SOPHOS

ENDPOINT PROTECTION BEST PRACTICES ZUR ABWEHR VON RANSOMWARE

Sophos-Whitepaper Juli 2020

Endpoint Protection Best Practices zur Abwehr von Ransomware

Wir haben 5.000 IT-Manager in 26 Ländern befragt: 51 % gaben an, dass sie im letzten Jahr von Ransomware betroffen waren. Bei 73 % dieser Vorfälle gelang es Angreifern, Daten zu verschlüsseln. Zudem betrugen die durchschnittlichen Kosten für die Behebung der Folgen dieser Angriffe weltweit stolze 761.106 USD.

Um sich effektiv vor Ransomware-Angriffen zu schützen, benötigen Sie eine korrekt konfigurierte Endpoint-Protection-Lösung. In diesem Whitepaper erfahren Sie, wie Ransomware-Angriffe ablaufen, wie sie abgewehrt werden können und wie Sie sich durch die korrekte Konfiguration Ihrer Endpoint-Lösung optimal vor solchen Angriffen schützen.

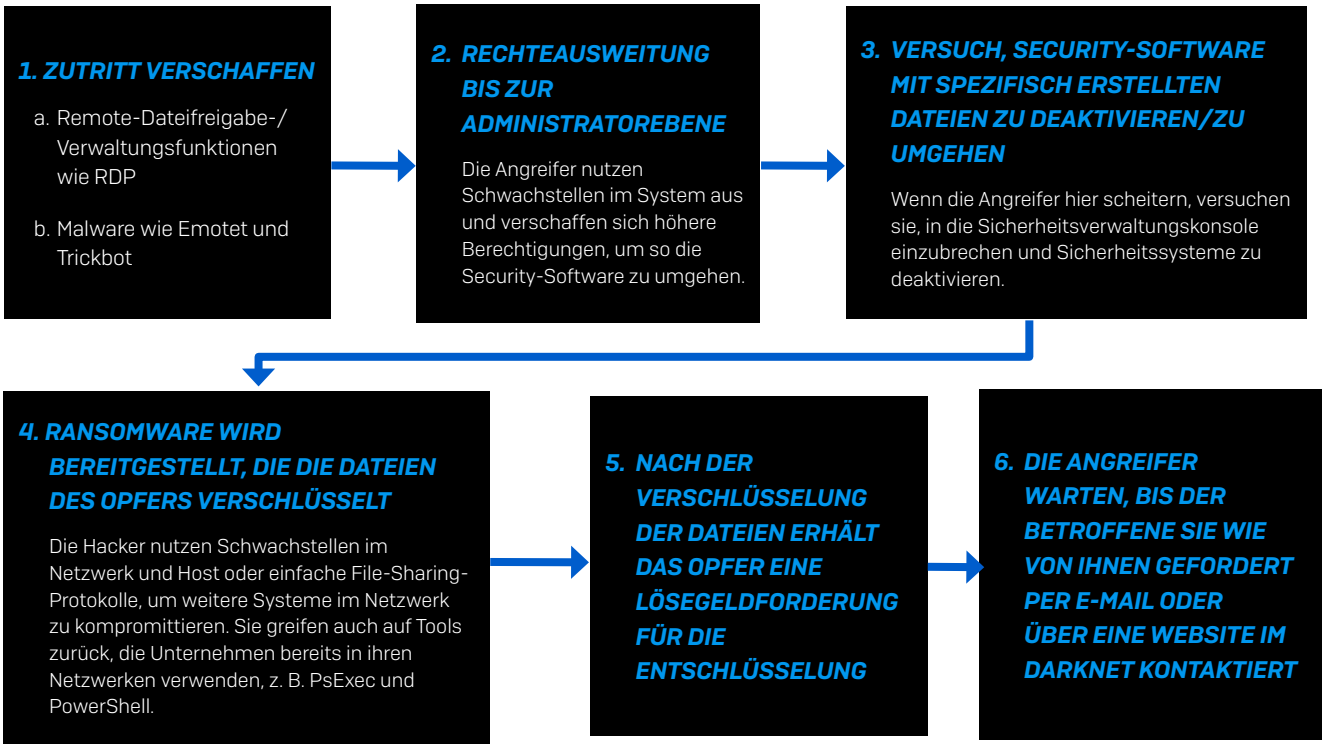
Wie Ransomware-Angriffe ablaufen

In den letzten Jahren konnten wir einen neuen Trend bei Ransomware beobachten, weg von groß angelegten Brute-Force-Angriffen hin zu gezielten, sorgfältig geplanten, manuell durchgeführten Angriffen, die sich wesentlich schwerer erkennen und abwehren lassen. Im Folgenden sehen wir uns die Vorgehensweise verschiedener Formen von Ransomware an und zeigen, was Ihr Unternehmen tun kann, um die Anfälligkeit für einen Angriff zu minimieren.

Gezielte Ransomware-Angriffe

Gezielte Ransomware-Angriffe erfordern viel manuelle Arbeit: In der Regel konzentrieren sich die Angreifer auf ein konkretes Opfer pro Angriff und stellen an dieses horrende Lösegeldforderungen. Sie verschaffen sich Zugriff auf das Netzwerk, bewegen sich lateral fort und identifizieren dabei wichtige Systeme. Um auf möglichst vielen Systemen Fuß zu fassen, schlagen die Angreifer gerne dann zu, wenn die Verteidiger unter Umständen nicht zu 100 % wachsam sind: nachts, an Wochenenden oder an Feiertagen. Um mehrschichtige Schutzfunktionen zu umgehen und maximalen Schaden anzurichten, greifen sie auf eine ganze Reihe von Angriffstechniken zurück.

Typischer Ablauf eines gezielten Ransomware-Angriffs:



