So schützt Proofpoint Sie vor Ransomware

Stoppen Sie die Verbreitung von Ransomware in Ihrem Unternehmen

Produkte

- Proofpoint Advanced Threat Protection
- Proofpoint Cloud Security

Wichtige Vorteile

- Verhinderung der Erstinfektion
- Verhinderung von Aufklärung, lateraler Bewegung und Persistenz
- Verhinderung von Datenexfiltration

Ransomware gehört derzeit zu den zerstörerischsten Cyberangriffen. Dabei werden Geschäftsabläufe unterbrochen, Behandlungen in Krankenhäusern unmöglich gemacht und ganze Stadtverwaltungen blockiert. Ransomware hat sich mittlerweile zu einer der gefährlichsten Cyberbedrohungen entwickelt. Die USA verzeichneten allein im letzten Jahr mehr als 65.000 Ransomware-Angriffe. Diese Bedrohung ist die größte Sorge von CISOs und zudem zu einer Angelegenheit der nationalen Sicherheit geworden. Besorgniserregend ist auch, dass viele Unternehmen auf einen Ransomware-Angriff ganz und gar nicht vorbereitet sind. Nur 13 % der vom Ponemon Institute befragten IT-Experten gaben an, dass ihr Unternehmen einen Ransomware-Angriff abwehren kann. Außerdem schätzen sich mehr als 68 % als „anfällig“ oder „sehr anfällig“ ein.[1]

Die wichtigsten Vektoren von Ransomware-Angriffen sind E-Mails und das Web. Die meisten Angriffe laufen heutzutage in mehreren Stufen ab, wobei zu Beginn der Angriffskette E-Mails oder kompromittierte Webseiten eine zentrale Rolle spielen. Über sie wird häufig eine Erst-Payload als Malware-Downloader übertragen. Diese Payloads dienen dazu, Zugang zum betroffenen System zu erlangen und anschließend zumeist Anmeldedaten zu stehlen sowie Zugang zum Netzwerk des Anwenders zu erlangen. Die Ransomware-Akteure nutzen die gestohlenen Anmeldedaten auch, um auf Dienste zuzugreifen, die mit dem Internet verbunden sind. Zu den häufig verwendeten Taktiken gehören E-Mails mit Anmeldedaten-Phishing, Brute-Force-Angriffe auf Kennwörter sowie Drive-by-Downloads.

Haben sie einmal den Zugriff auf ein System erlangt, setzen sich die Akteure dort fest, führen Aufklärungsaktionen durch und bewegen sich lateral durch das Netzwerk. Innerhalb des Systems können die Angreifer vertrauliche Dateien nicht nur verschlüsseln, sondern auch exfiltrieren, um die Opfer anschließend doppelt zu erpressen.

Angesichts des zunehmenden Erfolgs von Backup- und Wiederherstellungsmaßnahmen bei der Abwehr von Ransomware-Angriffen mussten die Bedrohungsakteure ihre Taktiken ändern und setzen daher nun Ransomware mit doppelter Erpressung ein. Bei dieser Taktik werden vertrauliche Daten zunächst exfiltriert und dann verschlüsselt. Lehnt das Opfer die Zahlung für

1 Ponemon Institute: „The Rise of Ransomware“ (Die Zunahme von Ransomware), Januar 2017.

die Entschlüsselung der Daten ab, hat der Bedrohungsakteur drei Möglichkeiten, um eine Zahlung zu erzwingen:

- Dem Opfer mit der Veröffentlichung der Daten drohen
- Die Daten an den Meistbietenden verkaufen
- E-Mails direkt an die Kunden sowie Partner des Opfers schicken und mit der Veröffentlichung ihrer Daten drohen

Da bei Ransomware-Angriffen zumeist E-Mails zur Erstinfektion eingesetzt werden, beginnt ein großer Teil der Angriffe – direkt oder indirekt – mit einer Phishing-E-Mail. Dabei werden die Anwender dazu verleitet, einen schädlichen Anhang zu öffnen oder auf eine schädliche URL zu klicken. Um diese Bedrohungen zu erkennen und die Kompromittierung von Anmeldedaten zu verhindern, benötigen Sie hochentwickelte Lösungen. Immer mehr Unternehmensdaten werden in der Cloud gespeichert. Das gilt auch für Kennwort-Dateien und vertrauliche Inhalte. Es ist wichtig, Datenkompromittierungen in der Cloud zu minimieren, damit so wenige Daten wie möglich in die Hände von Kriminellen gelangen.

