Präsentiert von

cisco

Abwehr von Ransomware

für dummies®

2. Cisco Sonderausgabe

- Merkmale von Ransomware erkennen
- Eine neue „Best-of-Breed"-Sicherheitsarchitektur aufbauen
- Ransomware-Angriffe verhindern

Lawrence Miller, CISSP

Über Cisco

Cisco entwickelt und verkauft ein breites Spektrum an Produkten und bietet Dienstleistungen und integrierte Lösungen an, um die Netzwerke, die das Internet bilden, auf der ganzen Welt weiterzuentwickeln und miteinander zu verbinden.

Als weltweit führender Anbieter in unserer Branche helfen wir unseren Kunden dabei, Verbindungen herzustellen, digital zu werden und erfolgreich zu sein. Gemeinsam ändern wir die Art und Weise, wie Menschen arbeiten, leben, ihre Freizeit verbringen und lernen.

Seit über 30 Jahren helfen wir unseren Kunden dabei, Netzwerke zu bauen und auf Informationstechnologie (IT) basierende Produkte und Dienstleistungen zu automatisieren, zu koordinieren, zu integrieren und zu digitalisieren.

In einer zunehmend verbundenen Welt trägt Cisco entscheidend dazu bei, Unternehmen, Regierungen und Städte auf der ganzen Welt durch differenzierte Innovationen zu transformieren.

Cisco Ransomware Defense
www.cisco.com/go/ransomware

Cisco Ransomware Defense stützt sich auf die Cisco Sicherheitsarchitektur, um Unternehmen durch eine Abwehrlösung zu schützen, die von der DNS-Ebene über Netzwerke und den E-Mail-Verkehr bis hin zum Endpunkt greift. Diese einfache, offene, automatisierte und wirksame Lösung verhilft Unternehmen zu einer optimalen Reaktionsfähigkeit auf Ransomware-Angriffe.

www.twitter.com/CiscoUmbrella
www.facebook.com/CiscoUmbrella
www.linkedin.com/company/OpenDNS
www.youtube.com/c/CiscoUmbrella

Abwehr von Ransomware

2. Cisco Sonderausgabe

Lawrence Miller

für dummies®

Abwehr von Ransomware Für Dummies®, 2. Cisco Sonderausgabe

Veröffentlicht von
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-69607-0 (pbk); ISBN 978-1-119-69611-7 (ebk)

Hergestellt in den Vereinigten Staaten.

10 9 8 7 6 5 4 3 2 1

Allgemeine Informationen zu unseren anderen Produkten und Dienstleistungen oder zur Erstellung eines individuellen *Für Dummies*-Buches für Ihr Unternehmen oder Ihre Organisation erhalten Sie von unserer Abteilung Business Development in den USA unter Tel. 877-409-4177, E-Mail: info@dummies.biz, oder besuchen Sie www.wiley.com/go/custompub. Für Informationen zur Lizenzierung der *Für Dummies*-Marke für Produkte oder Dienstleistungen kontaktieren Sie bitte: BrandedRights&Licenses@Wiley.com.

Danksagung des Verlags

Die folgenden Personen haben dabei geholfen, dieses Buch auf den Markt zu bringen:

Project Editor: Elizabeth Kuball

Acquisitions Editor: Ashley Coffey

Editorial Manager: Rev Mengle

Business Development Representative: Karen Hattan

Production Editor: Tamilmani Varadharaj

Spezielle Unterstützung: Rachel Ackerly, Lorraine Bellon, Scott Bower, Mary Briggs, John Damon, Tori Devereux, David Gormley, Dan Gould, Artsiom Holub, Gedeon Hombrebueno, Aivy Iniguez, Kate MacLean, Austin McBride, Ben Munroe, Mark Murtagh, Natalie Pino, Nicole Smith, Christina Soriano, Jolene Tam

Einführung

Die zunehmende Verbreitung von Ransomware ist in den vergangenen Jahren zu einem äußerst lukrativen kriminellen Geschäft geworden. Die betroffenen Organisationen glauben oft, es sei am kosteneffektivsten, ein Lösegeld zu zahlen, um ihre Daten zurückzubekommen – und leider stimmt das auch häufig.

Im Mai 2019 wurde die Stadt Baltimore Opfer eines Ransomware-Angriffs, der erhebliches Chaos verursachte. Es dauerte über eine Woche, bis Stadtbeamte wieder Zugriff auf kritische Infrastruktursysteme hatten. Die Wiederherstellung nach dem Angriff war schwierig und kostete die Stadt schätzungsweise 18 Millionen Dollar – wobei die Kriminellen nur 76.000 Dollar Lösegeld gefordert hatten.

Zwei kleinere Städte in Florida entschieden sich für einen anderen Ansatz. Im Juni 2019 beschlossen die Regierungen von Lake City und Riviera Beach nach Ransomware-Angriffen, die gesamte von den Angreifern geforderte Lösegeldsumme zu zahlen, um ihre Daten zurückzuerhalten. Die Entschlüsselung der gestohlenen Daten erforderte jedoch beträchtliche Arbeit. Die Städte zahlten den Hackern insgesamt 1 Million Dollar in Bitcoin. Forscher sind sich einig, dass Angriffe dieser Art immer häufiger stattfinden werden.

Was soll die nächste Stadt- oder Landesregierung tun, die von einem Ransomware-Angriff betroffen ist? Soll sie das geforderte Lösegeld zahlen oder mit dem langwierigen Prozess der manuellen Wiederherstellung ihrer kompromittierten Daten beginnen? In vielen Fällen ist es für Städte finanziell sinnvoller, das Lösegeld zu zahlen und ihre Zeit der Entschlüsselung ihrer Daten zu widmen, anstatt Geld für die Wiederherstellung ihrer Systeme auszugeben.

Laut einer Studie von IBM befürworten die meisten amerikanischen Steuerzahler nicht, dass ihre Steuergelder für die Zahlung von Ransomware-Forderungen verwendet werden. 80 Prozent der Befragten gaben an, sich über Ransomware-Angriffe auf ihre Stadt Sorgen zu machen, und 60 Prozent waren dagegen, dass ihre Regierungen Steuergelder verwenden, um Angreifern Lösegelder für die Rückgabe gestohlener Daten zu zahlen.

Das Problem besteht darin, dass jedes einzelne Unternehmen, das ein Lösegeld zahlt, die Entwicklung der nächsten Ransomware-Generation direkt mitfinanziert. So entstehen immer ausgeklügeltere Varianten, die gezieltere Angriffe ermöglichen. Die durch Ransomware-Angriffe

verursachten Kosten steigen ebenfalls. Laut einer aktuellen Studie von Cybersecurity Ventures werden Ransomware-Angriffe die Weltwirtschaft bis 2021 jährlich 6 Billionen US-Dollar kosten!

Soweit dies möglich ist, muss die Verbreitung von Ransomware verhindert werden. Ransomware muss erkannt werden, wenn sie versucht, Netzwerke anzugreifen, und sie muss eingedämmt werden, um den Schaden nach der Infizierung von Systemen und Endpunkten zu begrenzen. Zur Abwehr von Ransomware ist ein neuer architekturbasierter „Best-of-Breed"-Ansatz erforderlich, der die gesamte Organisation schützt und von der DNS-Ebene (Domain Name System) über das Rechenzentrum bis hin zu allen Endpunktgeräten greift – unabhängig davon, wo diese benutzt werden.

Über dieses Buch

Abwehr von Ransomware Für Dummies besteht aus fünf kurzen Kapiteln, in denen erläutert wird, wie Ransomware funktioniert, welche prägenden Merkmale sie hat (Kapitel 1), welche bewährten Sicherheitsverfahren (Best Practices) es gibt, um die mit Ransomware verbundenen Risiken zu reduzieren (Kapitel 2), warum eine neue Best-of-Breed-Sicherheitsarchitektur benötigt wird (Kapitel 3), was die Lösung Cisco Ransomware Defense zum Schutz vor Ransomware tun kann (Kapitel 4) und welche wichtigen Punkte Sie im Gedächtnis behalten sollte (Kapitel 5).

Annahmen über den Leser

Einem Zitat zufolge haben die meisten unserer Annahmen ihre Nutzlosigkeit überlebt. Ich erlaube mir trotzdem, einige Annahmen zu treffen:

Vor allem nehme ich an, dass Sie sich schon auf dem Gebiet der Datensicherheit auskennen. Vielleicht sind Sie eine Führungskraft im IT-Bereich, ein IT-Direktor, ein leitender IT-Architekt, Analyst, Manager oder ein Sicherheits-, Netzwerk- oder Systemadministrator. Dieses Buch wurde in erster Linie für technische Leser geschrieben, die bereits über Wissen im Bereich IT-Networking, Infrastruktur und Enterprise-Systeme verfügen.

Wenn Sie sich in diesen Annahmen wiedererkennen, dann ist dieses Buch für Sie! Wenn keine dieser Annahmen auf Sie zutrifft, sollten Sie trotzdem weiterlesen, denn dies ist ein sehr nützliches Buch, nach dessen Lektüre Sie genug über die Abwehr von Ransomware wissen, um gefährlich zu werden – zumindest für Angreifer!

In diesem Buch verwendete Symbole

In diesem Buch verwende ich gelegentlich besondere Symbole, um Ihre Aufmerksamkeit auf wichtige Informationen zu lenken. Sie werden auf die folgenden Hinweise stoßen:

MERKEN

Dieses Symbol macht auf Informationen aufmerksam, die Sie Ihrem nichtflüchtigen Speicher bzw. Ihrem Kopf anvertrauen sollten – neben all den Jubiläen und Geburtstagen!

TECHNISCHES

Den Schlüssel zum menschlichen Genom werden Sie hier nicht finden. Wenn Sie sich technisch aber noch verbessern wollen, sind Sie hier an der richtigen Stelle! Dieses Symbol erläutert den Jargon hinter dem Jargon und signalisiert, dass hier etwas tiefer auf technische Details eingegangen wird!

TIPP

Wir freuen uns, dass Sie sich für dieses Buch entschieden haben. Achten Sie auf diese Tipps! Dieses Symbol weist auf hilfreiche Empfehlungen und nützliche Informationen hin.

WARNUNG

Dieses Symbol macht auf Dinge aufmerksam, vor denen Sie Ihre Mutter schon immer gewarnt hat (oder auch nicht). Sie sollten diese Warnungen wirklich beherzigen, da sie Ihnen viel Zeit und Frust ersparen können!

Zusätzliche Informationen

Auf 48 Seiten können wir natürlich nur eine Auswahl der wichtigsten Themen behandeln. Wenn Sie am Ende dieses Buches unbedingt noch mehr erfahren wollen, gehen Sie einfach zu `https://umbrella.cisco.com/how-to-stop-ransomware`.

IN DIESEM KAPITEL

- Ransomware: prägende Merkmale
- Ransomware-Trends
- Wie Ransomware funktioniert

Kapitel 1
Was ist Ransomware?

Ransomware ist eine der am schnellsten wachsenden Malware-Bedrohungen und breitet sich epidemisch aus. Laut einem Bericht von Cybersecurity Ventures wurde 2019 alle 14 Sekunden ein weiteres Unternehmen Opfer eines Ransomware-Angriffs – bis 2021 wird es bereits alle 11 Sekunden geschehen. In diesem Kapitel erfahren Sie Näheres über Ransomware – was Ransomware ist, wie sie sich als Bedrohung weiterentwickelt und wie sie funktioniert.

Definition von Ransomware

Ransomware sind Schadprogramme (Malware), die bei einem Cyberangriff verwendet wird, um die Daten des Opfers zu verschlüsseln. Die Angreifer verwenden dazu einen Verschlüsselungscode, der nur ihnen bekannt ist, und fordern das Opfer auf, ein Lösegeld (gewöhnlich in einer *Kryptowährung* wie Bitcoin) zu zahlen, um wieder an die Daten zu gelangen.


TECHNISCHES

Eine Kryptowährung ist eine alternative digitale Währung, die Verschlüsselung verwendet, um das „Drucken" von Währungseinheiten (wie Bitcoins) zu regulieren und die Überweisung von Geldern zwischen Parteien zu verifizieren – ohne Zwischenhändler oder Banken.

Die Lösegeldbeträge sind gewöhnlich hoch, jedoch nicht exorbitant. Von Privatpersonen werden typischerweise Beträge zwischen 300 und 600 US-Dollar gefordert, während größere Organisationen meist mehr zahlen müssen. Dies ist ein beabsichtigtes Merkmal von Ransomware; es

soll Opfer dazu veranlassen, das Lösegeld so schnell wie möglich zu zahlen, anstatt sich mit Strafverfolgungsbehörden in Verbindung zu setzen und durch den Verlust von Daten und durch Negativschlagzeilen möglicherweise noch höhere direkte und indirekte Kosten in Kauf nehmen zu müssen. Allerdings nehmen diese Beträge im Laufe der Zeit zu, da die Angreifer beginnen, ihre Aufmerksamkeit auf Organisationen zu richten, die in der Lage sind, größere Beträge zu zahlen (und mehr zu verlieren haben). Die durchschnittliche Lösegeldforderung von Hackern für die Freigabe von Dateien, die durch ihre Lösegeldangriffe verschlüsselt wurden, hat sich 2019 auf über 12.000 Dollar fast verdoppelt, basierend auf Fällen, die von der Cybersicherheitsfirma Coveware bearbeitet wurden.

WARNUNG

Die Lösegeldbeträge können erheblich ansteigen, je länger das Opfer abwartet. Dies ist eine Taktik, mit der die Möglichkeiten des Opfers eingeschränkt werden sollen, damit es das Lösegeld so schnell wie möglich zahlt.