Die Folgen dieser Angriffe sind meist schwerwiegend. Hacker werden immer dreister und fordern bisweilen sechsstellige Summen. Außerdem ergab unsere Befragung, dass die Begleichung des Lösegelds die Kosten für die Angriffsbeseitigung in der Regel verdoppelt – im Durchschnitt müssen Unternehmen weltweit 1,4 Mio. USD begleichen.

Bereitstellung von Ransomware über RDP

Desktop-Sharing-Tools wie RDP (Remote Desktop Protocol) und VNC (Virtual Network Computing) sind harmlose und sehr praktische Tools, mit denen Administratoren remote auf Systeme zugreifen und diese verwalten können. Ohne ausreichenden Schutz bieten diese Tools allerdings eine willkommene Schwachstelle, die häufig für gezielte Ransomware-Angriffe genutzt wird.

Sorgen Sie deshalb dafür, dass RDP und ähnliche Remote-Management-Protokolle hinter einem VPN (Virtual Private Network) ausreichend geschützt sind, oder legen Sie zumindest fest, welche IP-Adressen per RDP zugreifen dürfen – sonst stehen Angreifern alle Türen offen. Denn viele Angreifer nutzen Brute-Force-Hacking-Tools, die Hunderttausende Kombinationen aus Benutzername und Passwort ausprobieren, bis sie sich erfolgreich Zugriff verschaffen und Ihr Netzwerk kompromittieren.

Allgemeine Best Practices zum Schutz vor Ransomware

Um vor Ransomware geschützt zu bleiben, benötigen Sie nicht nur die neuesten Sicherheitslösungen. Auch IT Security Best Practices wie regelmäßige Mitarbeiterschulungen sind unerlässlich. Befolgen Sie unbedingt die folgenden 10 Best Practices:

1. Installieren Sie Patches zeitig und regelmäßig

Malware nutzt häufig Sicherheitslücken in beliebten Anwendungen aus. Je früher Sie Ihre Endpoints, Server, Mobilgeräte und Anwendungen patchen, desto weniger Lücken können ausgenutzt werden.

2. Fertigen Sie regelmäßig Back-ups an und verwahren Sie diese offline und außerhalb des Büros

In unserer Befragung konnten 56 % der IT-Manager ihre verschlüsselten Daten mithilfe von Back-ups wiederherstellen. Verschlüsseln Sie Ihre Back-up-Daten und verwahren Sie diese offline und außerhalb des Büros, sodass Sie nicht über Cloud-Back-ups oder Speichergeräte in die falschen Hände geraten können. Außerdem sollten Sie einen Wiederherstellungsplan für den Notfall vorsehen.