Proofpoint stellt fest, dass Ransomware-Angriffe immer zielgerichteter erfolgen, größere Schäden anrichten und häufiger zu Geschäftsunterbrechungen führen. Proofpoint Advanced Threat Protection und Proofpoint Cloud Security können Ihnen helfen, Angriffe zu verhindern. Unsere umfassenden und integrierten Plattformen verringern das Risiko von Ransomware-Angriffen, da sie Kontrollen kombinieren und somit folgende Vorteile bieten:

- Verhinderung der Erstinfektion
- Erkennung des Erstzugriffs sowie Verhinderung von Aufklärung, lateraler Bewegung und Persistenz
- Verhinderung von Datenexfiltration

Verhinderung der Erstinfektion

So verhindern Proofpoint Advanced Threat Protection und Proofpoint Cloud Security die Erstinfektion:

- Erkennung und Blockierung von Ransomware- und Malware-Downloadern, die Ransomware-Angriffe auslösen
- Verhinderung von Anmeldedaten-Kompromittierung
- Überblick über Ransomware-Risiken
- Isolierung von URL-Klicks abhängig vom Risiko
- Schulung der Anwender, um schädliche E-Mails zu erkennen und zu melden
- Automatische Behebung von E-Mail-Bedrohungen

Erkennung und Blockierung von Ransomware- und Malware-Downloadern

Die Proofpoint Advanced Threat Protection-Plattform erkennt und blockiert Ransomware, die als Erst-Payload dient. Sie blockiert außerdem Malware, die Ransomware verbreitet. Mithilfe mehrerer Machine Learning-Module erkennt die Plattform Malware, schädlichen Code sowie Techniken zur Erkennungsumgehung und schützt die Anwender somit vor schädlichen Websites oder mit Ransomware infizierten Dateien.

Die Plattform führt zudem Reputations- sowie Inhaltsanalysen durch und analysiert in Sandbox-Umgebungen isolierte Bedrohungen, die infizierte URLs und Anhänge verbreiten. Wir setzen prädiktive Analysen ein, die verdächtige URLs anhand von veränderten Angreifertaktiken identifizieren und in einer Sandbox überprüfen. Ein Beispiel: Da Angreifer oft Malware auf legitimen Datenaustausch-Websites hosten, isoliert die Plattform alle Datenaustausch-URLs in einer Sandbox. Lösungen, die nur Reputationsanalysen durchführen, würden diese Angriffe nicht erkennen.

Verhinderung von Anmeldedaten-Kompromittierung

Um die Anmeldedaten von Anwendern zu stehlen, nutzen Angreifer verschiedene Taktiken wie Phishing, Brute-Force-Angriffe, das Dark Web und kompromittierte Daten im Cloud-Speicher der Anwender. Haben Angreifer erst einmal Zugriff auf Ihre Anmeldedaten, ist kein Downloader mehr nötig. Sie können sich einfach mit Ihren Anmeldedaten in Ihrem VPN oder bei mit dem Internet verbundenen Diensten anmelden und von dort aus vertrauliche Daten stehlen oder Dateien verschlüsseln. Mit dem Einsatz zusätzlicher Cloud-Dienste in Unternehmen kann es vorkommen, dass fahrlässige Anwender Kennwort-Dateien und vertrauliche Daten in die Cloud hochladen.

Proofpoint Advanced Threat Protection erkennt und stoppt Phishing-Nachrichten mittels mehrerer Erkennungsmodule, darunter auch Machine Learning-Klassifizierer, die URLs untersuchen. Proofpoint Cloud Security kann offen liegende vertrauliche Daten in Cloud-Konten erkennen, die von Angreifern ausgenutzt werden könnten.

Überblick über Ihre Ransomware-Risiken

Proofpoint bietet Ihnen einen Überblick über Ihre Very Attacked People™ (VAPs), also die Mitarbeiter in Ihrem Unternehmen, die besonders anfällig für Angriffe sind. Sie erkennen damit, wer am häufigsten und mit welchen Bedrohungen angegriffen wird. Anhand dieser Informationen können Sie die Abwehrstrategie an die Bedrohungen anpassen, die Ihre VAPs ins Visier nehmen.

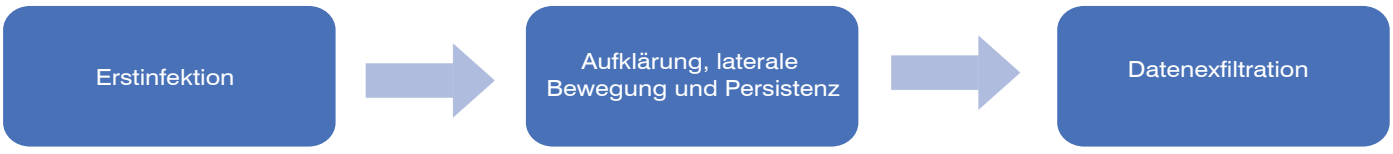

Abb. 1: Drei Schutzebenen.

