CYBERARK®

CyberArk Labs

Analyse von Ransomware und mögliche Strategien zur Eindämmung

RESEARCH

Einführung

Der Name „Ransomware“ bezieht sich auf eine Art von Malware, die darauf ausgelegt ist, Systeme zu infizieren und so viele Dateien wie möglich zu verschlüsseln, wobei die Möglichkeit zur Entschlüsselung der Daten nur gegen Zahlung eines Lösegelds eingeräumt wird. Obwohl dokumentierte Beschwerden über moderne Ransomware bis ins Jahr 2005 zurückreichen, hat die Verbreitung der Malware in letzter Zeit deutlich zugenommen. Allein 2015 wurden rund 407.000 Versuche zur Infektion mit Ransomware durchgeführt und mehr als 325 Millionen USD von den Opfern erpresst. Diese Zahlen dürften im Jahr 2016 weiter steigen .

Ransomware hat sich aus zwei Gründen zu einem bevorzugten Mittel der Erpressung durch opportunistische Angreifer entwickelt. Erstens sind die Sicherungs- und Wiederherstellungspraktiken vieler Unternehmen unzureichend. Sicherungen erfolgen oftmals nur sporadisch und in zu großen zeitlichen Abständen, was bedeutet, dass Unternehmen bei einer Fremdverschlüsselung und Freipressung ihrer Daten auf Endpunkten und Servern zwei Optionen haben, nämlich ihre Daten für immer zu verlieren oder – hoffentlich – gegen Zahlung von Bitcoins zurückzuerhalten. Zweitens setzen viele Unternehmen auf traditionelle Virenschutzlösungen, die Ransomware oft nicht wirksam blockieren. Diese Lösungen führen eine Bestandsliste bekannter Malware und blockieren die zukünftige Ausführung dieser Programme. Da sich Ransomware-Dateien mit jeder neuen Version leicht verändern und neue Versionen praktisch minütlich erstellt werden, haben herkömmliche Virenschutzlösungen kaum eine realistische Chance, eine Infektion zu verhindern.

Dieses Papier dokumentiert die Forschungen von CyberArk Labs zur Untersuchung von Ransomware und Erarbeitung möglicher Eindämmungsstrategien. Eine der wichtigsten Erkenntnisse: Durch den Entzug lokaler Administratorrechte und die Einführung von Richtlinien zur Anwendungskontrolle wurden 100 Prozent der Ransomware-Stichproben an der Verschlüsselung von Dateien gehindert.

Von Krankenhäusern über Schulen bis hin zu Banken, selbst ein Team des US-Motorsportverbandes NASCAR, fallen Organisationen immer häufiger Ransomware-Angriffen zum Opfer. Die von den Angreifern verlangten Lösegeldsummen können stark variieren. Ein Opfer berichtete von der Forderung eines Bitcoins für jedes infizierte System, zum damaligen Zeitpunkt etwa 450 USD pro Computer . Angesichts der Tatsache, dass sich bestimmte Stämme von Ransomware rasant in einer Umgebung ausbreiten können, kann die Gesamtforderung der Ransomware exponentiell höher als 450 USD sein.

1 http://cyberthreatalliance.org/cryptowall-report.pdf
2 http://www.securityweek.com/lechiffre-ransomware-hits-indian-banks-pharma-company

Forschungsansatz

Für seine Forschungen benötigte CyberArk echte Proben von Ransomware und eine realistische Testumgebung für Versuche mit der Ransomware. Das Team von CyberArk Labs entwickelte ein spezielles Labor mit echten, physischen Computern und echten Dateien, um der Ransomware die Ausführung und Ausbreitung wie im System eines zum Opfer gefallenen Unternehmens zu ermöglichen. Bisher hat das Team mehr als 23.000 Proben von Schadsoftware getestet und noch immer werden täglich Versuche mit neuen Proben durchgeführt. Unter diesen Proben findet sich Ransomware von über 30 verschiedenen Malware-Familien, wobei die meisten Proben Cryptolocker, Petya und Locky, den am weitesten verbreiteten und berüchtigtsten Ransomware-Familien, entstammen.