Ransomware in der modernen Bedrohungslandschaft

Ransomware ist keine neue Bedrohung. Das erste dokumentierte Beispiel für Ransomware war PC Cyborg, die 1989 begann, ihr Unwesen zu treiben. Seitdem hat sich Ransomware ständig weiterentwickelt und wird ständig raffinierter. Außerdem ist Ransomware im Zuge der folgenden Entwicklungen immer weitreichender und lukrativer geworden:

- **Digitale Transformation:** Da immer mehr Unternehmen ihre betrieblichen Abläufe digitalisieren und Mitarbeiter E-Mail, Cloud-Apps und Mobilgeräte zur Erledigung ihrer Arbeit verwenden, nimmt die Anzahl potenzieller Einstiegspunkte für Angreifer exponentiell zu. Sind sie erst in ein Netzwerk eingedrungen, können sich Infektionen schneller ausbreiten, wenn kritische Systeme angeschlossen sind.
- **Aufstieg von Kryptowährung:** Kryptowährung (wie Bitcoin) ermöglicht einfache und praktisch nicht zurückverfolgbare Zahlungen an anonyme Cyberkriminelle. Da Spekulationen mit Kryptowährung die Preise weiter in die Höhe treiben, wächst das Potenzial für hohe Lösegelder proportional.
- **Einführung von Ransomware-as-a-Service (RaaS):** *RaaS* (Ransomware, die für eine geringe Gebühr und/oder einen Prozentsatz der Lösegeldzahlung erworben werden kann), macht es für nahezu jeden leicht, Ransomware zu benutzen.

Trotz Aufsehen erregender Medienberichte über massive Verletzungen der Datensicherheit bei Organisationen und Unternehmen wie dem Amt für Personalverwaltung der Vereinigten Staaten (Office of Personnel Management – OPM), Equifax, Target, Home Depot und Capital One, ist der Aufstieg von Ransomware für Organisationen und Unternehmen zu einer allgegenwärtigen Bedrohung geworden – ebenso für Privatpersonen.

WARNUNG

Laut einem Bericht von Kaspersky brauchten 34 Prozent der Unternehmen, die einen Ransomware-Angriff erlitten, eine Woche oder länger, um ihre Daten zurückzuerlangen. Was würden Sie tun, wenn Ihr Unternehmen eine Woche lang in dieser Situation wäre?

Locky ist ein Beispiel für eine aggressive Ransomware-Variante, die 2016 täglich bis zu 90.000 Opfern Schaden zufügte. Zu dieser Zeit lag der durchschnittliche Lösegeldbetrag für Locky gewöhnlich zwischen 0,5 und 1 Bitcoin. Nach Statistiken von Ciscos Sicherheitssparte Talos zahlen durchschnittlich 2,9 Prozent der von einem Ransomware-Angriff betroffenen Opfer das Lösegeld. In diesem Fall könnte Locky in einem Zeitraum von 12 Monaten potenziell bis zu 33 Millionen Opfer infizieren und zu Lösegeldzahlungen zwischen 287 und 574 Millionen US-Dollar führen (siehe Tabelle 1-1).

TABELLE 1-1 Geschätzte Locky-Lösegeldzahlungen

Lösegeldbetrag	1 Bitcoin	0,5 Bitcoin
Opfer/Tag	90.000	90.000
Anzahl der Zahlungen/Tag	2.610	2.610
Bitcoin-Preis (2.Oktober 2016)	610,82 $ = 1 Bitcoin	610,82 $ = 1 Bitcoin
Profit an einem Tag	1.594.240 $	797.120 $
Profit in einem Monat	47.826.206 $	23.913.603 $
Profit in 12 Monaten	573.926.472 $	286.963.236 $

Wenngleich eine geschätzte Summe von 287 Millionen US-Dollar im Vergleich zu einer einzigen Datenschutzverletzung trivial erscheinen mag (etwa dem Target-Datenklau von 2013, der das Unternehmen Schätzungen zufolge über 300 Millionen US-Dollar kostete), sollte man nicht vergessen, dass die mit Datenschutzverletzungen verbundenen geschätzten Verluste auf den Kosten für die betroffenen Organisationen basieren – nicht auf den Kosten für die einzelnen Opfer, deren

Identitäten und/oder Kreditkartenangaben gestolen wurden. Die Kosten für die Organisation umfassen:

- **Gesetzliche Geldbußen und Strafen**, die von unterschiedlichen Aufsichtsgremien wie Payment Card Industry (PCI) verhängt werden
- **Rechtskosten**, die sich aus den mit einer Datenpanne verbundenen Rechtsstreitigkeiten ergeben
- **Entgangene Geschäftsmöglichkeiten** auf Grund von Geschäftsunterbrechungen, Markenschädigung und Verlust von Kunden
- **Problembehebung** einschließlich Vorfallsreaktion und Wiederherstellung, Öffentlichkeitsarbeit, Anzeige von Datenschutzverletzungen und Credit-Monitoring-Services für betroffene Personen

TIPP

Laut dem Ponemon Institute entstanden den 2019 von einer Datenschutzverletzung betroffenen Organisationen im Durchschnitt Kosten in Höhe von 3,92 Millionen US-Dollar – ein Anstieg von 12 Prozent gegenüber 2014.

Gleichzeitig war Locky 2018 weiterhin aktiv, als sich der Preis von Bitcoin um *mehr als das Zehnfache* erhöht hatte – am 2. Oktober 2018 war ein einziger Bitcoin über 6.500 Dollar wert! Da es keine Obergrenze für die Preise von Kryptowährung gibt, kann Ransomware zu einer großen finanziellen Belastung für anvisierte Unternehmen werden.

Cyberkriminelle verkaufen oft gestohlene Kreditkarten- und Identitätsangaben im *Dark Web* – einem anonymen Bereich des Webs (wo Schwarzmarkt-Drogenhandel, Verkauf von Kinderpornographie, Cyberkriminalität und andere Aktivitäten stattfinden, die sich der Überwachung oder Zensur entziehen wollen), welches spezielle Software, Konfiguration und/oder Autorisierung für den Zugriff erfordert – oft für wenige Cents oder Dollar pro Datensatz. Im Vergleich dazu kann ein Cyberkrimineller mit Lösegeldern von einzelnen Opfern oder Organisationen, die direkt an ihn gezahlt werden, hunderte bis zehntausende Dollar einnehmen.

Die tatsächlichen Kosten für die Opfer von Identitätsdiebstahl und Kreditkartenbetrug beliefen sich laut der Studie *2016 Identity Fraud* von Javelin Strategy and Research im Jahr 2015 auf 15 Milliarden US-Dollar. Eine weiterführende Studie ergab, dass Identitätsdiebstahl und Kreditkartenbetrug weiter abgenommen hatten – von 8,1 Milliarden US-Dollar im Jahr 2017 auf 6,4 Milliarden US-Dollar im Jahr 2018. Im Gegensatz zu der abnehmenden Entwicklung bei Identitätsdiebstahl und Kreditkartenbetrug (die wahrscheinlich auf strengere Sicherheitsmaßnahmen zurückzuführen ist), nehmen viele andere Cyberattacken – einschließ-

lich Ransomware – immer mehr zu. Untersuchungen von Accenture deuten darauf hin, dass bis zum Jahr 2023 weltweit fast 5,2 Billionen Dollar durch Cyberangriffe gefährdet sein könnten.

Da Ransomware-Angriffe immer größere wirtschaftliche Auswirkungen haben, ändern sich auch die Angriffsmuster. Anstatt Lösegeld von Einzelpersonen und kleinen Unternehmen zu fordern, operieren Angreifer verstärkt nach dem Motto „Qualität vor Quantität". Eine Studie von F-Secure ergab, dass immer mehr Angreifer ihr Netz nicht mehr weit auswerfen, sondern ihre Angriffe ganz gezielt ausrichten, um ihre Chancen auf eine hohe Auszahlung zu erhöhen. Die Lösegeldzahlungen für Ryuk sind zum Beispiel oft viel höher als durchschnittliche Lösegeldzahlungen, da Ryuk-Angriffe gezielt auf mittelgroße bis große Organisationen mit einer größeren Zahlungsfähigkeit ausgeführt werden.

Auch die Ransomware-Vektoren ändern sich. Früher verschickten Kriminelle eine große Anzahl von Phishing-E-Mails und hofften, dass einige Empfänger in die Falle tappen und ihre Netzwerke Ransomware-Angriffen aussetzen würden. Jetzt gibt es immer mehr Ransomware-Varianten, die Schwachstellen in Remote-Desktop-Protokollen ausnutzen, um in das Netzwerk einzudringen, wobei sie sich ungepatchte Systeme und Zero-Day-Exploits zunutze machen.

Wie Ransomware funktioniert

Ransomware wird gewöhnlich durch Exploit-Kits, *Wasserloch-Angriffe* (bei denen eine häufig besuchte Website mit Malware infiziert wird), *Malvertising* (schädliche Werbung) oder E-Mail-Pishingkampagnen verbreitet (siehe Abbildung 1-1).

TIPP

Gehen Sie zu `https://learn-umbrella.cisco.com/product-videos/ransomware-anatomy-of-an-attack`, um mehr über die Anatomie eines Ransomware-Angriffs zu erfahren.

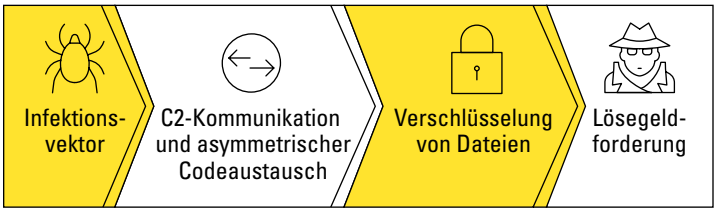


ABBILDUNG 1-1: Wie Ransomware einen Endpunkt infiziert.

Nach der Verteilung identifiziert die Ransomware normalerweise Benutzerdateien und Daten, die über eine Art eingebetteter Dateierweiterungsliste verschlüsselt werden sollen. Die Ransomware ist auch so programmiert, dass die Interaktion mit bestimmten Systemverzeichnissen vermieden wird (z. B. mit dem WINDOWS-Systemverzeichnis oder bestimmten Programmdateien-Verzeichnissen), um die Systemstabilität für die Lieferung des Lösegelds sicherzustellen, wenn der Payload nicht mehr läuft. Dateien an bestimmten Orten, die einer der aufgelisteten Dateierweiterungen entsprechen, werden dann verschlüsselt. Anderenfalls bleiben die Dateien verschont. Nach der Verschlüsselung der Dateien hinterlässt die Ransomware gewöhnlich eine Nachricht für den Benutzer, die Anleitungen zur Zahlung des Lösegelds enthält (siehe Abbildung 1-2).

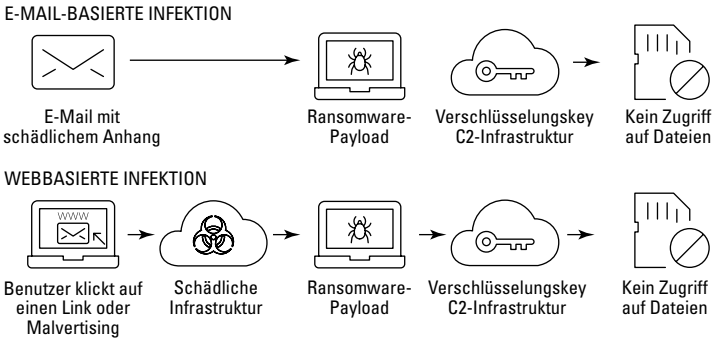


ABBILDUNG 1-2: Wie Ransomware funktioniert.

WARNUNG

Es gibt keine Ehre unter Dieben. Zwar stellen Angreifer gewöhnlich den zur Entschlüsselung Ihrer Dateien erforderlichen Schlüssel zur Verfügung stellen, nachdem sie das Lösegeld erhalten haben. Es gibt jedoch keine Garantie dafür, dass die Angreifer keine andere Malware und Exploit-Kits auf Ihrem Endpunkt oder anderen Netzwerksystemen installiert haben oder dass sie Ihre Daten nicht zu anderen kriminellen Zwecken verwenden oder versuchen, in Zukunft weitere Zahlungen zu erzwingen.

IN DIESEM KAPITEL

- Proaktive Verteidigung gegen Ransomware
- Automatisierte Abwehr von Ransomware und schnelle Reaktion auf Sicherheitsvorfälle
- Neuorganisierung nach einem Angriff

Kapitel 2
Best Practices zur Reduzierung von Ransomware-Risiken

In diesem Kapitel gehe ich auf die besten Sicherheitsmethoden und Strategien zur Risikominderung ein, die Ihrer Organisation, sofern sie umfassend und korrekt angewendet werden, bei der Abwehr von Ransomware und anderen Bedrohungen der Cybersicherheit helfen können.

Vor einem Angriff: Erkennen, durchsetzen und stärken

Nach Ansicht der MITRE Corporation, einer gemeinnützigen Organisation mit umfangreicher Beratertätigkeit für die Regierung, ist Angriff die beste Verteidigung gegen Cyber-Angriffe, besonders wenn starke Angriffs- und Verteidigungsteams zusammenarbeiten. Es gibt eine Reihe bewährter Verfahren, die Organisationen proaktiv implementieren können, bevor sie zum Ziel eines Angriffs werden. Wenn Angreifern der Einstieg nicht sofort gelingt, d. h. wenn sie keinen Fuß in die Tür bekommen, werden sie höchstwahrscheinlich ein anderes Opfer ins Visier nehmen – es sei denn, Ihr Unternehmen wird gezielt angegriffen.

