Cisco Ransomware Defense: Bekämpfung von Ransomware

Wünschen Sie sich besseren Schutz vor Ransomware auf allen Angriffsvektoren? Mit den Security-Produkten und der Architektur von Cisco ist das möglich.

Überblick

Dateien und Informationen sind für ein Unternehmen überlebenswichtig. Diese Informationen, von denen auch die Produktivität im Unternehmen abhängt, müssen unter allen Umständen intakt und sicher bleiben.

Genau an diesem Punkt setzt Ransomware an – bösartige Software oder Malware, die Informationen wie Dokumente, Fotos und Musikdateien auf dem Computer eines Privatbenutzers oder eines Unternehmens unzugänglich macht. Die Dateien werden erst nach Zahlung eines Lösegelds (Englisch „ransom“) wieder entsperrt und dem Eigentümer zurückgegeben. Ohne geeignete Verteidigungsmaßnahmen kann Ransomware ein Unternehmen nahezu handlungsunfähig machen.

In der Regel gelangt Ransomware durch Exploit-Kits, Malvertising (infizierte Werbeanzeigen auf einer Website, über die Malware übertragen werden kann), Phishing (betrügerische E-Mails von scheinbar vertrauenswürdigen Absendern) oder Spam-Kampagnen in das System. Die eigentliche Infektion kann beginnen, wenn ein Benutzer in einer Phishing-E-Mail auf einen Link oder einen Anhang klickt. Eine andere Möglichkeit ist der Besuch einer Website mit schädlichen Werbeanzeigen, die zu einer automatischen Infektion des Computers führen.

Abhilfe schafft Cisco® Ransomware Defense. Die Lösung reduziert das Risiko einer Ransomware-Infektion durch einen mehrschichtigen Ansatz, der von der DNS-Layer über den Endpunkt und das Netzwerk bis hin zu E-Mails und dem Web reicht. Wir bieten integrierte Verteidigungsmaßnahmen in einer Architektur, die höchste Transparenz mit optimaler Reaktionsfähigkeit in Bezug auf Ransomware vereint.

Vorteile

- **Reduzierung des Risikos einer Ransomware-Infektion**, damit Sie sich weiterhin auf Ihre Geschäftsabläufe konzentrieren können
- **Unmittelbarer Schutz** durch Sicherheitstools, die Bedrohungen blockieren, bevor diese Fuß fassen können
- **Bisher unerreichte Transparenz und Reaktionsfähigkeit** dank eines architekturbasierten Ansatzes, der von der DNS-Layer über das Netzwerk bis zum Endpunkt reicht
- **Verhinderung der lateralen Ausbreitung von Malware** durch strikte Netzwerksegmentierung
- **Branchenführende Threat-Intelligence von Cisco Talos** und Informationen über Ransomware

Eine rasant zunehmende, ernste Bedrohung

Dies ist das Jahr der Ransomware. Die Gewinnspannen der Angreifer sind beeindruckend. Ransomware hat sich schnell zur lukrativsten Malware-Art aller Zeiten entwickelt.

Laut FBI erpressen Angreifer damit schon bald eine Milliarde US-Dollar pro Jahr. Die Sicherheitsforscher von Cisco Talos haben ermittelt, dass eine einzige Ransomware-Kampagne bis zu 60 Millionen US-Dollar pro Jahr generieren kann. Sogar im Fernsehen ist Ransomware inzwischen Thema.

Die Angreifer verfügen über die nötigen finanziellen Mittel und den Willen, um immer wieder neue, noch gefährlichere Arten von Ransomware zu entwickeln. Wir glauben, dass Ransomware in Zukunft noch besser dazu in der Lage sein wird, sich selbständig zu verbreiten, damit weite Teile des Unternehmensnetzwerks unzugänglich gemacht werden können. Nach einem solchen Angriff wäre die IT-Funktionalität wieder auf dem Stand der 1970er Jahre.

Derzeit werden überwiegend einzelne und punktuelle Produkte gegen Ransomware eingesetzt. Besser geeignet wäre jedoch ein architekturbasierter Ansatz unter Berücksichtigung der verschiedenen Angriffsvektoren.

Im vorliegenden Lösungsüberblick werden die verschiedenen von Angreifern genutzten Vektoren und Methoden vorgestellt. Lösungen zur Abwehr von Ransomware müssen E-Mails und das Web absichern, den Zugriff auf schädliche Infrastrukturen im Internet verhindern, auf einen Endpunkt gelangte Ransomware-Dateien aufhalten, die verwendeten Command-and-Control Callbacks blockieren und die ungehinderte laterale Ausbreitung von Ransomware im Fall einer Infektion unterbinden.

Lösungsumfang

Cisco Ransomware Defense vereint verschiedene Bestandteile der Cisco Sicherheitsarchitektur im Kampf gegen Ransomware. Sie können sich für alle Komponenten entscheiden oder einzelne Komponenten für akute Anforderungen auswählen.