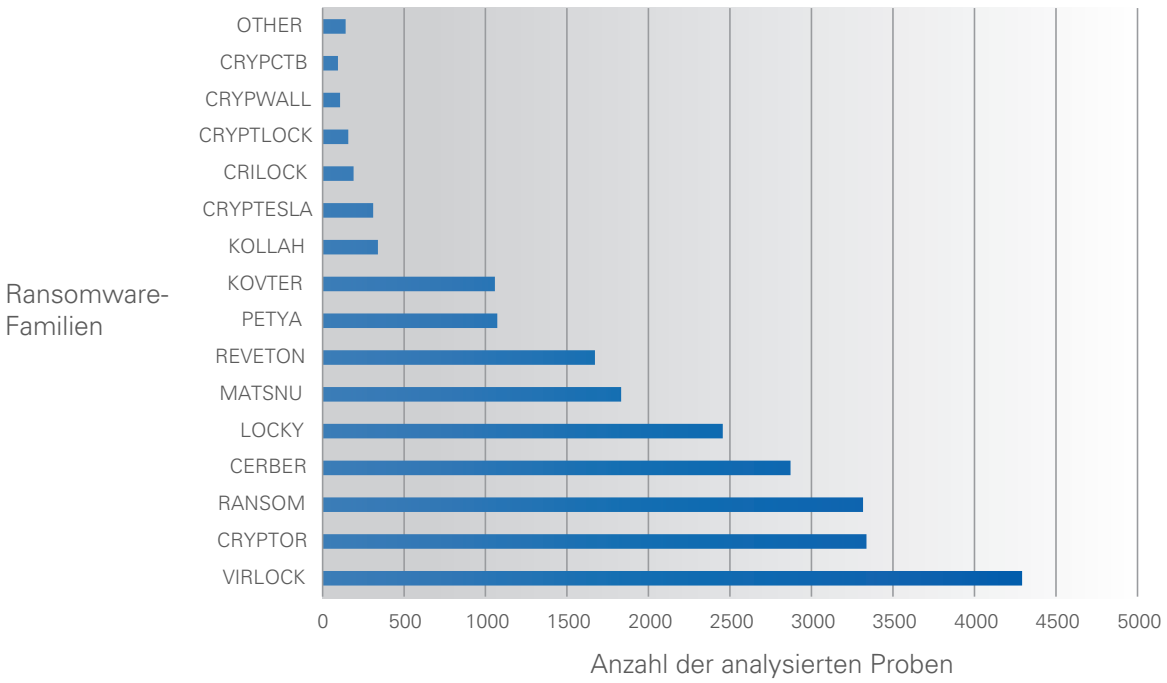
Angesichts der hohen Zahl der einzelnen Ransomware-Stämme stellen die 23.000 getesteten Proben nur eine kleine Teilmenge der bekannten Ransomware dar. Aufgrund der polymorphen Struktur der Ransomware ist die Stichprobe jedoch äußerst repräsentativ in Bezug auf die Ransomware insgesamt. Obwohl jede neue Ransomware-Datei leicht von ihrer Vorgängerversion abweicht, haben alle Versionen gemeinsame Infektions- und Ausführungsmethoden. Sie verfügen lediglich über verschiedene Dateihashes, um einer Erkennung zu entgehen.

Ziel dieser Studie war die Analyse der Verhaltensweisen der getesteten Ransomware-Proben, um besonders wirksame Strategien zur Eindämmung der durch diese Angriffe entstehenden Schäden zu bestimmen. Das Team als solches bewertete die Vorteile und Herausforderungen der folgenden Strategien:

- Whitelisting von Anwendungen
- Blacklisting von Anwendungen
- Greylisting von Anwendungen
- Least-Privilege-Kontrolle
- Sicherung und Wiederherstellung

DIAGRAMM DER GETESTETEN MALWARE-FAMILIEN – Aktualisiert am 27.07.2016

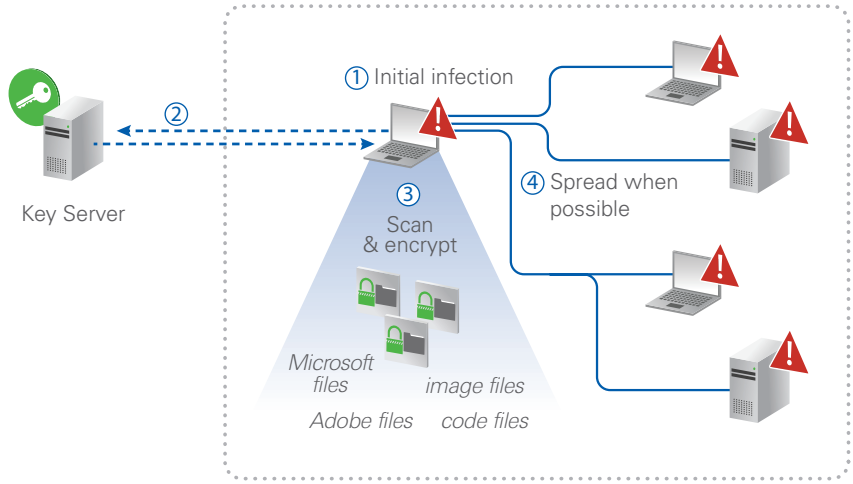
Abbildung 1. **Anzahl der getesteten und analysierten Proben aus jeder Ransomware-Familie**