Ransomware-Angriffe können opportunistisch sein – das Motiv der Angreifer sind oft Gewinne mit möglichst wenigen Risiken und Anstrengungen. Die effektivste Art, um die Angriffskette zu durchbrechen und Ransomware-Angriffe im Keim zu ersticken, besteht deshalb darin, Angreifer mit einem architekturbasierten Ansatz am Eindringen in Ihr Netzwerk zu hindern.

MERKEN

Die MITRE ATT&CK Matrix ist ein Framework, das Taktiken, Techniken und Verfahren beschreibt, die von Angreifern in verschiedenen Phasen verwendet werden, um Zugang zu Systemen zu erhalten und Cyberattacken zu starten. Die ATT&CK-Kategorien sind (in zeitlicher Reihenfolge):

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control (C2)
- Exfiltration
- Impact

Die ersten sechs Kategorien zielen darauf ab, Zugang zum Netzwerk und zu den Systemen der anvisierten Organisation zu erlangen.

Angreifer erhalten gewöhnlich durch eine der beiden folgenden Methoden Zugriff auf ihr Ziel:

- Social Engineering/Phishing, um einen ahnungslosen Benutzer zur Offenlegung seiner Netzwerk-Anmeldeinformationen zu bringen oder Malware zu installieren
- Verwendung legitimer Anmeldeinformationen, die gestohlen oder verkauft und oft durch eine Datenschutzverletzung offengelegt worden sind
- Ausnutzung einer Schwachstelle in einer öffentlich zugänglichen (Internet) Anwendung oder Dienstleistung

MERKEN

In seinem Data Breach Investigations Report 2019 stellte Verizon fest, dass Benutzer durch soziale Angriffe sind, die über Mobilgeräte ausgeführt werden, leichter verwundbar sind. Dafür gibt es zwei Gründe:

- Mobilgeräte sind klein und die Benutzerschnittstellen erschweren die Entscheidung, ob eine E-Mail oder Website legitim ist.
- Benutzer verwenden ihre Mobilgeräte oft beim Gehen, Sprechen, Fahren oder bei anderen Aktivitäten, die ihre Aufmerksamkeit einschränken können.

TIPP

Die folgenden Best Practices sollten implementiert werden, um Angreifer am Zugriff auf das Netzwerk und die Systeme Ihres Unternehmens zu hindern:

- **Durchführung regelmäßiger Maßnahmen zur Schulung des Sicherheitsbewusstseins Ihrer Endbenutzer.** Diese Schulungen sollten interessant gestaltet werden und die aktuellsten Informationen zu Sicherheitsbedrohungen und Taktiken enthalten. Sie sollten Folgendes tun:
  - Unternehmensinterne Richtlinien zu folgenden Punkten durchsetzen: kein Austausch und keine Offenlegung von Benutzerdaten (selbst gegenüber IT- und/oder Sicherheitspersonal), starke Passwortanforderungen und die Bedeutung der Authentifizierung für die Sicherheit (einschließlich des Konzepts der *Nachweisbarkeit*, das Nutzern die Verteidigungsmöglichkeit „Ich war es nicht!" gibt).
  - Die Benutzung zugelassener SaaS-Anwendungen (Software-as-a-Service – SaaS) wie Filesharing-Programmen fördern, damit weniger E-Mail-Anhänge versendet und Phishing-Angriffe mit bösartigen Anhängen reduziert (oder vollkommen eliminiert) werden.
  - Nicht natives Rendering für PDF- und Microsoft-Office-Dateien in der Cloud in Erwägung ziehen. Desktop-Anwendungen wie Adobe Acrobat Reader und Microsoft Word enthalten oft ungepatchte Schwachstellen, die ausgenutzt werden können.
  - Benutzer, die nicht regelmäßig Makros verwenden, dazu anhalten, niemals Makros in Microsoft-Dokumenten zu aktivieren. Vor kurzem wurde eine erneute Zunahme von makrobasierter Malware beobachtet, die komplexe Verschleierungsmethoden einsetzt, um sich der Entdeckung zu entziehen.
  - Verfahren zur Meldung von Vorfällen erklären und sicherstellen, dass Benutzer kein Problem damit haben, Vorfälle zu

melden, indem ihnen die Botschaft vermittelt wird: „Sie sind das Opfer, nicht der Täter" und „Das Vertuschen ist schlimmer (was den Schaden betrifft) als der Vorfall."

- An die physische Sicherheit denken. Obwohl sie weniger verbreitet sind als andere Formen von Social Engineering, sollten Benutzer immer wieder an die Richtlinien zur Besucherbegleitung und Taktiken wie Mülleimertauchen, Schulter-Surfen und Piggybacking (oder Tailgating) erinnert werden, die ihre persönliche Sicherheit und die Sicherheit ihrer Daten gefährden können.

» **Durchführung kontinuierlicher Risikobewertungen, um Sicherheitslücken und Schwachstellen in Ihrer Organisation zu erkennen, Bedrohungen zu verhindern und Risiken zu reduzieren**. Sie sollten:

- Regelmäßige Port- und Schwachstellen-Scans durchführen
- Für ein solides und zeitgerechtes Patch-Management sorgen
- Unnötige und verletzbare Services deaktivieren und Anleitungen zur Systemhärtung befolgen.
- Starke Passwortanforderungen durchsetzen und eine Zwei-Faktor-Authentifizierung implementieren (soweit dies möglich ist).
- Security Logging auf einem sicheren Log Collector oder einer SIEM-Plattform (Security Incident and Event Management) zentralisieren und Protokollinformationen häufig prüfen und analysieren.

TECHNISCHES

In der Vergangenheit erforderte die meiste Ransomware eine Form der Benutzerinteraktion, z. B. das Öffnen eines E-Mail-Anhangs oder das Klicken auf einen bösartigen Link, oder die Nutzung ungepatchter Systeme. Bei einigen Ransomware-Varianten ist die Hilfe eines Benutzers jedoch nicht erforderlich, um einen Angriff zu starten. Die Ransomware-Variante Sodinokibi nutzte eine kürzlich bekannt gewordene Sicherheitslücke in Oracle WebLogic aus, um Ransomware auf einen Server herunterzuladen und einen Angriff zu starten, bevor ein Patch zum Beenden des Angriffs veröffentlicht werden konnte.

Trotz bester Bemühungen wird es immer Zero-Day-Bedrohungen geben, die bislang unbekannte – und daher ungepatchte – Schwachstellen ausnutzen. Wenn es einem Angreifer gelingt, auf Ihr Netzwerk zuzugreifen, wird er als nächstes versuchen, eine C2-Kommunikation herzustellen, um

- einen fortdauernden effektiven Angriff sicherzustellen
- Privilegien zu eskalieren
- sich lateral durch Ihr Netzwerk, Rechenzentrum und Ihre Endbenutzerumgebung zu bewegen

Um die Auswirkungen eines Angriffs zu begrenzen, sollten Sie die folgenden Sicherheitsverfahren implementieren:

- Für Schutz auf DNS-Ebene (Domain Name System) sorgen, der es Ihnen ermöglicht, gefährliche Domains, IP-Adressen und Internet-Infrastruktur vorausschauend zu identifizieren, um das Risiko eines Angriffs zu reduzieren .
- Automatisch Schutzmaßnahmen wie Firewalls, fortgeschrittenen Malware-Schutz, Verschlüsselung und Data Loss Prevention an allen Endpunkten einschließlich persönlichen Mobilgeräten (sofern „Bring-Your-Own-Device" [BYOD] gestattet ist) und Wechselmedien (wie USB-Laufwerken) einsetzen, die Benutzern gegenüber transparent sind und keine Benutzereingriffe erfordern. Dies schützt Roaming- und Remote-Nutzer innerhalb und außerhalb des Netzwerks, selbst wenn sie nicht immer die besten Verfahren und geltenden Richtlinien befolgen.
- Sicherheitsfunktionen für E-Mail-Gateways aktivieren, darunter Blockieren oder Entfernen von ausführbaren Dateien und anderen potenziell bösartigen Anhängen, SPF-Verifizierung (Sender Policy Framework), um E-Mail-Spoofing und E-Mail-Throttling (oder „Greylisting") und potenzielle Spam-E-Mails zu reduzieren.
- Sicherheitsprodukte und -services einsetzen, die den Internetverkehr, E-Mails und Dateien analysieren, um die Infizierung und Datenexfiltration (in Kapiteln 3 und 4 näher erläutert) zu verhindern, und Threat-Intelligence-Services einen tieferen Kontext und eine schnelle Untersuchung nutzen.
- Eine robuste, inhärent sichere Architektur entwickeln und einsetzen, die Segmentierung verwendet, um die laterale Bewegung von Angreifern in Ihrer Umgebung einzuschränken.
- Das Least-Privilege-Prinzip durchsetzen und „Privilege Creep" bei Benutzern eliminieren, damit Angreifer Privilegien nicht eskalieren können.
- Regelmäßig kritische Systeme und Daten sichern und in regelmäßigen Abständen alle Backups testen, um sicherzustellen, dass sie in einem guten Zustand sind und wiederhergestellt werden können. Verschlüsseln Sie auch Ihre Sicherheitskopien und bewahren Sie diese offline oder in einem getrennten Backup-Netzwerk auf.

» Ihre Reaktionsfähigkeit auf Sicherheitsvorfälle testen und bewerten und die gesamte Effektivität Ihrer Verteidigung kontinuierlich überwachen und messen.

TIPP

Die meiste Ransomware stützt sich auf eine robuste C2-Kommunikationsinfrastruktur, um beispielsweise Verschlüsselungscodes und Zahlungsbotschaften zu senden. Eine Organisation, die Angreifer daran hindert, sich mit Ransomware zu verbinden, die ihr Netzwerk infiziert hat, kann einen Ransomware-Angriff erfolgreich abwehren. Wenn ein Angreifer zum Beispiel nicht in der Lage ist, Verschlüsselungscodes an einen infizierten Endpunkt zu senden oder einem Opfer mitzuteilen, wie es eine Lösegeldzahlung vornehmen soll, schlägt der Ransomware-Angriff fehl. Wie Tabelle 2-1 zeigt, stützen sich die verbreitetsten Ransomware-Varianten bei der C2-Kommunikation heutzutage stark auf das DNS. In einigen Fällen wird auch ein Tor-Browser (The Onion Router) für die C2-Kommunikation verwendet. Es ist daher wichtig, dass beide Kommunikationsarten mit einer Methode wie einem Proxy blockiert werden können.

TABELLE 2-1 C2-Kommunikation bei Ransomware

Name	Verschlüsselungscode	Zahlungsnachricht
Locky	DNS	DNS
TeslaCrypt	DNS	DNS
CryptoWall	DNS	DNS
TorrentLocker	DNS	DNS
PadCrypt	DNS	DNS, Tor
CTB-Locker	DNS, Tor	DNS
FAKBEN	DNS	DNS, Tor
PayCrypt	DNS	DNS
KeyRanger	DNS, Tor	DNS

Während eines Angriffs: Erkennen, blockieren und abwehren

Wenn Ihr Unternehmen angegriffen wird, ist eine schnelle und effektive Reaktion erforderlich, um den Schaden in Grenzen zu halten. Jede Situation erfordert bestimmte Maßnahmen und Anstrengungen. Während

eines Angriffs ist jedoch nicht der richtige Zeitpunkt, um herauszufinden, ob Ihr Unternehmen effektiv auf Sicherheitsverletzungen reagieren kann oder nicht! Ihre Reaktion auf Sicherheitsvorfälle muss gut koordiniert sein und von allen Beteiligten gut verstanden werden. Dafür ist zu sorgen, bevor es zu einem Angriff kommt. Außerdem muss Ihre Reaktion auf Sicherheitsvorfälle gut dokumentiert werden und wiederholbar sein, damit Sie Vorfälle nach dem Angriff rekonstruieren, daraus lernen und Verbesserungsmaßnahmen ergreifen können.

Ein entscheidender Faktor für eine effektive Reaktion auf Sicherheitsvorfälle – und das wird häufig übersehen – ist der Informationsaustausch, d. h.:

- **Allen Stakeholdern rechtzeitig korrekte Informationen zukommen lassen:** Führungskräfte müssen alle relevanten Informationen erhalten, damit angemessene Ressourcen zugewiesen werden können, um eine adäquate Reaktion auf Vorfälle und die Behebung von Problemen sicherzustellen, so dass damit kritische und informierte Geschäftsentscheidungen getroffen werden können und Mitarbeiter, Strafverfolgungsbehörden, Kunden, Anleger und die allgemeine Öffentlichkeit ihrerseits angemessene Informationen erhalten.
- **Automatisch neue Security Intelligence über die gesamte Architektur hinweg verbreiten:** Das Zusammenführen kritischer Daten aus unterschiedlichen Systemen wie Security Information and Event Management (SIEM), Threat-Intelligence und Sandbox-Tools ermöglicht es dem Incident Response Team, Sicherheitsvorfälle mit erheblichen Auswirkungen effektiv zu erkennen und vorzuselektieren. Wenn zum Beispiel ein neuer Malware-Payload an einem Endpunkt entdeckt wird, sollte er automatisch zur Analyse an eine cloudbasierte Threat-Intelligence-Plattform weitergeleitet werden, um Indicators of Compromise (IoCs) zu finden und zu extrahieren . Dann sollten neue Gegenmaßnahmen automatisch implementiert und durchgeführt werden.