Ransomware Defense umfasst folgende Komponenten:

- Cisco Umbrella blockiert Bedrohungen auf der DNS-Layer, weit weg vom Netzwerk.
- Cisco Advanced Malware Protection (AMP) für Endpunkte verhindert, dass schädliche Ransomware-Dateien am Endpunkt ausgeführt werden.

- Cisco Email Security (Cloud- und standortbasiert) hält Phishing- und Spam-Mails auf, über die Ransomware übertragen wird.
- Advanced Malware Protection kann Email Security-Produkten sofort hinzugefügt werden. Eine unkomplizierte Lizenz ermöglicht die statische und dynamische Analyse (Sandboxing) unbekannter Anhänge, die das Cisco Email Security-Gateway passieren.
- Cisco FirePOWER™ Next-Generation Firewall (NGFW) blockiert Command-and-Control-Datenverkehr und alle schädlichen Dateien, die das Netzwerk durchqueren.
- Cisco ISE, bereitgestellt über das Cisco Netzwerk, nimmt eine dynamische Netzwerksegmentierung vor, damit sich Ransomware nicht lateral ausbreiten kann.

Mit Ransomware Defense können Unternehmen das Netzwerk als Kontrollinstrument einsetzen und damit die Verbreitung von Ransomware eindämmen. Im schlimmsten Fall, nämlich bei einer Infektion, kann sich die Ransomware dann nicht mehr so einfach im Netzwerk ausbreiten.

Cisco Security Services bieten sofortige Unterstützung bei der Reaktion auf Vorfälle nach einem Ausbruch. Sie können auch die Bereitstellung von AMP, NGFW und anderen Produkten der Lösung optimieren.

Wichtigste Funktionen

- Blockierung von Ransomware, damit sie nicht in das Netzwerk gelangt oder auf Laptops heruntergeladen wird
- Eindämmung von Ransomware, wenn sie sich bereits im Netzwerk befindet

Security-Services zur Bekämpfung von Ransomware

Das Cisco Security Services Incident Response-Team kann Unternehmen für die Reaktion auf Vorfälle vorbereiten und im Fall einer Ransomware-Infektion reaktiv eingreifen.

Mit den Cisco Security Integration Services bewältigen Sie auch die Herausforderungen bei der Lösungsintegration. Sie optimieren die Bereitstellung von Lösungstechnologien wie AMP für Endpunkte und Cisco FirePOWER NGFW. Unser Team verfügt über umfassendes Know-how bei der Bereitstellung integrierter Sicherheitslösungen. So kann es zur beschleunigten Einführung der benötigten Sicherheitstechnologie mit möglichst wenig Störungen beitragen.

Generell müssen Organisationen dafür sorgen, dass geeignete Technologien und Richtlinien für Daten-Backups vorhanden sind, um die Auswirkungen eines Ransomware-Befalls zu mindern.

„Wir haben ein großes Risiko im Hinblick auf das Web als Angriffsvektor für Ransomware abgedeckt und die Benutzerfreundlichkeit der Internetverbindungen deutlich erhöht.“

– Octapharma

Cisco Capital

Auf Ihre Ziele abgestimmte Finanzierungslösungen

Mit Cisco Capital® können Sie die Technologien erwerben, die Sie benötigen, um Ihre geschäftlichen Ziele zu erreichen und wettbewerbsfähig zu bleiben. Mit unserer Unterstützung senken Sie Ihre Kapitalausgaben, beschleunigen Ihr Wachstum und optimieren Ihre Investitionen und Ihren ROI. Cisco Capital bietet Ihnen flexible Optionen für die Finanzierung von Hardware, Software, Services und zusätzlichen Drittanbietergeräten – das alles bei planbarer Zahlung. Cisco Capital ist in mehr als 100 Ländern verfügbar. Mehr dazu hier

Vorteile von Cisco

Ransomware kann auf vielen verschiedenen Wegen in Ihr Unternehmen gelangen. Phishing-E-Mails, infizierte Web-Banner, Spam – egal welcher Angriffsvektor, es wird ein umfassender Schutz benötigt. Nur Cisco bietet einen architekturbasierten Ansatz gegen Ransomware, denn punktuelle Lösungen alleine reichen nicht aus. Unsere Lösung beruht auf den Erkenntnissen der branchenführenden Cisco Talos Research Group, die Bedrohungen durch Ransomware eingehend untersucht hat. Das Ergebnis ist ein effektiver mehrschichtiger Sicherheitsansatz. Wir blockieren Ransomware und bekämpfen sie, falls sie dennoch in Ihr Netzwerk gelangen sollte – was sich nicht völlig ausschließen lässt.

C22-737492-01 08/16