Erkenntnisse: Der Verschlüsselungspfad

Vor der Beurteilung möglicher Eindämmungsstrategien versuchte das Forschungsteam zunächst, Erkenntnisse über das typische Verhalten von Ransomware zu erlangen. Abbildung 2 zeigt den typischen Workflow, dem die Mehrheit der Ransomware nach Beginn der Ausführung folgte. Eine interessante Beobachtung: Obwohl die verschiedenen Ransomware-Familien über ähnliche Workflows verfügten, hatten verschiedene Familien verschiedene „Auslöser" bzw. Aktionen, die zur Ausführung der Ransomware führten. Einige Familien begannen die Ausführung sofort, während andere auf eine Internetverbindung, auf eine Bewegung des Mauszeigers oder die Ausführung einer Microsoft Office-Anwendung warteten.

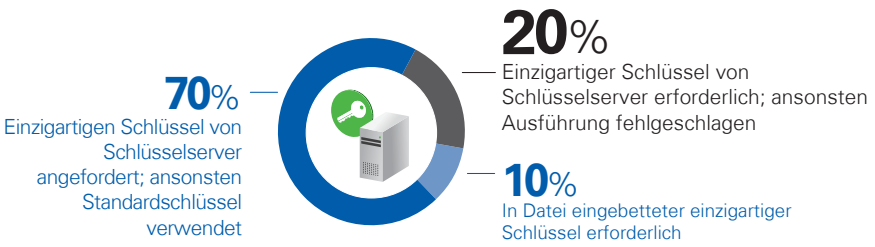
Abbildung 2: **Workflow von Dan**



Nachdem die Ausführung der Ransomware ausgelöst wurde, versuchten 90 Prozent der analysierten Proben, zuerst mit einem vom Angreifer verwalteten Schlüsselserver zu kommunizieren, auf dem sich der einzigartige öffentliche Schlüssel zur Verschlüsselung der Dateien auf dem Computer befand. In 20 Prozent aller Fälle schlug die Ausführung der Ransomware fehl, wenn keine Verbindung zu diesem Server hergestellt werden konnte. Dennoch konnten 70 Prozent der Ransomware mit einem öffentlichen Standardschlüssel ausgeführt werden, auch wenn die Übermittlung eines einzigartigen Schlüssels vom Schlüsselserver nicht möglich war. Dieser Ansatz ist für einen Angreifer unter Umständen weniger effektiv, da das Opfer möglicherweise bereits einen Standardschlüssel erworben hat, mit dem es alle entsprechend verschlüsselten Dateien entschlüsseln kann. Bei den verbleibenden 10 Prozent der Proben war der einzigartige öffentliche Schlüssel in der Ransomware-Datei selbst enthalten, wodurch die Notwendigkeit einer externen Verbindung wegfiel. Basierend auf dieser Beobachtung stellte das Forschungsteam fest, dass Unternehmen durch die Verhinderung eines externen Verbindungsaufbaus der Ransomware in der Regel entweder die Ausführung der Ransomware verhindern oder die Angreifer zur Verwendung eines Standardschlüssels zwingen und somit die finanziellen Auswirkungen des Angriffs minimieren können.