Nach einem Angriff: Betrachten, kontrollieren und beheben

Nach einem Angriff sind die folgenden Maßnahmen erforderlich:

TIPP

- Die normalen Geschäftsabläufe wieder aufnehmen, darunter Wiederherstellung von Backups und Reimaging-Systemen
- Beweismaterial für die Strafverfolgung und Prüfung erfassen und aufbewahren

- Forensische Daten analysieren, um künftige Angriffe vorherzusehen und zu verhindern, zum Beispiel durch das Identifizieren von verbundenen Domains und Malware mit zugehörigen IP-Adressen, File-Hashes und Domains
- Ursachenanalyse durchführen, Lehren ziehen und soweit erforderlich Sicherheitsressourcen umgruppieren

Prädiktive Threat Intelligence verhilft Ihrem Unternehmen zu einer proaktiven Sicherheitsposition und versetzt Sie in die Lage, die C2-Infrastruktur, die Angreifer für gegenwärtige und zukünftige Angriffe ausnutzen, klar zu erkennen und dadurch der Bedrohung immer einen Schritt voraus zu sein.

IN DIESEM KAPITEL

- Best-of-Breed oder All-in-One
- Das Beste aus beiden Welten mit einem integrierten Sicherheitsportfolio

Kapitel 3
Entwicklung einer neuen „Best-of-Breed"-Sicherheitsarchitektur

In diesem Kapitel betrachten wir die gegenwärtig verwendeten Sicherheitsarchitekturen und deren Herausforderungen und stellen sie einer neuen „Best-of-Breed"-Architektur gegenüber, die in der Lage ist, besser gegen Bedrohungen vorzugehen – einschließlich Ransomware.

Die Einschränkungen gegenwärtiger Sicherheitsarchitekturen

In der Vergangenheit glaubten viele Unternehmen, in puncto Sicherheit eine Wahl zwischen zwei Optionen treffen zu müssen:

- Sie konnten Best-of-Breed-Produkte erwerben, die zwar bestimmte neue Bedrohungsarten effektiv abwehrten, sich aber nicht vollständig in einen architekturbasierten Ansatz zur Integration von Sicherheitslösungen eingliedern ließen.
- Sie konnten einen systembasierten Ansatz wählen und eigenständige (oder punktuelle) Sicherheitsprodukte, die „gut genug" waren, in eine intelligente Systemarchitektur aufnehmen.

Viele Unternehmen verwenden heute eine hierarchische Netzwerkarchitektur, die aus einer Zugriffsschicht, einer Verteilungsschicht und einer Kernschicht mit mehreren eigenständigen Sicherheitsprodukten besteht, die in einer DMZ oder lokalen Servicezone eingesetzt werden, z. B. einer Firewall und/oder einem Web-Proxy-Server. Leider ist dies nicht dasselbe wie eine echte „Defense-in-Depth"-Strategie (siehe Abbildung 3-1).

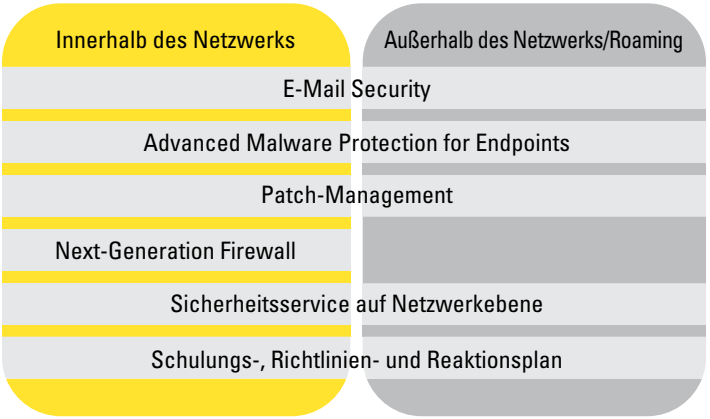


ABBILDUNG 3-1: Sicherheit erfordert die Verwaltung von Risiken über verschiedene Schichten hinweg.

Die derzeitigen Ansätze weisen die folgenden Einschränkungen auf:

- **Es gibt keine Integration oder Korrelation.** Zu viele eigenständige Sicherheitsprodukte überschwemmen die begrenzten Sicherheitsressourcen zwangsläufig mit weitschweifigen, unkoordinierten Informationen, die nicht leicht analysiert werden können, sodass Sicherheitsteams oft nach der sprichwörtlichen „Nadel im Heuhaufen" suchen müssen.
- **Perimeterbasierte Sicherheit ist nur ein Teil einer effektiven Architektur.** Firewalls, sichere Web-Gateways und Sandbox-Technologien, die nur am Netzwerkrand eingesetzt werden, sehen nur den Nord-Süd-Verkehr, der das Internet durchläuft. Der Ost-West-Verkehr im Rechenzentrum, d. h. der Verkehr zwischen Anwendungen und Endbenutzern, kann bis zu 80 Prozent des gesamten Netzwerkverkehrs ausmachen. Daher ist eine vollkommene Transparenz im gesamten Netzwerk erforderlich.

- **Die Mitarbeiter haben das Gebäude verlassen.** Nicht nur haben Cyberkriminelle ihre Vorgehensweise (ihre Taktiken und Methoden) geändert – ebenfalls verändert hat sich die Art, wie Benutzer arbeiten und digital interagieren. Da immer mehr Remote- und Roaming-Benutzer unterwegs sind und mit unterschiedlichen Geräten direkt über die Cloud arbeiten, sind perimeterbasierte Sicherheitstechnologien und Virtual Private Networks (VPNs) nicht mehr in der Lage, Geräte und Unternehmensdaten umfassend zu schützen. Auf viele cloudbasierte Services (wie Salesforce.com und Office 365) kann leicht ohne eine VPN-Verbindung zugegriffen werden, und diese Anwendungen und Daten werden nur durch einfache Sicherheitsmechanismen wie Antimalware-Schutz abgesichert. Laut der Enterprise Strategy Group gehen 79 Prozent der Unternehmen dazu über, in Zweigniederlassungen direkt auf das Internet zuzugreifen (DIA), wodurch sie traditionelle Sicherheitsvorrichtungen an der Peripherie umgehen und die Benutzer der Gefahr von Angriffen aussetzen. Moderne Sicherheitslösungen müssen es Ihrem Unternehmen ermöglichen, die Cloud zu nutzen und von jedem Gerät, überall und jederzeit zu arbeiten – und dabei den bestehenden Schutz weit über den traditionellen Netzwerkperimeter hinaus zu erweitern.
- **Es ist keine ausreichende Transparenz vorhanden.** Herkömmliche portbasierte Firewalls sind vielen Bedrohungen gegenüber blind, die Umgehungstechniken wie nicht standardisierte Ports, Port-Hopping und Verschlüsselung verwenden.
- **Es gibt keine ausreichende Segmentierung und herkömmliche Segmentierung kann problematisch sein.** Netzwerke werden gewöhnlich in „vertrauenswürdige" und „nicht vertrauenswürdige" Zonen mit statischen Virtual LANs (VLANs) segmentiert, die auf Switches definiert sind, welche oft schwer zu konfigurieren und zu warten sind. Diese willkürliche Struktur berücksichtigt jedoch nicht die neue Normalität in modernen Rechenzentren – virtuelle Maschinen (VMs), die sich dynamisch durch Rechenzentren und in der Cloud bewegen. Stattdessen muss die mehrfache granulare Segmentierung (einschließlich Mikrosegmentierung) an Netzwerkgeräten im gesamten Rechenzentrum mit dynamischer softwaredefinierter Segmentierung definiert werden.
- **Statische Updates sind nur der Anfang.** Das Herunterladen und Installieren von Anti-Malware-Signaturdateien ist lediglich der Ausgangspunkt für eine effektive Bekämpfung von Zero-Day-Bedrohungen, die sich ständig weiterentwickeln. Wie können Sie sich vor unbekannten und Zero-Day-Bedrohungen schützen und wie gut sind Sie darauf vorbereitet, mit gutartigen Dateien umzugehen, die

plötzlich bösartig werden? Statische Signaturdateien müssen mit cloudbasierter Threat Intelligence in Echtzeit und einem dynamischeren und kontinuierlichen Sicherheitsansatz unterstützt werden – für das riskanteste 1 Prozent der Angriffe, die zu kostspieligen Sicherheitsverletzungen führen können.

Definition der neuen Best-of-Breed-Sicherheitsarchitektur

Um Unternehmen vor Ransomware und anderen modernen Bedrohungen zu schützen, macht sich die neue „Best-of-Breed"-Sicherheitsarchitektur anstatt der herkömmlichen punktuellen Produkte einen integrierten, portfoliobasierten Ansatz zunutze, der einfach, offen und automatisiert ist. Diese neue Architektur

- ermöglicht es, automatisch auf Threat Intelligence zurückzugreifen und Daten in einem umfassenden Rahmen und in Verbindung mit anderen Sicherheitsprodukten und -services zu aggregieren und zu korrelieren – sowohl On-Premises als auch in der Cloud
- reduziert die Komplexität und sorgt für eine vollständige Transparenz in der gesamten Umgebung
- ermöglicht eine bessere Integration mit neuen und vorhandenen Sicherheitsinvestitionen und verwendet offene, erweiterbare Standards und Technologien
- verwendet Integrationsmethoden, um eine automatisierte Sicherheitsreaktion zu gewährleisten, damit Sicherheit effektiver wird und andere IT-Teams weniger belastet werden

Was bedeutet das für Ihr Unternehmen? Diese neue Best-of-Breed-Sicherheitsarchitektur erkennt mehr Bedrohungen schneller und ermöglicht eine bessere Behebung und Prävention in der Zukunft. Ein plattformbasierter Ansatz bietet Ihnen das nötige Kontextbewusstsein, um die einzelnen Bedrohungssignale zusammenzusetzen, die jedes für sich bei der Analyse übersehen werden könnten. Darüber hinaus hilft er Bedrohungsjägern, nicht nur zu verstehen, welche Bedrohungen sich in ihrer Umgebung befinden, sondern auch, wie sie überhaupt dorthin gelangt sind – und andere daran zu hindern, in die Umgebung einzudringen.

Diese neue Best-of-Breed-Sicherheitsarchitektur besteht aus den folgenden Komponenten (siehe Abbildung 3-2):

- Next-Generation Firewalls (NGFWs) und Next-Generation Intrusion-Prevention-Systeme (NGIPSs) mit Transparenz über schädliche Vorfälle samt Datenanreicherung von anderen Sicherheitsprodukten
- Threat Intelligence aus branchenführenden Quellen und Cloud-basierte Produktdaten, mit der Möglichkeit, Daten zu hochaktuellen Vorfällen für weitere Untersuchungen und Reaktionen zu erfassen und zu priorisieren
- Schutz auf DNS-Ebene (Domain Name System), um den Schutz über die Firewalls des Unternehmens hinaus zu erweitern
- Sicherer Web-Gateway zum Schutz aller Ports und Protokolle
- Cloud Access Security Broker (CASB) zum Schutz vor riskanten, nicht zugelassenen Cloud-Anwendungen
- Hochgranulare, softwaredefinierte Netzwerk-Segmentierung mit rollenbasierter Durchsetzung von Richtlinien – unabhängig von Standort, Gerät oder IP-Adresse
- E-Mail-, Web- und Endpunktsicherheit, um die Transparenz zu erweitern und Bedrohungen zu korrelieren
- Fortschrittlicher Malware-Schutz mit Sandbox-Funktionen vom Netzwerk bis zum Endpunkt
- Automatisierte Plattform-Integrationen in Verbindung mit zentralisierter Transparenz und Verwaltung, um Komponenten miteinander zu verknüpfen und Ihrem Sicherheitsteam die Arbeit zu erleichtern

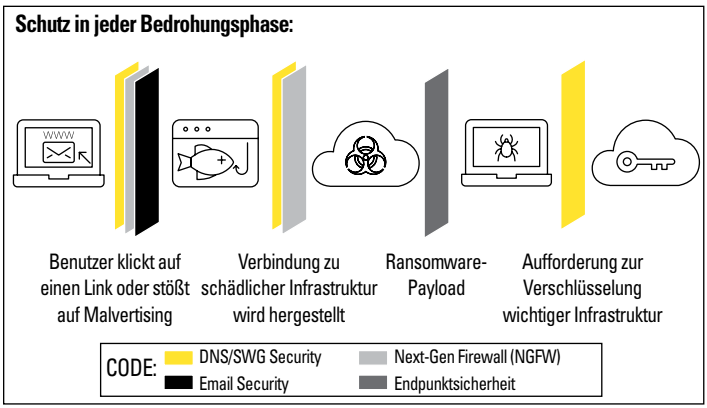


ABBILDUNG 3-2: Die neue Best-of-Breed-Sicherheitsarchitektur bietet mit Defense-in-Depth die bestmögliche Verteidigung gegenüber Bedrohungen.

TIPP

In Kapitel 4 erfahren Sie mehr über den Sicherheitsansatz von Cisco und die neue Best-of-Breed-Sicherheitsarchitektur mit Cisco Ransomware Defense. Abbildung 3-3 zeigt Cisco Security-Produkte, die Ransomware-Angriffe erkennen, auf sie reagieren und sie verhindern.

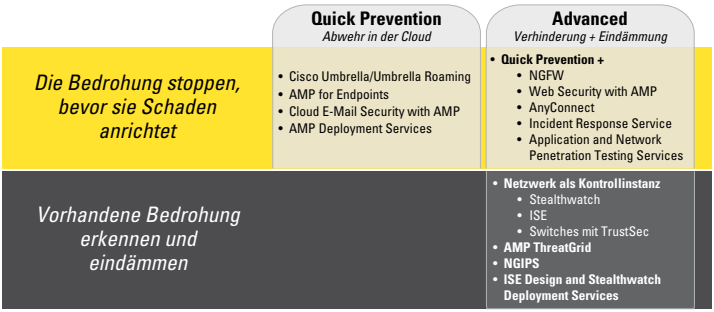


ABBILDUNG 3-3: Cisco Ransomware Defense Lösungspakete sind verfügbar.