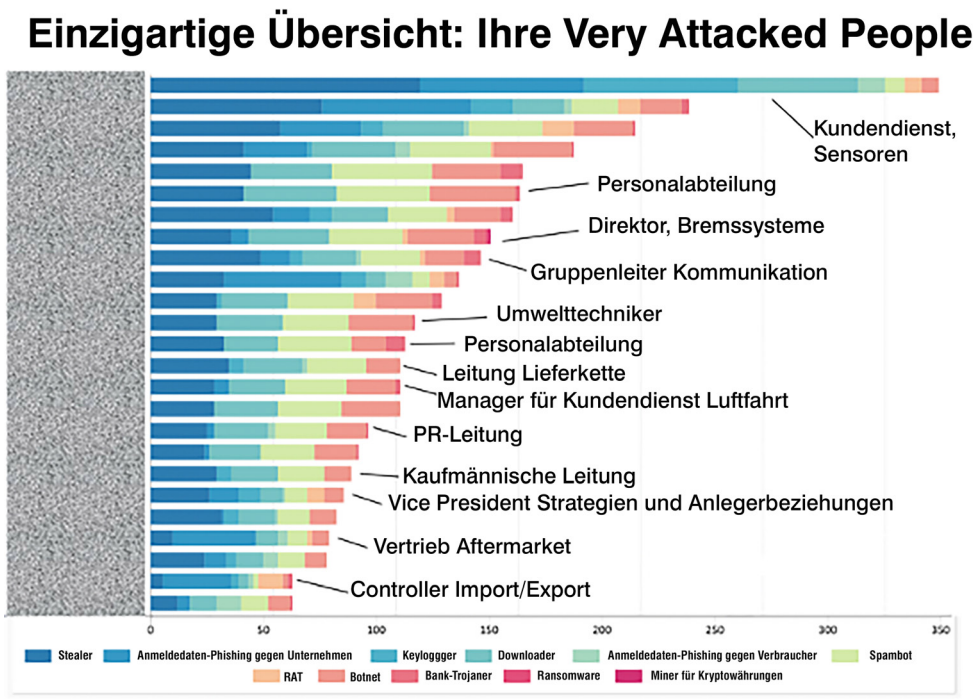

Abb. 2: Mit Proofpoint erhalten Sie einen Überblick über Ihre Very Attacked People (VAPs).

Zudem bietet Proofpoint detaillierte Informationen über Bedrohungen und Angriffskampagnen. Das Threat Insight-Dashboard enthält umfangreiche Forensikdaten, einschließlich Bedrohungsakteur, Verbreitung, Beispiel-E-Mails, vorgesehener Empfänger, Angriffsfortschritt und viele mehr.

Verringerte Auswirkungen durch integrierte Email Isolation

Angreifer können URLs nach der Zustellung manipulieren und somit die Ersterkennung umgehen. Proofpoint Browser Isolation verringert deshalb die Auswirkungen, die entstehen, wenn Anwender auf schädliche URLs klicken. Die Lösung bietet Time-of-Click-Schutz für URLs in geschäftlichen E-Mails und isoliert Browser-Aktivitäten in einem geschützten Container, der Anwendern nur eine sichere Version anzeigt. Sie verhindert ebenfalls Downloader der ersten Stufe sowie Diebstahl von Anmeldedaten und sorgt damit im Prinzip für eine Unterbrechung der Angriffskette.

Sie können risikoabhängige Isolierung implementieren, die auf Richtlinien und den Erkenntnissen über Ihre VAPs basiert. Zudem lassen sich URLs mit besonders großem Risiko in isolierte Browsersitzungen umleiten. Die Lösung bietet die Möglichkeit, strengere Richtlinien für angegriffene Mitarbeiter festzulegen, bei denen alle Anwenderklicks isoliert werden. Je nachdem, welche Anwender angegriffen werden, lassen sich die Isolierungsrichtlinien auch an das Risiko des Anwenders und der angeklickten URL anpassen.