Kurven- oder Kreisdiagramm – Abhängigkeit von einzigartigem Schlüssel

Abbildung 3: **Anteil der von einem einzigartigen Verschlüsselungsschlüssel abhängigen Ransomware**



Anschließend begann die Ransomware mit dem Scannen der infizierten Computer, um nach bestimmten Dateitypen zu suchen. Die Ransomware-Proben suchten unter anderem nach folgenden Dateitypen und -erweiterungen:

- Microsoft Office-Dateien: .doc, .docx, .xls, .xlsx, .ppt, .pptx
- Adobe-Dateien: .pdf, .ai, .psd, .indd, .ps, .eps
- Bilddateien: .jpeg, .png, .gif, .bmp, .tiff, .pcx, .emf, .rle, .dib
- Code-Dateien: .c, .h, .cpp, .py, .vb

Nach dem Aufspüren der Dateien begann die Ransomware mit dem Verschlüsselungsprozess. Einige Ransomware-Familien durchsuchten die Verzeichnisse einzeln methodisch nach Dateien und verschlüsselten diese unmittelbar nach der Entdeckung. In diesen Fällen nahm der gesamte Prozess von der Verschlüsselung bis zur Benachrichtigung nur wenige Sekunden bis Minuten in Anspruch. Andere gingen subtiler vor, um einer Entdeckung zu entgehen. Die Proben innerhalb dieser Familien generierten zuerst eine Liste aller zu verschlüsselnden Dateien und begannen dann den Verschlüsselungsvorgang nach dem Zufallsprinzip, um unter dem Radar der Lösungen zur Bedrohungserkennung des Endpunkts zu bleiben.

Während die Ransomware damit beschäftigt war, Dateien zu verschlüsseln, versuchte sie gleichzeitig, die Anzahl der betroffenen Systeme zu maximieren. Hierfür durchsuchte die Ransomware den infizierten Computer nach angeschlossenen Laufwerken, Endpunkten und Servern und verbreitete sich dann so weit wie möglich, um die Anzahl der freizupressenden Systeme zu erhöhen. Dies erfolgte in der Regel auf zwei Arten. Erstens waren die meisten Ransomware-Proben in der Lage, gemeinsam genutzte Laufwerke und Netzlaufwerke zu ermitteln, die über die infizierten Endpunkte zugänglich waren. Wenn das Benutzerkonto Zugriff auf diese Laufwerke hatte, traf dies auch auf die Ransomware zu. Zweitens scannten die Ransomware-Proben häufig nach verbundenen Computern und versuchten, die Anmeldedaten auch für den Zugriff auf diese Computer zu nutzen. War die Anmeldung erfolgreich, konnte sich die Ransomware weiter verbreiten und somit die Gesamtzahl der infizierten Systeme steigern und die Wiederherstellungskosten für das Opfer in die Höhe treiben.

Nachdem die Verschlüsselung abgeschlossen war und die Ransomware ihren Versuch unternommen hatte, sich im Netzwerk auszubreiten, erhielten die Benutzer einen Lösegeldhinweis ähnlich dem in Abbildung 4. Um den zum Entschlüsseln der betroffenen Dateien erforderlichen Schlüssel zu erhalten, mussten die Benutzer Lösegeldzahlungen an die Angreifer leisten. In der Regel wurden diese Zahlungen in Bitcoin gefordert. Für Bitcoin-Neulinge richteten einige Angreifer sogar „Helpdesks“ ein, die den Opfern beim Erwerb von Bitcoins und der Übermittlung der Zahlung helfen sollten

Abbildung 4: **Ransomware-Hinweis für von CTB-Locker infizierte Benutzer**

Gemeinsamkeiten aller Ransomware-Familien

Während die Proben innerhalb der verschiedenen Ransomware-Familien leicht unterschiedliche Merkmale aufwiesen, hatten alle drei Dinge gemeinsam:

- Die Ransomware konnte mühelos Computer infizieren
- Nach der Infektion wurde die überwiegende Mehrheit der Dateien erfolgreich verschlüsselt
- Die Ransomware-Dateien selbst konnten leicht entfernt werde

Infektion

Eine der wichtigsten Erkenntnisse war, dass die Ransomware durch herkömmliche Virenschutzsoftware häufig nicht aufzuhalten war. Grund dafür ist, dass herkömmliche Virenschutzprogramme mit bekannten Blacklists arbeiten, was bedeutet, dass eine bestimmte Malware-Datei bereits bekannt sein (also schon mindestens einen Computer infiziert haben) muss, um auf eine Blacklist zu gelangen. Aufgrund der polymorphen Struktur der meisten Ransomware-Familien gleicht keine Probe genau einer anderen. Stattdessen generieren die Angreifer mit jedem neuen Zielopfer schnell eine neue leicht veränderte Version der Malware-Datei, um die Blacklisting-Technologien zu meiden und damit einer Erkennung zu entgehen.