NHL UNIVERSITY SCHÜTZT STUDENTEN UND LEHRKÖRPER VOR CYBERBEDROHUNGEN

Die Herausforderung: Studenten, Lehrkörper und Personal vor Ransomware-Angriffen schützen

Die NHL University ist mit mehr als 12.000 Studenten und über 1.200 Mitarbeitern eine der führenden Universitäten in den Niederlanden. Im Februar 2016, zu Beginn der Prüfungsperiode, wurde die Universität Opfer eines Ransomware-Angriffs. Nachdem sie der erste Ransomware-Angriff verwundbar gemacht hatte, wurden weitere Cyberattacken auf ihr Netzwerk gestartet, die ihre wichtigsten Systeme bedrohten. Aufgrund der anhaltenden Angriffe waren die NHL-Administratoren nicht sicher, ob die Prüfungen überhaupt fortgesetzt werden konnten.

Mit der Hilfe von Dimension Data und Cisco konnte die NHL die Krise jedoch bewältigen und ihren Security-Stack verbessern. Sie setzte Cisco Umbrella ein, um alle Geräte und Benutzer auf DNS-Ebene zu schützen – unabhängig davon, wo sie sich auf dem Campus befanden. Später fügte die NHL Advanced Malware Protection (AMP) für die 1.900 unterstützten Geräte innerhalb ihres Netzwerks hinzu, um einen zusätzlichen Schutz vor Malware-Infektionen zu gewährleisten. Mit ihrer neuen Sicherheitsarchitektur konnte die Universität die Prüfungen planmäßig fortsetzen. Doch das war nur der Anfang.

Die Lösung: Eine vollständige Sicherheitslösung und die Unterstützung eines zuverlässigen Beraters

Da Studenten, Dozenten und Mitarbeiter ihre eigenen Geräte auf dem Campus benutzen, musste die NHL genau verstehen, welche Sicherheitsprobleme in ihrem Netzwerk auftreten und was sie dagegen tun kann. Nach der Implementierung ihrer neuen Sicherheitslösungen erkannte die NHL, dass sie die Hilfe von Experten benötigte, um die Time-to-Value zu verkürzen, Mitarbeiter schnell zu schulen, alle Funktionen auf die richtige Weise zu nutzen und die Tools in ihren Systemen zur Verfolgung von Key Performance Indicators (KPIs) zu verbinden. Deshalb wandte sich die NHL an das Cisco Adoption Team. Gemeinsam führten die NHL und Cisco Workshops durch, in denen Möglichkeiten aufgezeigt und Sicherheitsprobleme gelöst wurden.

Nach dem Einsatz von Cisco Umbrella bestand die nächste Aufgabe darin, AMP-Technologie zum Schutz der Endpunkte im NHL-Netzwerk erfolgreich zu implementieren. Seit der Einführung von Cisco Umbrella und AMP hatte die NHL mit keinen weiteren Ransomware-Problemen zu kämpfen. Nach diesem anfänglichen Erfolg unterstützte das Cisco Adoption Team die NHL auch bei der Entwicklung von Dashboards zur Überwachung und Messung der Aktivitäten in ihren Netzwerken und bei der Bereitstellung von Berichten für Führungskräfte zum Nachweis darüber, dass Bedrohungen effektiv bekämpft werden. Das Cisco-Team unterstützte die NHL auch bei der Entwicklung von Prozessen und Arbeitsabläufen, die sie in die Lage versetzten, proaktive Maßnahmen zur Verhinderung zukünftiger Angriffe zu ergreifen.

Die Auswirkungen: Gewinnung von Netzwerktransparenz und -intelligenz und Vorbereitung auf die Zukunft

Die Geschichte geht jedoch noch weiter. Im Jahr 2018 schloss sich die NHL mit der Stenden Hogeschool zu einer neuen Multi-Campus-Universität zusammen: NHL Stenden University. Mit 25.000 Studenten und 2.250 Mitarbeitern an zehn Standorten in der ganzen Welt hat sich die Größe der Universität jetzt verdoppelt – und damit auch das Potenzial neuer Bedrohungen. In Zusammenarbeit mit Cisco überprüfte die NHL ihre Sicherheitsarchitektur im gesamten Universitätssystem und investierte im Vorfeld der Fusion erheblich in Software und Hardware, um ihre Sicherheitsposition vor dem Zusammenschluss zu verbessern.

Angesichts der steigenden Anzahl von Ransomware-Angriffen, die weltweit stattfinden, ist es nur eine Frage der Zeit, bis die großen Universitäten als hochkarätige Ziele anvisiert werden. Die NHL Stenden University ist jetzt bereit, sich der Herausforderung zu stellen.

IN DIESEM KAPITEL

- Abwehr von Ransomware in der Cloud
- Angriffsvektoren für Ransomware an Endpunkten und im E-Mail-Verkehr
- Durchsetzung von Sicherheitsrichtlinien bei Next-Generation Firewalls und Segmentierung
- Cisco Security Advisory Services

Kapitel 4
Cisco Ransomware Defense

Cisco Ransomware Defense bietet einen integrierten Ansatz, der Schutz vor Ransomware für alle Bürostandorte und Benutzer bietet – selbst außerhalb des Virtual Private Network (VPN). Unterstützt durch die unübertroffene Bedrohungsintelligenz von Cisco Talos vereint die einheitliche Architektur von Cisco komplementäre Sicherheitsprodukte wie Domain Name System (DNS), Web-, E-Mail-, Endpunkt- und Netzwerksicherheit. In diesem Kapitel erfahren Sie mehr über Cisco Ransomware Defense und warum Ciscos Lösung den effektivsten Schutz vor Ransomware bietet – vom Netzwerk zu E-Mail und vom Endpunkt zur Cloud.


TIPP

Es mag den Anschein haben, dass diese Liste eine Menge von Tools enthält. Die gute Nachricht ist, dass Sie sich nicht in jedes einzelne davon einloggen bzw. es separat verwalten müssen! Cisco Threat Response automatisiert Integrationen über viele Cisco Sicherheitsprodukte hinweg und aggregiert deren Informationsquellen in einer integrierten Plattform. Dadurch erhalten Sie eine größere Transparenz und einen besseren Kontext, damit Sie Sicherheitsaktivitäten in Ihrer gesamten Umgebung einfach untersuchen und korrigieren können.

Schutz vor Ransomware beginnt mit DNS

Ein Ransomware-Angriff hat viele Phasen. Bevor der Angreifer einen Angriff startet, muss er eine Internet-Infrastruktur aufbauen, um die Ausführungs- und C2-Phasen (Command-and-Control) zu unterstützen. Cisco Umbrella stellt die erste Verteidigungslinie dar und stoppt Ransomware-Angriffe (und andere Cyberattacken) früher in der Angriffskette, da Internetverbindungen zu gefährlichen Websites, die Ransomware verteilen, sofort blockiert werden. Umbrella ist in das Fundament des Internets integriert und setzt Sicherheit auf DNS- und IP-Ebene durch (siehe Abbildung 4-1).

Cisco Umbrella kann auch in Cisco SD-WAN integriert werden, um zusätzliche Verteidigungsebenen gegen Ransomware-Angriffe für direkte Internet-Zugriffe in Satellitenbüros zu bieten. Zu diesen zusätzlichen Kontrollen gehören ein sicheres Web-Gateway, eine Cloud-basierte Firewall und die CASB-Funktionalität (Cloud Access Security Broker), die von einer einzigen nativen Cloud-Plattform aus bereitgestellt werden.

TECHNISCHES

SD-WAN steht für *Software-Defined Wide Area Networking*.

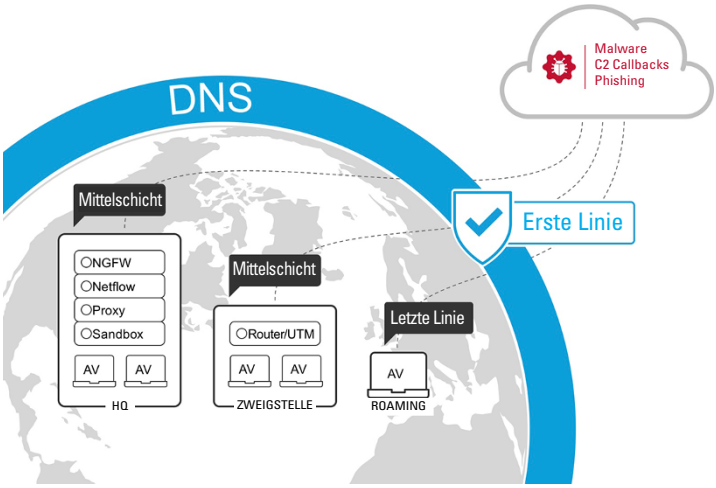


ABBILDUNG 4-1: DNS ist die erste Verteidigungslinie gegen Ransomware-Angriffe.

Im Gegensatz zu Appliances schützt der Cloud-Service Endpunkte sowohl innerhalb als auch außerhalb des Unternehmensnetzwerks. Im Gegensatz zu Agents erstreckt sich der Schutz auf DNS-Ebene auf jedes

mit dem Netzwerk verbundene Gerät – und das mühelos. Dies ist die schnellste und einfachste Art, alle Ihre Benutzer zu schützen, und sie ist in nur 30 Minuten einsatzbereit.

TIPP

Um mehr zu erfahren, laden Sie das E-Book *Umbrella Advantage* unter `https://learn-umbrella.cisco.com/ebooks/the-umbrella-advantage-what-makes-cisco-umbrella-unique` herunter.

CISCO IT IMPLEMENTIERT UMBRELLA ZUR ABWEHR VON RANSOMWARE UND ANDERER BEDROHUNGEN

Als Cisco im April 2016 begann, Umbrella für seine interne IT einzusetzen, hatte das Unternehmen zwei wesentliche Ziele:

- **Einen besseren Schutz gegen Malware, Botnets und Datenschutzverletzungen zu erzielen:** Als ein globales DNS-Anbieternetz sieht Umbrella 2 Prozent der weltweiten Internet-Requests. Es erlangt schnell einen Überblick über neuartige Bedrohungen und blockiert sie, bevor sie die Möglichkeit haben, Schaden anzurichten.
- **Einblicke in riskantes Benutzerverhalten zu erlangen:** Umbrella erstellt Logs, die alle Aktivitäten im Internet – unabhängig von Port und Protokoll – aufzeichnen. Die Logs bieten den Security- und IT-Teams von Cisco mehr Transparenz und Prüfungsmöglichkeiten.

Der Übergang zu Umbrella war außergewöhnlich einfach. „Wir haben leistungsstarke neue Kontrollen hinzugefügt, ohne neue Hardware einsetzen, das Netzwerk neu konfigurieren, umfassende Interoperabilitätstests durchführen oder unsere anderen Systeme ändern zu müssen", sagt Rich West, Information Security (InfoSec) Architect bei Cisco.

Cisco bildete ein aus acht Mitgliedern der IT- und InfoSec-Abteilungen bestehendes Team zur Planung und Implementierung von Umbrella. Die technischen Aspekte des Übergangs nahmen sehr wenig Zeit in Anspruch. Die Teammitglieder verbrachten die meiste Zeit in Meetings mit Anwendungsverantwortlichen und Netzwerkbetriebsteams, um die Vorteile des Übergangs zu erläutern und etwaige Fragen zu den Auswirkungen auf die Anwendungs- oder Netzwerkleistung zu beantworten.

Die Umstellung war einfach und erforderte lediglich das Hinzufügen von vier Codezeilen zur DNS-Konfigurationsdatei auf Ciscos internen DNS-Servern, um Anfragen an Umbrella weiterzuleiten. Die DNS-Server der Cisco IT richten jetzt rekursive DNS-Anfragen an Umbrella, anstatt ihre

(Fortsetzung)

(Fortsetzung)

vorgeschalteten Nachbarn zu fragen. Die Umstellung war so nahtlos, dass die Benutzer nicht einmal merkten, dass eine Veränderung stattgefunden hatte.

Cisco Umbrella vereinigt mehrere Sicherheitsservices auf einer einzigen Cloud-Plattform, um den Internetzugang zu sichern und die Nutzung von Cloud-Apps in Ihrem Netzwerk, in Ihren Zweigstellen und bei Roaming-Benutzern zu kontrollieren. Bevor Benutzer eine Verbindung zu einem beliebigen Online-Ziel herstellen, fungiert Umbrella als sicherer Zugang zum Internet und bietet eine umfassende Überprüfung und Kontrolle, um die Einhaltung von Vorschriften zu unterstützen und Bedrohungen zu blockieren. Umbrella bietet außerdem einen interaktiven Zugang zu Bedrohungsinformationen, um die Reaktion auf Vorfälle und die Erforschung von Bedrohungen zu unterstützen.

WIE EIN GLOBALES FERTIGUNGSUNTERNEHMEN RANSOMWARE BEKÄMPFT

Die Herausforderung: Begrenzte Ressourcen stehen schier grenzenlosen Herausforderungen gegenüber

In den Jahrzehnten seit seiner Gründung im Jahr 1983 ist Octapharma ständig gewachsen und gehört heute zu den größten Herstellern von Humanproteinen. Seit Octapharma jüngst eine Initiative angestoßen hat, die eine Verdopplung der Produktionskapazität und eine Steigerung der Effizienz insgesamt vorsieht, expandiert das Unternehmen wie nie zuvor.

