten im Netzwerk genau beobachten

Nur das, was Sie sehen, können Sie auch schützen. Daher benötigen Sie einen transparenten Überblick über Ihr gesamtes Netzwerk. Dies klingt nach einer gewaltigen Aufgabe, ist aber unabdingbar. Denn nur wenn Sie alle Vorgänge in Ihrem Netzwerk und Rechenzentrum im Blick behalten, können Sie Angreifer aufspüren, die an den Abwehrmechanismen am Perimeter vorbei gelangt sind und in Ihre interne Umgebung eindringen.

Schützen Sie den Perimeter, indem Sie eine sogenannte demilitarisierte Zone (DMZ) einrichten und diese stärken. Die DMZ ist ein physisches oder logisches Subnetz, das die externen Services Ihres Unternehmens auf ein üblicherweise größeres und nicht vertrauenswürdiges Netzwerk (z. B. das Internet) beschränkt und dort zur Verfügung stellt. Auf diese Weise erhält Ihr LAN eine zusätzliche Sicherheitsebene, da externe Netzwerkknoten nur noch auf die Server in der DMZ direkt zugreifen können, jedoch nicht mehr auf andere Bereichen Ihres internen Netzwerks.

☐ 7. Erstinfektionen vorbeugen

Es kann vorkommen, das Ihre Nutzer ohne böse Absicht auf kompromittierte Websites zugreifen oder Malvertising-E-Mails öffnen und dadurch Malware in Ihr Netzwerk einschleppen. Die ursprüngliche Ransomware-Infektion geschieht in der Regel über einen E-Mail-Anhang oder einen schädlichen Download. Indem Sie schädliche Websites sowie im Rahmen von Ransomware-Kampagnen versendete E-Mails und Anhänge blockieren, können Sie Ihr Netzwerk davor schützen.

Es empfiehlt sich außerdem, den Austausch von Dateien zwischen Nutzern innerhalb Ihres Unternehmens und mit Ihren Partnern über ein unternehmensweites Programm zu regeln. Mit einer File-Sharing-Lösung und der Anweisung an Benutzer, niemals Dateien per E-Mail auszutauschen bzw. diese zu akzeptieren, können Infektionen über Anhänge aus Phishing-E-Mails nahezu vollständig vermieden werden.

☐ 8. Endgeräte absichern

Eine Antiviruslösung allein kann Endgeräte nicht ausreichend vor Ransomware schützen. Und da BYOD (Bring-Your-Own-Device) immer beliebter wird, benötigen Sie eine Lösung, mit der Sie die Kontrolle über die Laptops, Mobilgeräte und Tablets in Ihrem Netzwerk behalten. Entscheidend dabei: Die Lösung muss Ihnen einen Überblick darüber verschaffen, wer und was sich mit Ihrem Netzwerk verbindet und es Ihnen ermöglichen, anhand von Richtlinien zu verhindern, dass kompromittierte Websites aufgerufen oder verdächtige Dateien heruntergeladen werden.

Gehen Sie nach dem Prinzip der „geringstmöglichen Berechtigungen“ vor, d. h. Sie erteilen jedem Konto nur die Rechte, die zur Erfüllung der jeweiligen Aufgaben absolut erforderlich sind. Dieses Prinzip kann z. B. auf Nutzerberechtigungen auf Endgeräten und Netzwerkfreigaben angewandt werden – wird es allerdings häufig nicht. Die Idee hinter diesem Prinzip: Schadsoftware wird in der Regel über die Berechtigungsstufe des aktuell angemeldeten Nutzers ausgeführt. Verfügt dieser über Administratorrechte, gilt das Gleiche auch für den Angreifer. Verwenden Sie außerdem immer eine Zwei-Faktor-Authentifizierung. Denn ein Hacker stiehlt vielleicht Kennwörter, aber es ist nahezu unmöglich, sie gleichzeitig mit einem Smartphone oder Token zu stehlen.

☐ 9. Minutenaktuelle Threat-Intelligence nutzen

Um eine Bedrohung proaktiv abwehren zu können, müssen Sie den Gegner kennen. Threat-Intelligence informiert Ihre Sicherheitsteams frühzeitig darüber, welche Regionen, Branchen und sogar welche Unternehmen Cyberkriminelle ins Visier nehmen, sodass sie schnell entsprechende Maßnahmen ergreifen können. Wie erhalten Sie also minutenaktuelle Threat-Intelligence? Indem Sie die Augen offen halten und auf die Informationen von Threat-Intelligence-Organisationen wie Cisco Talos zurückgreifen.

Das Team von Cisco Talos umfasst mehr als 250 Sicherheitsforscher, die Rund um die Uhr an Maßnahmen zum Schutz vor neuen und bekannten Cyber-Bedrohungen arbeiten. Das Team veröffentlicht Sicherheitsinformationen in Blog-Beiträgen, Newslettern, auf Social-Media sowie in Community-Foren und in Lehrvideos, um das Internet für alle sicherer zu machen. Davon können Sie profitieren, indem Sie ihre Erkenntnisse verfolgen und Ihr Unternehmen informieren, wenn in Ihrem Umfeld eine Bedrohung auftritt.

☐ 10. Auf keinen Fall erpressen lassen

Auch wenn viele Unternehmen versucht sind, das Lösegeld zu zahlen, um die Kontrolle über ihre Systeme zurückzuerhalten, sollte dies nur das äußerste Mittel sein. Wenden Sie sich stattdessen an die Behörden und weigern Sie sich, die Kriminellen mit dem Lösegeld zu finanzieren.

Weitere Informationen

Weitere Informationen über Netzwerktransparenz und die Cisco Ransomware Defense-Lösung finden Sie unter http://www.cisco.com/go/ransomware.