Diese einfache Art der Infektion führte das Forschungsteam zu dem Schluss, dass die gängigen Virenschutzbemühungen im Kampf gegen polymorphe Malware nicht ausreichen. Um die Infektion von Computern mit Ransomware zu vermeiden, müssen Unternehmen einen proaktiveren Ansatz für die Sicherheit von Endpunkten und Servern, wie das Whitelisting und/oder Greylisting von Anwendungen, wählen.

Verschlüsselung

Eine zweite wichtige Erkenntnis: Obwohl zur Ausführung vieler Stämme moderner Malware lokale Administratorrechte erforderlich sind, benötigen einige Ransomware-Stämme keine solchen Rechte. Während 70 Prozent der getesteten Ransomware versuchte, lokale Administratorrechte zu erlangen, schlugen nur 10 Prozent fehl, wenn diese Rechte verwehrt wurden.

Dies führte das Forschungsteam zu dem Schluss, dass Unternehmen nicht nur lokale Administratorrechte entziehen, sondern auch proaktiv Anwendungen kontrollieren sollten, um eine Dateiverschlüsselung zu verhindern. So fand das Team von CyberArk Labs etwa heraus, dass die durch Ransomware verursachte Dateiverschlüsselung in 100 Prozent der Fälle verhindert werden kann, wenn Berechtigungen zum Lesen, Schreiben und Ändern von Dateien durch unbekannte Anwendungen verwehrt und lokale Administratorrechte entzogen werden.

Entfernung

Im Gegensatz zu einigen Stämmen hochentwickelter Malware, die sich häufig nur schwer lokalisieren und entfernen lässt, waren die analysierten Ransomware-Proben nach ihrer Erkennung und Lokalisierung leicht entfernbar. Dies bedeutet, dass Opfer von Ransomware-Angriffen, die ihre Daten proaktiv sichern, die Auswirkungen von Ransomware deutlich reduzieren und vermeiden können, sich zwischen der Zahlung eines hohen Lösegeldes und einem dauerhaften Datenverlust entscheiden zu müssen. Stattdessen können diese Unternehmen bei einer Verschlüsselung ihrer Daten die Ransomware-Dateien auf den infizierten Computern lokalisieren und aus dem System entfernen und anschließend die verschlüsselten Dateien aus der Sicherung wiederherstellen.

Folglich kann die proaktive Sicherung von Dateien auf Endpunkten und Servern helfen, die durch Ransomware verursachten Schäden zu minimieren. Durch die häufige Sicherung wichtiger Daten wird die Beseitigung der Folgen von Ransomware-Angriffen deutlich einfacher. Gleichzeitig lässt sich das Ausmaß der durch diesen Malware-Stamm verursachten Schäden begrenzen.

Bewertung von Eindämmungsstrategien

Bevor eines oder mehrere Verfahren zur Eindämmung der Risiken von Ransomware gewählt werden kann, sollten Unternehmen die Vorteile und Herausforderungen der einzelnen Optionen abwägen. In diesem Abschnitt werden die von CyberArk Labs bewerteten und getesteten Eindämmungsstrategien sowie ihre Vor- und Nachteile beschrieben.

Die Studie hat gezeigt, dass das Greylisting von Anwendungen zusammen mit dem Entzug lokaler Administratorrechte zu **100 Prozent wirksam bei der Verhinderung der Dateiverschlüsselung durch Ransomware** war.

Whitelisting von Anwendungen

Das Whitelisting von Anwendungen ist naturgemäß zu 100 Prozent wirksam im Kampf gegen Ransomware, da bei diesem Verfahren alle Anwendungen blockiert werden, die nicht explizit vertrauenswürdig sind. Obwohl Ransomware-Angriffe mit dieser Eindämmungsstrategie äußerst wirksam verhindert werden können, ist sie in der Praxis nur schwer umzusetzen. Für ein effektives Whitelisting von Anwendungen müssen IT-Teams genau wissen, welche Anwendungen und Anwendungsversionen jeder einzelne Benutzer und jedes System im Unternehmen braucht, und jede einzelne Anwendungsversion muss vom IT-Team explizit auf die Whitelist gesetzt werden. Das Whitelisting von Anwendungen mag ein optimaler Ansatz für Server sein, die in der Regel statisch sind. Auf dynamischen Benutzerendpunkten hingegen, die oftmals eine Vielzahl von Geschäftsanwendungen erfordern, kann dieser Ansatz die Produktivität der Benutzer zum Erliegen bringen.