Dieser Wachstumsschubs macht sich im gesamten Unternehmen bemerkbar – sogar auf Ebene des Netzwerks. „An vielen Standorten stellen wir neues Personal ein. Damit steigt natürlich auch die Zahl der Mobilgeräte und Cloud-Services, die in unserem Unternehmen genutzt werden, was in der Folge auch neue Schwachstellen in unserem Netzwerk bedeutet", so Jason Hancock, Leiter Netzwerktechnik bei Octapharma „In unserem Netzwerk sind die schädlichen Aktivitäten sprunghaft angestiegen, einschließlich Ransomware."

„Dieser Entwicklung durch Aufstockungen unserer Teams entgegenzuwirken, wäre angesichts des anhaltenden Mangels an Security-Fachkräften schwierig gewesen – und auch kaum mit den Effizienzzielen unseres Unternehmens vereinbar. Daher mussten wir uns nach neuen Lösungen umsehen", fügt er hinzu.

„Mit Blick auf die Effizienz – sowohl unseres Teams als auch der Endnutzer –, mussten wir als erstes dafür sorgen, dass das Netzwerk nicht mehr alle 15 Minuten ausfällt. Als ich 2014 in die Firma kam, ging es in erster Linie darum, die Systeme stabiler zu machen und dann schrittweise unseren Malware-Schutz zu verbessern. Hierbei konzentrierte ich mich zunächst auf besonders aggressive Varianten, darunter auch die CryptoLocker-Ransomware, mit der es bei uns in der Vergangenheit bereits zu einem Sicherheitsvorfall kam."

Die Lösung: Funktionalität, die einfach passt

„Als ich bei Octapharma anfing, war bereits seit einiger Zeit ein Projekt im Gange, in dessen Rahmen die bei uns eingesetzten Web-Security-Appliances zum Cloud-Service desselben Anbieters migriert werden sollten, den einer meiner Vorgänger ausgewählt hatte. Dieses Projekt sollte ich dann zum Abschluss bringen", erinnert sich Hancock. „Als ich aber sah, womit ich es zu tun hatte, war mir sofort klar, dass wir mit diesem Produkt nicht weit kommen würden."

„Wir stießen auf erhebliche Probleme, die zunehmend Zweifel an der Eignung des Produkts für unsere Umgebung aufkommen ließen. Das fing schon bei der Internetfunktionalität an." Hancock berichtet weiter: „Wir erhielten reichlich Beschwerden über Probleme mit dem Internetservice, sowohl im Zusammenhang mit dem Cloud-Service, als auch mit dem Client, der auf den Endnutzersystemen installiert war."

„Darüber hinaus war der Funktionsumfang für uns nicht ausreichend, und auch die Administration gestaltete sich schwierig – wir mussten unsere Teams umfangreich schulen, bevor sie mit der komplexen, nicht intuitiven Verwaltung von Richtlinien und diversen Komponenten zurechtkamen."

„Als wir die Lösung nach einer äußerst holprigen Installationsphase dann endlich an unseren Standorten in Nordamerika ausgerollt hatten, fiel unser Netzwerk regelmäßig aus – teilweise für mehrere Stunden." Diese Probleme ließen unser Team natürlich denkbar schlecht aussehen, konnten aber auch nicht über den Support des Herstellers behoben werden." „Vonseiten des Herstellers riet man uns dann schließlich, die Migration in die Cloud abzubrechen und stattdessen virtuelle Appliances einzuführen. Doch dazu hätten wir den Traffic von weltweit mehr als 50 Standorten umleiten müssen, was nicht nur unerwünscht, sondern in einigen Fällen auch unmöglich war."

„An diesem Punkt schritt ich ein. Ich machte deutlich, dass wir das Problem nur mit Cisco Umbrella lösen würden, und dass ich diese Lösung binnen sechs Wochen ausrollen und damit unser gesamtes globales

(Fortsetzung)

(Fortsetzung)

Netzwerk schützen könnte." In die bestehende Lösung war bereits viel Geld geflossen, aber sie funktionierte eben nicht bei uns. Deshalb schlug ich eine Lösung vor, von der ich aus früherer Erfahrung wusste, dass sie Erfolg haben würde: Umbrella."

Die Ergebnisse: Deutlicher Rückgang der Ransomware-Vorfälle

Der Rollout der Lösung gestaltete sich äußerst einfach – und zeigte sofort Ergebnisse. „Seit der Einführung von Umbrella haben wir keine Probleme mit der Web-Sicherheit mehr", so Hancock.

„Wir sind jetzt deutlich weniger anfällig für Ransomware-Angriffe. Tatsächlich gab es seither keinen einzigen Fall mehr, bei dem sich ein Nutzer durch Klicken auf einen schädlichen Link eine Ransomware eingefangen hätte. Tatsächlich werden bei uns jetzt jede Woche mehrere Zehntausend solcher Web-Anfragen mithilfe unserer Sicherheitsrichtlinie blockiert. Und das schließt noch nicht einmal die Blockierungen auf Grundlage unserer Kategorie-Richtlinien mit ein", fügt er hinzu. „Das Risiko, uns über das Web mit Ransomware zu infizieren, ist erheblich gesunken. Und das bei deutlich stabileren Internetverbindungen für unsere Endnutzer."

„Wir haben uns sogar einige Phishing-E-Mails herausgesucht und auf die darin enthaltenen Links geklickt, um zu sehen was passiert: Der Zugriff auf diese Websites wurde von Umbrella zuverlässig blockiert."

Hancock berichtet zudem von einem weiteren Vorteil, mit dem er nicht gerechnet hatte: „Als wir die Daten aus dem Umbrella-Dashboard mit den Daten von unseren internen Systemen abglichen, fanden wir weitere infizierte Systeme, die zuvor durchs Raster gefallen waren."

Nachdem Bedrohungen bei Octapharma jetzt auf DNS-Ebene blockiert werden, will Hancock den Schutz des Netzwerks durch ein proaktives Sicherheitsmanagement zusätzlich stärken. „Umbrella kann Websites auf Grundlage von Kategorie-Richtlinien äußerst effektiv blockieren. Damit bildet die Lösung ein zentrales Element unserer Verteidigungsstrategie. Ich prüfe derzeit weitere Tools aus dem Cisco Security-Portfolio, um diese Strategie weiter voranzutreiben", merkt Hancock an. „Dafür in Frage kommen z. B. Firewalls, Malwareschutz für Endpunkte und Möglichkeiten bei Cisco, die Produkte in unserem Security-Stack besser zu koordinieren."

Für Jason Hancock war schon immer klar: Die Überzeugung für eine Sache kommt, wenn man ihre Vorteile sofort sehen kann. „Zu Hause nutze ich Umbrella schon seit Jahren", sagt er. „Und jetzt habe ich die Lösung bereits in zwei Unternehmen mit sehr großem Erfolg eingeführt. Meine Kollegen sind genauso begeistert von dem hochgradig effektiven Sicherheitsansatz von Cisco wie ich selbst."

Sicherung von Endpunkten und Umgang mit E-Mail-Bedrohungen

Malware-Bedrohungen sind heute raffinierter als jemals zuvor. Fortschrittliche Malware, einschließlich Ransomware, entwickelt sich unaufhaltsam weiter und kann unerkannt bleiben, nachdem sie ein System kompromittiert hat. Dazu werden u. a. die folgenden Methoden eingesetzt:

- Schlafmethoden
- Polymorphismus und Metamorphismus
- Verschlüsselung und Verschleierung
- Verwendung unbekannter Protokolle

Gleichzeitig bietet fortschrittliche Malware eine Startrampe für hartnäckige Angreifer, um sich lateral durch das kompromittierte Netzwerk eines Unternehmens zu bewegen.

E-Mail-Pishingkampagnen sind ein besonders beliebter – und erstaunlich effektiver – Malware-Angriffsvektor für Cyberkriminelle. Viele Ransomware-Varianten verwenden Phishing-Methoden zum Infizieren ihrer Opfer.

Cisco Ransomware Defense Lösungen wie Cisco Advanced Malware Protection (AMP) for Endpoints und Cisco Cloud E-Mail Security with AMP sichern Endpunkte ab und verhindern E-Mail-Bedrohungen.

Cisco Advanced Malware Protection for Endpoints

Traditionelle Anti-Malware-Software, die ausschließlich Point-in-Time-Erkennungsmethoden verwendet, wird niemals zu 100 Prozent effektiv sein. Eine einzige Bedrohungen, die nicht erkannt wird, reicht jedoch schon aus, um Ihre gesamte Umgebung zu kompromittieren. Durch die Verwendung gezielter kontextbewusster Malware in Verbindung mit entsprechenden Ressourcen, Expertise und Ausdauer können raffinierte Angreifer Point-in-Time-Verteidigungsmaßnahmen überlisten. Point-in-Time-Erkennung ist auch blind in Bezug auf den Umfang und die Tiefe einer Sicherheitsverletzung, die bereits eingetreten ist. In vielen Fällen können die betroffenen Organisationen dann die Ausbreitung von Outbreaks oder ähnliche Angriffe nicht verhindern.

TIPP

Zwar ist keine Anti-Malware-Lösung in der Lage, Ransomware zu beseitigen oder Dateien zu entschlüsseln, nachdem ein Endpunkt infiziert worden ist, Cisco kann Unternehmen jedoch dabei helfen,

Ransomware proaktiv zu erkennen und zu blockieren, bevor sie das Netzwerk erreichen kann.

Auf der Grundlage dieses Verständnisses von Malware hat Cisco AMP for Endpoints entwickelt. Mit dieser Lösung stellt Cisco ein komplettes System von Erkennungsressourcen und Big-Data-Analysefunktionen bereit, um Dateien und Traffic kontinuierlich zu analysieren und fortgeschrittene Malware-Bedrohungen zu identifizieren und abzuwehren. Hochentwickelte Machine-Learning-Verfahren bewerten über 400 mit jeder Datei verbundene Eigenschaften. Erweiterte Suchfunktionen sorgen dafür, dass Sie alles über den Endpunkt wissen, wodurch Sicherheitsuntersuchungen dramatisch beschleunigt werden. *Retrospective Security* – die Fähigkeit, eine Zeitreise in die Vergangenheit zu unternehmen und Prozesse, Dateiaktivitäten und Nachrichtenverkehr zurückzuverfolgen, um das volle Ausmaß einer Infektion zu verstehen, ihre Ursachen aufzuspüren und den Schaden zu beheben – kann Dateien erkennen und melden, die noch gefährlich geworden sind. Diese Kombination aus kontinuierlichen Analysen und Retrospective Security bietet einen fortgeschrittenen Malware-Schutz, der über die traditionelle Point-in-Time-Erkennung hinausgeht (siehe Abbildung 4-2).

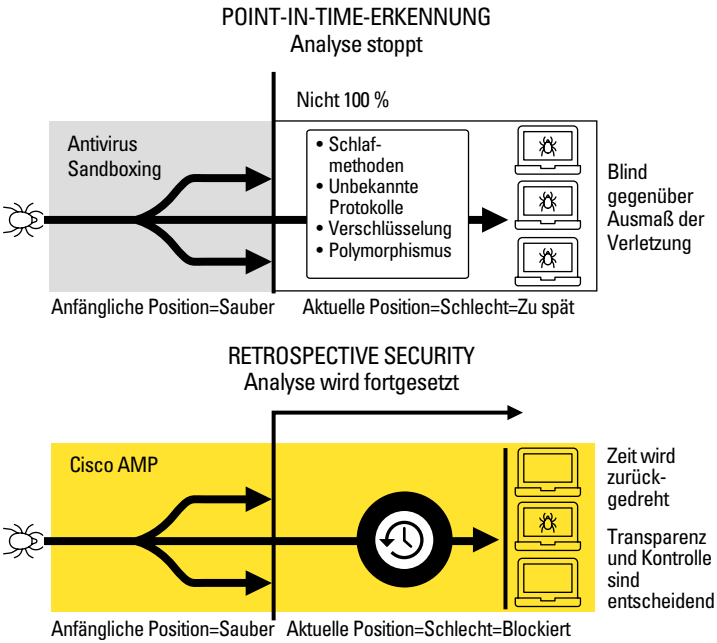


ABBILDUNG 4-2: Point-in-Time-Erkennung im Vergleich zu kontinuierlichen Analysen und Retrospective Security.

Cisco Advanced Malware Protection for E-Mail Security

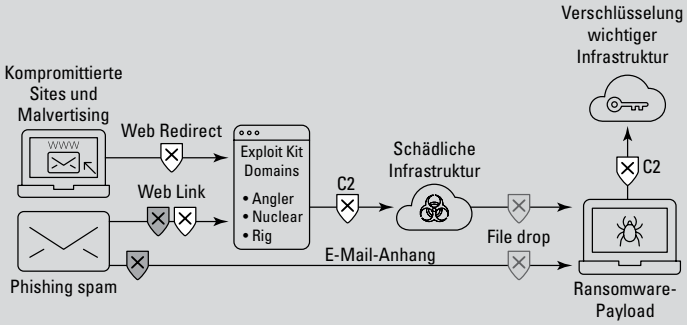
E-Mail ist ein wichtiges Kommunikationsmittel, durch das Unternehmen jedoch zahlreichen komplexen Bedrohungen ausgesetzt werden. Cisco E-Mail Security with Advanced Malware Protection (AMP) blockiert Spam und Phishing-E-Mails sowie bösartige Anhänge und URLs, die oft ein wichtiger Angriffsvektor für Ransomware sind. Die AMP-Technologie für den E-Mail-Gateway ist dieselbe, die am Endpunkt eingesetzt wird.