Förderung des Sicherheitsbewusstseins Ihrer Anwender

Um Ransomware effektiv zu verhindern, müssen Sie Ihre Mitarbeiter schulen, denn sie sind schließlich Ihre letzte Verteidigungslinie. Für einen erfolgreichen Ransomware-Angriff müssen Anwender auf einen Link klicken oder einen Anhang herunterladen. Dem neuesten Verizon Data Breach Investigations Report 2021 zufolge gingen 85 % der Datenschutzverletzungen mit einer menschlichen Komponente einher.[2]

Die Threat Protection-Plattform umfasst auch Security Awareness Training, das Ihre Anwender über Ransomware informiert und sie schult, nicht auf verdächtige Nachrichten zu klicken. Anwendern, die besonders häufig angegriffen werden und bereits mit realen Bedrohungen zu tun hatten, können zusätzliche Schulungen zugewiesen werden. Mit Materialien aus unserer umfangreichen Content-Bibliothek können Sie die Inhalte der Endnutzer-Schulungen über Mitteilungen und Sicherheitswarnungen weiter festigen. Es lassen sich auch simulierte Angriffe mit Vorlagen durchführen, die auf realen Ködern basieren, die in Milliarden von Proofpoint analysierten Nachrichten beobachtet wurden. Die Plattform bietet einfache Verfahren, um verdächtige E-Mails über unsere PhishAlarm-Schaltfläche zu melden und mit Warnungs-Tags zu versehen.

Automatische Behebung schädlicher Nachrichten

Sicherheitsteams haben oft zu wenig Personal und werden häufig mit Warnmeldungen überwältigt, die schnell gesichtet und untersucht werden müssen. Die Threat Protection-Plattform bietet mSOAR-Funktionen (email-focused Security Orchestration Automation and Response), die die Untersuchung und Behebung gemeldeter sowie schädlicher oder unerwünschter Nachrichten automatisieren.

2 Verizon: „DBIR: Data Breach Incident Report“ (Untersuchungsbericht zu Datenkompromittierungen), 2021.

Die Anmeldedaten Ihrer Anwenderkonten sind der Schlüssel zu Ihrem Unternehmen. Mit einem einzigen Benutzernamen mit passendem Kennwort kann ein Ransomware-Akteur Angriffe in und aus Ihrem Unternehmen heraus durchführen.

Die von Anwendern gemeldeten Nachrichten werden automatisch analysiert und ihr Kontext mit verschiedenen Bedrohungsdaten sowie Reputationssystemen angereichert. Wird eine Nachricht als schädlich erkannt, kann sie zusammen mit allen zugehörigen Nachrichten automatisch unter Quarantäne gestellt werden. Ihr Sicherheitsteam muss nicht mehr jede Warnmeldung manuell untersuchen sowie schädliche Nachrichten beheben und spart damit sehr viel Zeit und Mühe. Um den Kreis zu schließen und richtiges Verhalten zu bestärken, erhalten die Anwender eine individuelle E-Mail, die bestätigt, dass die Nachricht in der Tat schädlich war.

Die Threat Protection-Plattform analysiert Nachrichten auch nach der Zustellung. Werden diese nach der Zustellung als schädlich erkannt, entfernt die Plattform sie automatisch aus den Posteingängen der Anwender. Dabei werden auch Nachrichten entfernt, die an andere Anwender weitergeleitet oder über Verteilerlisten verschickt wurden.

Erkennung des Erstzugriffs sowie Verhinderung von Aufklärung, lateraler Bewegung und Persistenz

So werden Ransomware-Bedrohungen von Proofpoint Cloud Security erkannt:

- Überwachung und Erkennung kompromittierter Cloud-Konten
- Suche nach schädlichen Datei-Uploads auf Cloud-Konten
- Schutz vor Command-and-Control-Verbindungen durch Proofpoint Web Security

Erkennung von Cloud-Kontoübernahmen

Die Anmeldedaten Ihrer Anwenderkonten sind der Schlüssel zu Ihrem Unternehmen. Mit einem einzigen Benutzernamen mit passendem Kennwort kann ein Ransomware-Akteur – besonders bei Cloud-Anwendungen wie Microsoft 365 oder Google Workspace – Angriffe in und aus Ihrem Unternehmen heraus durchführen. Das in Proofpoint Cloud Security enthaltene CASB bietet adaptive Echtzeit-Zugriffskontrollen, die sich nach dem jeweiligen Risiko, Kontext und der Position im Unternehmen richten. Die Lösung blockiert automatisch Zugriffsversuche von gefährlichen Standorten und Anmeldeversuche bekannter Bedrohungsakteure. Zudem greift das CASB auf Kontextdaten zurück und nutzt sie als Bestätigung einer Anwenderidentität sowie zur Verhinderung gefährlicher Zugriffe. Zu den Kontextdaten gehören Standort des Anwenders, Gerät, Netzwerk und Zeitpunkt der Anmeldung. Zum Schutz vor Ransomware-Akteuren können Sie Zugriffskontrollen festlegen, indem Sie beispielsweise Multifaktor-Authentifizierung durchsetzen und den Zugriff auf nicht verwaltete Geräte beschränken.