Blacklisting von Anwendungen

Mit diesem Ansatz können Unternehmen die Ausführung bekannter Malware (d. h. Malware, die bereits mindestens einen Computer infiziert hat) in ihrer Umgebung verhindern. Während hiermit ältere Versionen von opportunistischer Malware erkannt und blockiert werden können, ist diese Methode äußerst unwirksam beim Schutz vor Ransomware. Jeden Tag werden Tausende von neuen Ransomware-Versionen veröffentlicht, womit herkömmliche Blacklists schlichtweg überfordert sind . In der Folge stellte das Forschungsteam fest, dass das Blacklisting von Anwendungen zwar eine allgemein bewährte Methode darstellt, zur Erkennung oder Verhinderung von Ransomware aber nicht ausreicht.

Greylisting von Anwendungen

Dieser Ansatz erlaubt es Unternehmen, die Ausführung bekannter Malware auf Blacklists in ihren Umgebungen zu verhindern und gleichzeitig die Berechtigungen für alle Anwendungen, die nicht explizit vertrauenswürdig sind, zu begrenzen. Der Ansatz bietet also mehr Flexibilität als das Whitelisting und kann dazu dienen, Aktionen unbekannter Anwendungen, wie das Herstellen einer Internetverbindung und das Lesen, Schreiben oder Ändern von Dateien, zu verhindern. Ohne Internetzugriff war die Ransomware nicht in der Lage, auf ihren Schlüsselserver zuzugreifen. Dies führte dazu, dass 20 Prozent der Ransomware sofort unwirksam und 70 Prozent gezwungen waren, die Verschlüsselung mit einem Standardschlüssel zu versuchen. Hinzu kommt, dass durch die Beschränkung der Berechtigungen zum Lesen, Schreiben und Ändern von Dateien die Ransomware nicht in der Lage war, Dateien aufzurufen und zu verschlüsseln. Beim Testen dieses Ansatzes mit den Ransomware-Proben verzeichnete das Team von CyberArk Labs eine Erfolgsquote von 99,97 Prozent im Hinblick auf die Verhinderung der Dateiverschlüsselung, wenn der infizierte Benutzer über lokale Administratorrechte verfügte. Waren keine Administratorrechte vorhanden, lag die Erfolgsquote bei 100 Prozent.

3 http://www.businessinsider.com/fighting-ransomware-with-antivirus-2016-1

Least-Privilege-Kontrolle

Dieser Schritt ist nicht nur eine Sicherheitsroutine, sondern gilt auch als einer der „Zehn unveränderlichen Gesetze zur Sicherheit" von Microsoft. Interessanterweise stellte das Team von CyberArk Labs fest, dass der Entzug lokaler Administratorrechte zwar häufig Wirkung im Kampf gegen einen Großteil moderner Malware zeigt, allein jedoch nur bei 10 Prozent der analysierten Ransomware-Proben funktionierte. Durch diese Beobachtung wird noch einmal deutlich, wie wichtig der Entzug lokaler Administratorrechte in Kombination mit der Kontrolle von Anwendungen ist. Bevor sie lokale Administratorrechte vollständig entziehen, sollten Unternehmen aber unbedingt ihre Umgebung analysieren, um mögliche mit diesem Schritt verbundene Produktivitätsprobleme zu erkennen. Einige legitime Geschäftsanwendungen und Aufgaben erfordern Administratorrechte, um ordnungsgemäß zu funktionieren, weshalb sich der sofortige Entzug dieser Berechtigungen ohne Ausnahmeregeln für erforderliche Aufgaben negativ auf den Geschäftsbetrieb auswirken kann.

Sicherung und Wiederherstellung

Die Datensicherung sollte Bestandteil der Disaster-Recovery-Strategie jedes Unternehmens sein. Eine automatisierte Sicherung gewährleistet, dass die gesicherten Dateien vollständig und aktuell sind. Die Dateisicherung kann Ransomware-Angriffe nicht verhindern, aber den dadurch entstehenden Schaden deutlich reduzieren. Anstatt einer Lösegeldzahlung zur Entschlüsselung der betroffenen Daten können Unternehmen diese einfach aus der letzten Sicherung wiederherstellen. Sie sollten die Kosten für die Sicherung und Speicherung gegen die Kosten eines Datenverlustes mit Wiederherstellungsmaßnahmen abwägen und zu sichernde Dateien oder Vermögenswerte je nach Risikotoleranz und Budget des Unternehmens priorisieren.