Cisco E-Mail Security with AMP schützt den geschäftskritischen E-Mail-Verkehr mit mehrschichtigen Schutzmaßnahmen, darunter

- Global Threat Intelligence
- Spam-Schutz
- Graymail-Erkennung und Abmeldung
- Fortschrittlicher Malware-Schutz
- Outbreak-Filter

CISCO NUTZT SEINE EIGENEN PRODUKTE

Cisco IT stützt sich bei seiner bedrohungsorientierten E-Mail-Sicherheitsstrategie auf Cisco E-Mail Security with AMP. Die folgende Darstellung zeigt, wie Cisco Umbrella, Cisco AMP for Endpoints und Cisco E-Mail Security with AMP zusammenarbeiten, um Ransomware-Angriffe auf unterschiedliche Weise abzuwehren.



- Web-Interaktionstracking
- Kontrolle ausgehender Nachrichten
- Erkennung gefälschter E-Mails
- Data Loss Prevention (DLP)

Schutz des Netzwerks mit Next-Generation Firewalls und Segmentierung

Cisco Firepower, die bedrohungsorientierten Next-Generation Firewalls (NGFWs) von Cisco, bieten einen integrierten Schutz vor Bedrohungen für das gesamte Angriffskontinuum – vor, während und nach einem Angriff – und eine einmalige Transparenz, die mit veralteten portbasierten Firewalls nicht möglich wäre. Cisco TrustSec-Technologie bietet eine dynamische softwaredefinierte Netzwerksegmentierung. Sie verwendet das vorhandene Netzwerk, um granulare rollenbasierte Sicherheitsrichtlinien auf einzelnen Netzwerksegmenten durchzusetzen – unabhängig vom Standort oder Gerät des Benutzers. Das Ergebnis ist eine einfachere Segmentierung, die die laterale Ausbreitung im Netzwerk einer Organisation verhindert. Dadurch kann der durch Malware verursachte Schaden eingedämmt werden, wenn eine Sicherheitsverletzung stattgefunden hat.

Cisco Firepower Next-Generation Firewalls

Cisco Firepower Next-Generation Firewall (NGFW) mit Advanced Malware Protection (AMP) und Threat Grid Sandbox-Technologie blockiert bekannte Bedrohungen und Command-and-Control-Callbacks (C2) und stellt gleichzeitig dynamische Analysen für unbekannte Malware und Bedrohungen zur Verfügung. Cisco Firepower bietet:

- **Genaue Anwendungstransparenz und -kontrolle (Application Visibility and Control – AVC):** Identifizieren und Kontrollieren des Benutzerzugriffs bei über 4.000 kommerziellen Anwendungen und Unterstützung für kundenspezifische Anwendungen.
- **Cisco Next-Generation IPS:** Äußerst effektiver Schutz vor Bedrohungen und vollkommene Kontextsensitivität in Bezug auf Benutzer, Infrastruktur, Anwendungen und Inhalte zur Erkennung von Angriffen auf mehreren Angriffsvektoren und zur Automatisierung von Verteidigungsmaßnahmen.

- **Reputations- und kategoriebasierte URL-Filterung:** Diese Filterung bietet eine umfassende Alarmierung und Kontrolle von verdächtigem Webverkehr. Sie setzt Richtlinien auf Millionen von URLs in mehr als 80 Kategorien durch.
- **Fortgeschrittener Malware-Schutz:** Effektive Erkennung von Sicherheitsverletzungen und geringe Gesamtbetriebskosten (Total Cost of Ownership – TCO) sorgen für einen hohen Schutzwert. Erkennung, Verständnis und Abwehr von Malware und neuen Bedrohungen, die von anderen Sicherheitsebenen nicht erkannt wurden – durch eine einfache Software-Lizenz aktiviert.

Das Netzwerk als Sensor und Kontrollinstanz

Cisco verwendet das Netzwerk, um Sicherheitsrichtlinien durch softwaredefinierte Segmentierung dynamisch durchzusetzen, Angriffsflächen zu reduzieren, Angriffe durch die Eindämmung der lateralen Ausbreitung von Bedrohungen im Netzwerk zu verhindern und die Zeit zu verkürzen, die zum Abblocken von Bedrohungen benötigt wird, nachdem sie erkannt wurden.

Mit den Lösungen von Cisco ist das Netzwerk selbst in der Lage, als Sensor und Kontrollinstanz zu agieren. Die Identity Services Engine (ISE) von Cisco mit TrustSec und Stealthwatch vereinfacht die Bereitstellung und Verwaltung eines sicheren Netzwerkzugriffs, bietet eine größere Transparenz in Bezug auf ungewöhnliche Netzwerkaktivitäten, beschleunigt die Sicherheitsprozesse und setzt Richtlinien überall im Netzwerk konsistent durch. Im Gegensatz zu Zugriffskontrollmechanismen, die auf der Netzwerktopologie basieren, werden die Cisco TrustSec-Kontrollen mittels logischer Richtliniengruppierungen definiert, damit die Ressourcensegmentierung und der sichere Zugriff ständig aufrechterhalten werden, selbst wenn sich Ressourcen in mobilen und virtualisierten Netzwerken bewegen. Was bedeutet das alles? Die Richtliniendurchsetzung mit TrustSec kann die Ausbreitung eines Ransomware-Angriffs durch das gesamte Netzwerk verhindern.

MERKEN

Die Cisco TrustSec-Funktionalität ist in die Switching-, Routing-, WLAN- und Firewall-Produkte von Cisco integriert, um Inventar und Anwendungen in den Rechenzentrumsnetzen von Unternehmen zu schützen.

Herkömmliche Zugriffskontrollmethoden segmentieren und schützen das Inventar unter Verwendung von Virtual LANs (VLANs) und Access Control Lists (ACLs). Cisco TrustSec verwendet dagegen Sicherheitsgruppenrichtlinien, die in einer Klartext-Matrix geschrieben und von IP-Adressen und VLANs abgekoppelt sind. Benutzer und Assets mit derselben Rollenklassifikation werden einer Sicherheitsgruppe zugeordnet.

Cisco TrustSec-Richtlinien werden zentral erstellt und automatisch an kabelgebundene, drahtlose und VPN-Netzwerke verteilt, damit Benutzer und Ressourcen einen gleichbleibenden Zugriff und Schutz erhalten, wenn sie sich in virtuellen und mobilen Netzwerken bewegen. Softwaredefinierte Segmentierung hilft dabei, die Zeit zu reduzieren, die mit netzwerktechnischen Aufgaben und mit Compliance-Validierung verbracht wird.

Optimierte Bereitstellung und effektive Reaktion auf potenzielle Bedrohungen

Die Cisco Security Advisory Services umfassen Bereitstellungsservices für die Cisco Ransomware-Defense-Lösungen, darunter Firepower und AMP sowie Incident Response.

Das Security Services Incident Response Team von Cisco kann Folgendes zur Verfügung stellen:

- Proaktive Incident-Response-Services, die Ihrer Organisation dabei helfen, ihre Reaktionsfähigkeit auf Sicherheitsvorfälle zu bewerten und/oder zu verbessern.
- Reaktive Reaktion im Falle eines Ransomware-Angriffs oder eines anderen Sicherheitsvorfalls.

Darüber hinaus befassen sich die Security Integration Services von Cisco mit architekturbezogenen Herausforderungen auf Lösungsebene, wobei die Bereitstellung von Technologien wie Advanced Malware Protection (AMP) for Endpoints und Cisco Firepower Next-Generation Firewalls (NGFWs) optimiert wird.

MERKEN

Diese Komponenten bilden die Grundlage des „Cisco Ransomware Defense"-Ansatzes. Es gibt jedoch noch eine Reihe weiterer Lösungen von Cisco, mit denen Sie Ihre Sicherheitsposition in allen Bereichen Ihres Unternehmens verbessern können. Entdecken Sie das gesamte Cisco Sicherheitsportfolio unter `www.cisco.com/c/en/us/products/security`.

ZUVERLÄSSIGE PERFORMANCE MIT CISCO

Die Herausforderung: Entwicklung des Defense-in-Depth-Schutzes

Prologis, Inc., ein weltweit führender Anbieter von Immobilien und Logistikflächen, vermietet moderne Distributionseinrichtungen an einen vielfältigen Stamm von circa 5.200 Kunden in zwei wesentlichen Kategorien: Business-to-Business und Einzelhandel/Online-Fulfillment. Das Unternehmen hat über 60 Niederlassungen in 20 Ländern auf vier Kontinenten.

„Als globales Unternehmen sind wir an vielen Orten der Welt tätig. Dabei stützen wir uns stark auf Cloud Computing", sagt Tyler Warren, Security Solutions Architect bei Prologis. „Da sich der Großteil der IT-Infrastruktur von Prologis in der Cloud befindet, haben wir weder typische Infrastruktur noch Perimeter, wodurch es schwierig ist, geeignete Sicherheitslösungen zu finden."

Als ein börsennotiertes, cloudzentriertes globales Unternehmen muss Prologis seine Systeme schützen und dafür sorgen, dass sie nicht kompromittiert werden. Tyler Warrens Ziel ist es daher, den Security-Stack des Unternehmens auszubauen, damit dies nicht passieren kann.

„Die Anzahl der Bedrohungen nimmt ständig zu und es wurde schnell klar, dass Prologis seine vorhandenen Sicherheitsmaßnahmen verstärken musste, um sein Netzwerk und seine Benutzer innerhalb und außerhalb des Netzwerks vor bösartigen Aktivitäten wie Command-and-Control-Callbacks, Malware und Phishing zu schützen", sagt er. „Ein mehrschichtiges Sicherheitsmodell erschien uns sinnvoll, da kein Sicherheitselement allein stark genug ist, um alles abzufangen."

Die Lösung: Verstärkte Sicherheit, die perfekt auf das Personal und die vorhandenen Ressourcen zugeschnitten ist

„Der Ausbau unseres Security-Stacks war mit einigen Versuchen und Irrtümern verbunden. Alle Elemente sollten miteinander kompatibel und nahtlos integrierbar sein – ohne negative Auswirkungen auf die Benutzer. Vor allem mussten unsere Sicherheitslösungen in der Lage sein, uns dort zu schützen, wo wir arbeiten: überall auf der Welt und in der Cloud", sagt Warren.

Die kurze Blockliste von Prologis mit sehr spezifischen als offensiv eingestuften Inhaltstypen erforderte eine Webfilterung, für die anfangs ein anderer Anbieter verantwortlich war. Warren sagt: „Wir fanden es schwierig, diese erste Lösung zu verwalten. Vor allem aber stand sie nicht im Einklang mit unserem Unternehmensziel, alles in die Cloud zu verschieben."

„Wir brauchten eine Sicherheitsebene, mit der wir bestimmte mit der Internetnutzung von Mitarbeitern verbundene Sicherheitsprobleme

(Fortsetzung)

(Fortsetzung)

beheben konnten, und wir mussten unsere Webfilterung verbessern", sagt er. „Wir begrüßten es, dass Umbrella als erste Verteidigungslinie bösartige Aktivitäten abwehrt."

Auf der Suche nach der besten Lösung für diese Anforderungen führte Prologis Machbarkeitsprüfungen mit Cisco und drei anderen Anbietern durch. Nachdem die anderen Anbieter aufgrund verschiedener Faktoren, u. a. Hardware-Anforderungen, Komplexität, zeitintensive Implementierung und Preis eliminiert worden waren, entschied sich Prologis für Cisco Umbrella.

„Umbrella erfüllt alle unsere Anforderungen", sagt Warren. „Es deckt unsere spezifischen Sicherheitsbelange ab, übernimmt die Webfilterung und unterstützt unsere Remote-Nutzer – alles in einer einzigen cloudbasierten, leicht implementierbaren Lösung."

Die Ergebnisse: Durchsetzung von Richtlinien mit dramatischer Leistungssteigerung

„Wir mussten nicht lange warten, bis wir Resultate sahen", sagt Warren. „Die Fähigkeit, Richtlinien überall konsistent durchzusetzen – auch für Geräte außerhalb des Netzwerks – ist für Prologis extrem wichtig. Die Implementierung des Umbrella Roaming Client verlief so nahtlos, dass niemand durch die Umstellung beeinträchtigt wurde."

Ein weiteres positives Ergebnis ist die erhebliche Leistungssteigerung. „Nachdem wir Umbrella installiert hatten, erlebten wir eine enorme Leistungsverbesserung. Da sich die meisten von Prologis verwendeten Anwendungen in der Cloud befinden, ist Performance extrem wichtig für uns. Bei hundert Prozent der Anwendungen, die wir benutzen, haben wir erhebliche Leistungssteigerungen erlebt."

Die anderen Funktionen von Umbrella haben sich ebenfalls als nützlich erwiesen. „Automatisiertes Reporting ist wertvoll – besonders der Cloud Services Report – da ich eindeutige, verwertbare Daten darüber vorlegen kann, wie gut das Netzwerk geschützt ist und wie viel Schatten-IT in der Cloud stattfindet. Das hat mir wirklich die Augen geöffnet." „Durch das Reporting kann ich Probleme schneller ermitteln. Die Lösung hat vielen Menschen das Leben erleichtert, da sie uns gezeigt hat, wie unerlässlich unsere Defense-in-Depth-Sicherheitsinfrastruktur für unser Unternehmen ist."

„Es war eine hervorragende Entscheidung, Umbrella in unseren Security-Stack aufzunehmen. Alle sind begeistert von der verbesserten Sicherheit und Leistung, die wir nach der Implementierung der Lösung erzielt haben."

IN DIESEM KAPITEL

- Herausforderungen bei der Abwehr von Ransomware
- Entwicklung und Implementierung einer inhärent sicheren Umgebung
- Einfachheit ist der Schlüssel
- Automatisierung von Aufgaben, um neuen Bedrohungen einen Schritt voraus zu sein

Kapitel 5
Abwehr von Ransomware: Zehn wichtige Punkte, die Sie im Gedächtnis behalten sollten

In diesem Kapitel gehe ich auf einige wichtige Punkte bei der Abwehr von Ransomware ein, die Sie im Gedächtnis behalten sollten!