3. Aktivieren Sie Dateierweiterungen

Dateierweiterungen sind in Windows standardmäßig deaktiviert und nur über die Dateiminiaturansicht ersichtlich. Bei aktivierten Dateierweiterungen können Sie Dateitypen, die normalerweise nicht an Sie und Ihre Benutzer gesendet werden (z. B. JavaScript-Dateien), einfach erkennen.

4. Öffnen Sie JavaScript (.JS)-Dateien in Notepad

Wenn Sie eine JavaScript-Datei in Notepad öffnen, können keine Schad-Skripte ausgeführt werden und Sie können den Inhalt der Datei überprüfen.

5. Aktivieren Sie keine Makros in Dokumentanhängen, die Sie per E-Mail erhalten

Microsoft hat die automatische Ausführung von Makros schon vor Jahren aus Sicherheitsgründen deaktiviert. Viele Infektionen funktionieren nur, wenn Sie Makros aktivieren. Aktivieren Sie also keine Makros!

6. Vorsicht bei Anhängen, die Ihnen unaufgefordert zugesendet werden

Cyberkriminelle verlassen sich oft auf ein uraltes Dilemma: Benutzer wissen, dass sie ein Dokument erst öffnen sollten, wenn sie sicher sind, dass es unbedenklich ist. Aber um festzustellen, ob das Dokument unbedenklich ist, müssen sie es öffnen. Lassen Sie im Zweifel lieber die Finger von einem Anhang, der Ihnen verdächtig erscheint.

7. Überwachen Sie Administrator-Rechte

Überprüfen Sie kontinuierlich die lokalen und Domain-Administrator-Rechte. Behalten Sie im Auge, wer Administrator-Rechte hat, und entziehen Sie die Rechte ggf., wenn sie nicht benötigt werden. Bleiben Sie nur so lange wie wirklich nötig mit Administrator-Rechten angemeldet und vermeiden Sie in diesem Zeitraum Surfen, das Öffnen von Dokumenten und andere reguläre Arbeitsschritte.

8. Halten Sie die Sicherheitsfunktionen in Ihren Geschäftsanwendungen aktuell

In Office gibt es mittlerweile das Steuerelement „Ausführung von Makros in Office-Dateien aus dem Internet blockieren", mit dem Sie sich vor externen Schadinhalten schützen und Makros intern weiterhin nutzen können.

9. Kontrollieren Sie den externen Netzwerkzugriff

Lassen Sie Ports nicht für jeden geöffnet. Sperren Sie den RDP-Zugriff Ihres Unternehmens und andere Remote-Management-Protokolle. Verwenden Sie außerdem eine Zwei-Faktor-Authentifizierung, und stellen Sie sicher, dass sich Remote-Benutzer bei einem VPN authentifizieren.

10. Verwenden Sie sichere Passwörter

Über ein schwaches und leicht zu erratendes Passwort können sich Hacker in Sekundenschnelle Zugriff auf Ihr gesamtes Netzwerk verschaffen. Wir empfehlen daher komplexe Passwörter ohne Bezug auf Ihre Person mit mindestens 12 Zeichen und einer Mischung aus Groß-und Kleinschreibung sowie zufälligen Satzzeichen (Bsp.: Ju5t.LiKETh1s!).

Best Practices für Ihre Endpoint-Protection-Lösung

Neben einer Next-Gen Firewall ist der Einsatz einer Endpoint-Protection-Lösung eine der effektivsten Methoden zum Schutz vor Ransomware-Angriffen. Diese muss jedoch korrekt konfiguriert sein, um optimalen Schutz zu bieten.

Befolgen Sie diese Best Practices, um Ihre Endpoints vor Ransomware zu schützen:

1. Aktivieren Sie alle Richtlinien und stellen Sie sicher, dass alle Funktionen eingeschaltet sind

Es mag offensichtlich klingen, aber tatsächlich ist dies die effektivste Methode, um den Schutz Ihrer Endpoint-Lösung optimal zu nutzen. Richtlinien sind dazu da, bestimmte Bedrohungen zu stoppen. Deshalb sollten Sie regelmäßig überprüfen, ob Ihre Richtlinien auch wirklich aktiviert sind. So stellen Sie sicher, dass Ihre Endpoints optimal geschützt bleiben – vor allem vor neueren Ransomware-Stämmen.