Empfehlungen

Auf der Grundlage seiner Studie empfiehlt das Team von CyberArk Labs die Anwendung der folgenden Eindämmungsmaßnahmen, um die mit Ransomware verbundenen Risiken ohne negative Auswirkungen auf die Produktivität des Unternehmens zu senken.

- Führen Sie eine Greylist für Anwendungen auf Benutzerendpunkten ein, um unbekannte Anwendungen (z. B. neue Ransomware-Instanzen) daran zu hindern, auf das Internet zuzugreifen und die zur Verschlüsselung Ihrer Dateien erforderlichen Lese-, Schreib- und Änderungsberechtigungen zu erlangen.
- Führen Sie eine Whitelist für Anwendungen auf Servern ein, um die Sicherheit dieser Vermögenswerte zu maximieren.
- Entziehen Sie lokale Administratorrechte von Standardbenutzerkonten, um die Angriffsfläche zu reduzieren.
- Lassen Sie die Kontoberechtigungen für bestimmte legitime Aufgaben automatisch erweitern, damit die Benutzer produktiv bleiben, ohne über unnötige Berechtigungen zu verfügen.
- Nutzen Sie Virenschutzprogramme, um sich vor allgemeiner und bekannter Malware zu schützen.
- Sichern Sie die Daten von Endpunkten und Servern häufig, um eine effektive Disaster Recovery zu gewährleisten.

Für die besten Ergebnisse empfiehlt CyberArk Labs Unternehmen die Bewertung ihrer Umgebungen, um alle Endpunkte und Server mit sensiblen oder wichtigen Dateien zu lokalisieren. Nach dem Whitelisting von Anwendungen auf statischen Servern sollten Unternehmen bestimmen, welche Dateitypen auf Endpunkten die wichtigsten Informationen enthalten (z. B. XLSX, PPTX, PDF usw.). Eine solche Bewertung kann Unternehmen bei der Ermittlung besonders wichtiger Dateitypen unterstützen und helfen, effektive Greylisting-Richtlinien zu erstellen, um diese Dateitypen vor unbekannten Anwendungen zu schützen.

Fazit

Nach dem Analysieren und Testen von mehr als 23.000 Proben von Ransomware hat CyberArk Labs nachgewiesen, dass ein alternativer, proaktiver Sicherheitsansatz wirksam beim Schutz vor Ransomware sein und dadurch die negativen Folgen dieser Art von Angriff deutlich minimieren kann.

Neben dem Entzug lokaler Administratorrechte von Standardbenutzerkonten und einer regelmäßigen Datensicherung, beides gängige Verfahren im IT-Bereich, sollten Unternehmen auch einen Greylist-Ansatz für die Anwendungskontrolle auf Endpunkten in Betracht ziehen. Mit einem solchen Ansatz können Unternehmen unbekannte Anwendungen, die weder explizit vertrauenswürdig sind noch auf einer Blacklist stehen, daran hindern, auf das Internet zuzugreifen und die Berechtigungen zum Lesen, Schreiben und Ändern bestimmter Dateitypen zu erlangen. Somit können sich Unternehmen auf den Schutz ihrer Dateien – dem Ziel bösartiger Anwendungen – konzentrieren, anstatt sich nur auf die potenzielle Erkennung polymorpher Malware zu verlassen, was in der Praxis ein sehr kompliziertes Unterfangen ist. Bei den Versuchen im CyberArk Lab erwies sich die Kombination aus Greylisting von Anwendungen und Entzug lokaler Administratorrechte als zu 100 Prozent wirksam bei der Verhinderung des Zugriffs auf geschützte Dateitypen und deren Verschlüsselung durch Ransomware.

ÜBER CYBERARK LABS

CyberArk Labs ist ein Team von Experten für Cyber-Sicherheit, die gezielte Angriffe auf Firmennetzwerke, die Methoden, Werkzeuge und Verfahren der Angreifer sowie die Methoden und Verfahren zur Erkennung und Eindämmung solcher Angriffe erforschen.

US HEADQUARTERS

CyberArk
60 Wells Avenue
Newton, MA 02459
1-888-808-9005
or (617) 965-1544