Mit Proofpoint erhalten Sie einen Überblick darüber, ob es laterale Bewegungen oder Risiken für Ihre Daten aufgrund eines kompromittierten Kontos gibt. Zudem können Sie sehen, ob eine verdächtige Anmeldung mit einem Konto korreliert, das schädliche E-Mails verschickt. Mit der Lösung erkennen Sie, ob ein Bedrohungsakteur durch E-Mail-Weiterleitungen und Delegierungsregeln oder mittels OAuth-Token einen langfristigen Zugang einrichten wollte. Außerdem werden Sie über verdächtige Dateiaktivitäten informiert.

Verhinderung von Ransomware-Verbreitung über Cloud-Anwendungen

Ransomware kann durch die Weitergabe infizierter Dateien und über automatische Synchronisation verbreitet werden, was schwerwiegende Folgen für Ihr Unternehmen sowie Ihre Partner und Kunden haben kann. Proofpoint Cloud Security überwacht Ihre Dateifreigaben in der Cloud und warnt Sie bei einer verdächtigen Datei. Zudem führt Proofpoint Sandbox-Analysen der Dateien in Cloud-Anwendungen durch. Schädliche Dateien in der Cloud werden automatisch unter Quarantäne gestellt oder auf andere Weise isoliert.

Schutz vor Command-and-Control-Verbindungen durch Proofpoint Web Security

Ist ein Gerät kompromittiert, sendet es ein Signal an den Server des Bedrohungsakteurs, woraufhin dieser die nächsten Anweisungen schickt. Da er die Kontrolle über das Gerät hat, kann er eine Reihe verschiedener Aktionen ausführen, die von der Verteilung von Ransomware bis hin zur Exfiltration von Daten reichen.

Die Lösungen Web Security und Browser Isolation in Proofpoint Cloud Security blockieren Verbindungen zu kompromittierten Websites und hindern somit, dass der Ransomware-Akteur die Kontrolle über das Gerät übernehmen und weitere Schäden anrichten kann. Die Daten dazu liefert Proofpoint Nexus Threat Graph. Die Lösung kombiniert Billionen von Echtzeit-Datenpunkten aus mehreren Bedrohungsvektoren weltweit, eine hochentwickelte KI sowie Machine Learning und wird durch ein globales Forschungsteam unterstützt, mit dem Sie den größten aktuellen Cyberbedrohungen immer einen Schritt voraus sind.

Verhinderung von Datenexfiltration

So verhindern Proofpoint Advanced Threat Protection und Proofpoint Cloud Security die Datenexfiltration:

- Suche nach frühen Anzeichen von Datenexfiltration
- Erkennung und Verhinderung unzulässiger Datenbewegungen

Web Security und Browser Isolation in Proofpoint Cloud Security gewährleisten Datensicherheit mit Risikokontext durch Echtzeit-Scans zur Datenverlustprävention (DLP). In Kombination mit Browser Isolation bietet Proofpoint Web Security granulare Datenkontrollen wie schreibgeschützten Zugriff sowie die Möglichkeit, den Zugriff auf Cloud-Anwendungen und Webseiten zu erlauben bzw. zu blockieren. Proofpoint Browser Isolation sichert den Anwenderzugriff auf Anwendungen und Daten ab, indem Browser-Sitzungen in einem geschützten Container isoliert werden.

Mit Proofpoint CASB gewinnen Sie zudem schnell einen Überblick über verdächtige Dateiaktivitäten und können vor allem verdächtige Anmeldungen erkennen. Ihr Sicherheitsteam kann sofort erkennen, ob Dateiaktivitäten von Angreifern oder von Anwendern stammen und somit umgehend reagieren.

Abgesehen vom Schutz vertraulicher Daten in Cloud-Anwendungen kann Proofpoint ebenso verhindern, dass vertrauliche Inhalte über Command-and-Control-Verbindungen exfiltriert, auf nicht verwaltete (dem Angreifer gehörende) Geräte heruntergeladen und über E-Mails verschickt werden.

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter **proofpoint.com/de**.

'INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter mehr als die Hälfte der Fortune-1000-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter **www.proofpoint.de**.

proofpoint.

0203-004-01-03 12/21