Ransomware entwickelt sich ständig weiter

Ransomware ist eine Bedrohung, die sich schnell weiterentwickelt. Ransomware ist eine Bedrohung, die sich schnell weiterentwickelt. Laut einer vor kurzem veröffentlichten Studie von Cybersecurity Ventures wird im Jahr 2021 alle 11 Sekunden eine neue Organisation zum Opfer eines Ransomware-Angriffs werden – und es kommen ständig neue Varianten! Eine effektive Abwehr von Ransomware ist heute wichtiger als je zuvor, um die Daten Ihres Unternehmens vor Angriffen zu schützen.

Die wirtschaftlichen Auswirkungen von Ransomware-Angriffen werden immer schwerwiegender und Angriffsmuster gehen verstärkt in Richtung „Qualität vor Quantität“. Dies wird häufig mit Ransomware-Varianten wie Ryuk und gezielteren Angriffen auf mittlere bis große Organisationen mit mehr Finanzkraft erreicht.

Zum schnellen Wachstum und zur Weiterentwicklung von Ransomware haben unterschiedliche Faktoren beigetragen, darunter Initiativen zur digitalen Transformation (durch die die Anzahl potenzieller Einstiegspunkte und die Fähigkeit zur Ausdehnung von Angriffen erheblich erhöht wird), der Aufstieg von Bitcoin (was eine einfache, kaum rückverfolgbare Zahlung von Lösegeldern an Cyberkriminelle ermöglicht) und das Aufkommen von Ransomware-as-a-Service (RaaS – siehe folgender Abschnitt), mit der es für fast jeden leicht ist, Ransomware zu verwenden.

Ransomware-as-a-Service ist eine neue Bedrohung

RaaS ist zu einer neuen Bedrohung geworden, die es für praktisch jede Person mit begrenzten technischen Fähigkeiten kinderleicht macht, ein Cyberkrimineller zu werden. Tox – eines der ersten RaaS-Angebote, das im Mai 2015 entdeckt wurde – kann mittels eines Tor-Browsers aus dem Dark Web heruntergeladen und dann wie folgt verwendet werden:

1. Einen Lösegeldbetrag eingeben.
2. Eine Lösegeldbotschaft erstellen.
3. Ein CAPTCHA eingeben, damit die Entwickler von Tox wissen, dass Sie kein Bot sind.

RaaS-Software kann gewöhnlich kostenlos oder für eine geringe Gebühr heruntergeladen werden. Der tatsächliche Gewinn für die Entwickler der RaaS-Software ist ein Anteil an den eingenommenen Lösegeldern – gewöhnlich zwischen 5 und 30 Prozent.

Lösegeldzahlungen lösen keine Sicherheitsprobleme

Die meisten Opfer von Ransomware-Angriffen glauben, es sei am einfachsten und schnellsten, einfach das Lösegeld zu zahlen, um das Problem aus der Welt zu schaffen. Durch das Zahlen des Lösegeldes erhalten Sie zwar gewöhnlich wieder Zugang zu Ihren Dateien, doch Ihre Probleme sind damit noch lange nicht gelöst.

In den meisten Fällen werden Ihre Dateien zwar entschlüsselt, wenn Sie das Lösegeld zahlen, doch dafür gibt es keine Garantie. Es ist zwar im besten Interesse der Cyberkriminellen, Ihre Dateien wiederherzustellen,

wenn Sie das Lösegeld zahlen (denn wenn bekannt wird, dass Dateien bei einer Ransomware-Kampagne nach der Zahlung nicht wieder entschlüsselt werden, haben zukünftige Opfer keinen Anlass, das Lösegeld zu zahlen), doch unter Dieben gibt es keine Ehre. Dies gilt besonders für RaaS, denn „Neulinge" schauen oft nicht über den Tellerrand hinaus – und wenn der Entschlüsselungscode aus irgendeinem Grund nicht funktioniert, kann man nicht einfach den Kundendienst anrufen!

Es gibt auch keine Garantie, dass der Täter keine andere Malware oder Exploit-Kits installiert, um zukünftige Cyberangriffe auf Ihre Organisation vorzubereiten. Eine Kopie Ihrer Dateien kann zu anderen Zwecken ausgeschleust worden sein, z. B. um die sensiblen Daten Ihrer Organisation im Dark Web zu verkaufen.

Durch die Zahlung von Lösegeldern wird Cyberkriminalität direkt finanziert und unterstützt. Es ist genau dasselbe, wie Lösegeld an Terroristen oder Schurkenstaaten zu zahlen, um Geiseln freizukaufen. Die Täter werden finanziert, ermutigt und darin bestärkt, diese verbrecherischen Handlungen auch in Zukunft fortzusetzen.

Die Zahlung eines Lösegelds ändert auch nichts an der Tatsache, dass eine ernsthafte Sicherheitsverletzung in Ihrer Organisation aufgetreten ist. Je nach der Art, dem Ausmaß und den Umständen der Sicherheitsverletzung sowie je nach Branchenvorschriften und Gerichtsbarkeit, denen Ihre Organisation unterliegt, kann von Ihnen verlangt werden, die Sicherheitsverletzung öffentlich bekannt zu machen und hohe Bußgelder und Strafen zu zahlen – nach der Zahlung eines Lösegeldes ein Schlag ins Gesicht!

TIPP

Um den Schaden nach einem Ransomware-Angriff zu begrenzen, sollten Unternehmen immer dafür sorgen, dass regelmäßig als nachweislich unbeschädigte Sicherungskopien von allen wichtigen Dateien und aktuelle Abbilder von allen kritischen Systemen angefertigt werden.

Eine mehrschichtige Sicherheitsarchitektur sollte auf offenen Standards basieren

Offene und erweiterbare Standards ermöglichen eine neue „Best-of-Breed"-Architektur, mit der neue und vorhandene Technologien leicht in eine umfassende Sicherheitslösung integriert werden können.

Einsatz integrierter Best-of-Breed-Lösungen

Defense-in-Depth ist eine Strategie, die in der Sicherheitsbranche seit langem eingesetzt wird. Leider erforderte Defense-in-Depth bis jetzt die Implementierung von eigenständigen (oder punktuellen) Sicherheitsprodukten, die sich nicht leicht in andere Sicherheitslösungen der Umgebung integrieren ließen.

Mit der neuen Best-of-Breed-Architektur können Unternehmen integrierte portfoliobasierte Lösungen einsetzen, die die Komplexität ihrer Sicherheitsumgebung reduzieren und ihre allgemeine Sicherheitsposition verbessern.

Sicherheit in der gesamten Netzwerkumgebung

Sicherheit muss in der gesamten Computing-Umgebung eines Unternehmens inhärent vorhanden und allgegenwärtig sein – im Netzwerk, über das Rechenzentrum hinweg, an Endpunkten, bei Mobilgeräten und in der Cloud.

Geringere Komplexität in der Sicherheitsumgebung

Sicherheitstechnologien sollten einfach einzusetzen und zu verwenden sein. Durch eine zu große Komplexität erhöht sich die Anzahl potenzieller Risiken auf Grund von Fehlkonfigurationen und Fehlern. Außerdem können wichtige Indicators of Compromise (IoC) und andere Daten in umständlichen und weitschweifigen Protokollen untergehen. Scheuen Sie nicht davor zurück, Sicherheitsdienste von Drittanbietern in Anspruch zu nehmen und sich deren umfassende Erfahrungen zunutze zu machen. Sie können Ihnen dabei helfen, Ihr bereits vorhandenes Wissen zu ergänzen und die Umgebung und Sicherheitsposition Ihres Unternehmens besser zu verstehen, um einen integrierten Sicherheitsplan aufzustellen und unnötige Komplexität zu vermeiden.

Einsatz von cloudbasierter Threat-Intelligence in Echtzeit

Ransomware und andere Bedrohungen der Cybersicherheit entwickeln sich in einem rasanten Tempo. Zero-Day-Angriffe stellen für die meisten Unternehmen die größte Bedrohung dar. Mithilfe cloudbasierter Threat-Intelligence in Echtzeit können IT-Teams, sobald neue Bedrohungen auftauchen, so schnell wie möglich angemessene Gegenmaßnahmen ergreifen und sich Sicherheits-Know-how zunutze machen, das weit über das Unternehmen hinausreicht.

Automatisierung von Sicherheitsmaßnahmen zur Verkürzung der Reaktionszeiten

Sicherheitsmaßnahmen sollten nach Möglichkeit automatisiert werden, um mit Bedrohungen Schritt zu halten, die sich innerhalb weniger Minuten oder sogar Sekunden im gesamten Unternehmensnetzwerk ausbreiten können.

Hier sind einige Beispiele zu Sicherheitsmaßnahmen, die automatisiert werden können

- Verteilung und Installation von Anti-Malware- und Intrusion-Prevention-System- (IPS-) Signaturdateien
- Zentralisierte Erfassung, Korrelation und Analyse von Sicherheitsprotokollen und Bedrohungsdaten
- Bedrohungsschutz, der Anfragen an bösartige Ziele blockiert, bevor überhaupt eine Verbindung hergestellt wird, und der Bedrohungen an jedem Port abwehrt, bevor sie Ihr Netzwerk und Ihre Endpunkte erreichen
- Dynamische Access Control Lists (ACLs), Domain- und Website-Whitelisting/-Blacklisting und Erstellen von Firewall-Regeln
- Bereitstellen und Entfernen von Benutzerkonten und Verwaltung von Zugriffsrechten

Melden, wenn man etwas sieht

Das Federal Bureau of Investigation der Vereinigten Staaten (FBI) fordert Opfer von Ransomware-Angriffen dringend auf, genaue Angaben zu Infektionen zu machen. Dadurch erhält das FBI einen umfassenden

Überblick über die Verbreitung und die Auswirkungen von Ransomware. Laut FBI ist es eine große Herausforderung, „die genaue Anzahl der Opfer von Ransomware zu bestimmen, da viele Infektionen nicht gemeldet werden."

Das FBI befürchtet, dass Opfer Infektionen aus verschiedenen Gründen nicht melden. Viele Betroffene scheinen keinen Sinn darin zu sehen, besonders, wenn sie glauben, das Problem intern durch die Zahlung eines Lösegeldes oder durch Entfernen der Malware-Infektion aus der Welt schaffen zu können.

MERKEN

Das FBI warnt ausdrücklich vor Lösegeldzahlungen: „Die Zahlung eines Lösegeldes garantiert nicht, dass das Opfer seine Daten zurückerhält. Einige Personen oder Organisationen erhalten niemals einen Entschlüsselungscode, auch wenn sie das Lösegeld gezahlt haben. Durch die Zahlung eines Lösegelds werden die Täter darin bestärkt, auch von anderen Opfern Geld zu verlangen, und es kann ein Anreiz für andere Kriminelle sein, sich mit ähnlichen rechtswidrigen Aktivitäten Gewinne zu verschaffen."

TIPP

Wenn Sie eine Infektion melden wollen, gehen Sie zu `www.ic3.gov` und machen Sie folgende Angaben:

- Datum der Infektion und Informationen zum betroffenen Unternehmen (wie Branche und Unternehmensgröße).
- Ransomware-Variante (auf der Lösegeldnachricht oder durch die Dateiendung identifiziert)
- Wie die Infektion aufgetreten ist (zum Beispiel ein Link in einer E-Mail-Nachricht oder beim Browsen im Internet)
- Gefordertes Lösegeld und ggf.gezahlter Betrag.
- Bitcoin-Wallet-Adresse des Angreifers (möglicherweise in der Lösegeldnachricht enthalten)
- Durch die Ransomware-Infektion erlittener Gesamtverlust (einschließlich Lösegeldsumme und Erklärung des Opfers zu den Folgen der Straftat)

Cisco Umbrella

Weiterentwickelte moderne Bedrohungen erfordern einen modernen Sicherheitsansatz.

68% der Unternehmen haben zielgerichtete Angriffe erlebt, bei denen Zweigstellen und Roaming-Benutzer die Quelle der Kompromittierung waren.*

So schützen Sie sich:
https://umbrella.cisco.com/how-to-stop-ransomware

* Enterprise Strategy Group, 2019

Lassen Sie nicht zu, dass Ransomware Ihre Dateien in Geiselhaft nimmt!

Ransomware ist eine sich schnell entwickelnde Malware-Bedrohung, die die globale Wirtschaft bis 2021 voraussichtlich 6 Billionen US-Dollar kosten wird. Schlimmer noch: Durch die Zahlung von Lösegeldern, die in die Zehntausende gehen können, finanzieren die Opfer die nächsten Generationen von Ransomware direkt mit!

In diesem Buch erfahren Sie, wie Sie Ihr Unternehmen vor Ransomware und anderen Bedrohungen schützen können.

Im Buch ...

- Ransomware stoppen, bevor sie Ihr Netzwerk erreicht
- Fortschrittlichen Malware-Schutz an Endpunkten und E-Mail-Gateways einsetzen
- Command-and-Control-Callbacks blockieren
- Sicherheitsabläufe vereinfachen

Lawrence Miller, CISSP, ist seit über 25 Jahren in verschiedenen Branchen im Bereich Sicherheit in der Informationstechnologie tätig. Er ist Mitautor des Buches *CISSP Für Dummies* und hat über 90 weitere *Für-Dummies*-Bücher zu zahlreichen technischen und sicherheitsbezogenen Themen verfasst.

Besuchen Sie Dummies.com®
für Schritt-für-Schritt-Anweisungen mit Bildern, Kurzanleitungen oder andere Bücher!

ISBN: 978-1-119-69607-0
Nicht für den Weiterverkauf bestimmt

9 781119 696070

für dummies®

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.