Darüber hinaus ist das Einschalten von Funktionen, die dateilose Angriffstechniken und Ransomware-Verhalten erkennen, entscheidend, um zu verhindern, dass Kriminelle Ihre Endpoints infiltrieren und schädliche Ransomware-Stämme einschleusen. Außerdem können Sie mit diesen Funktionen Angriffe auch einfacher beheben, wenn Ihre Umgebung doch einmal kompromittiert werden sollte.

2. Überprüfen Sie regelmäßig Ihre Ausschlüsse

Mit Ausschlüssen können vertrauenswürdige Verzeichnisse und Dateitypen von den Malware-Scans ausgenommen werden. Sie werden manchmal genutzt, um Beschwerden von Benutzern abzumildern, die der Meinung sind, dass die Schutzlösung ihre Systeme verlangsamt. Ausschlüsse können auch verwendet werden, um das Risiko möglicher Fehlalarme zu verringern.

Im Laufe der Zeit kann eine wachsende Liste ausgeschlossener Verzeichnisse und Dateitypen jedoch immer mehr Benutzer im Netzwerk betreffen. Und Malware, die es schafft, in ausgeschlossene Verzeichnisse zu gelangen – vielleicht versehentlich von einem Benutzer verschoben – wird wahrscheinlich erfolgreich sein, weil sie von der Überprüfung ausgeschlossen ist.

Überprüfen Sie Ihre Ausschlussliste regelmäßig in Ihren Bedrohungsschutz-Einstellungen und beschränken Sie die Anzahl der Ausschlüsse auf ein Minimum.

3. Aktivieren Sie mehrstufige Authentifizierung (MFA) in Ihrer Sicherheitskonsole

Eine mehrstufige Authentifizierung, kurz MFA, bietet eine zusätzliche Schutzebene nach dem ersten Faktor, der oft ein Passwort ist. MFA für Ihre Anwendungen zu aktivieren, ist in der Regel eine gute IT-Sicherheitspraxis, und wird dringend für alle Benutzer empfohlen, die Zugriff auf Ihre Sicherheitskonsole haben.

Auf diese Weise machen Sie den Zugriff auf Ihre Endpoint-Protection-Lösung noch sicherer und verhindern, dass unbeabsichtigt oder absichtlich versucht wird, Ihre Einstellungen zu ändern, was Ihre Endpoints anfällig für Angriffe machen könnte. MFA ist auch für den Schutz von RDP von zentraler Bedeutung.

4. Stellen Sie sicher, dass jeder Endpoint geschützt und auf dem neuesten Stand ist

Überprüfen Sie kontinuierlich, ob Ihre Geräte geschützt und auf dem aktuellen Stand sind, um optimalen Schutz zu gewährleisten. Ein Gerät, das nicht richtig funktioniert, ist möglicherweise nicht geschützt und kann anfällig für Ransomware-Angriffe sein. Diese Telemetrie wird häufig von Endpoint-Security-Tools bereitgestellt. Außerdem nützlich ist ein Programm, mit dem sich überprüfen lässt, ob alle Sicherheitsvorgaben eingehalten werden, um regelmäßig nach potenziellen IT-Problemen zu suchen.

5. Setzen Sie Sicherheitsvorgaben durch

Überprüfen Sie regelmäßig, dass alle Sicherheitsvorgaben eingehalten werden. Dies ist wichtig, damit Ihre Endpoints und die darauf installierte Software effizient laufen.

Die Implementierung eines gezielten Programms für diese Überprüfung ist besonders wichtig für den Schutz vor Ransomware-Angriffen und anderen Cybersecurity-Bedrohungen. So können Sie beispielsweise sicherstellen, dass RDP nur dort ausgeführt wird, wo Sie es benötigen und erwarten. Außerdem können Sie so regelmäßige Überprüfungen auf Konfigurationsprobleme durchführen, die Geräteleistung überwachen und unerwünschte oder nicht benötigte Programme entfernen. Im Rahmen einer solchen Überprüfung können Sie ermitteln, ob Software-Anwendungen, einschließlich Ihrer Security-Software, aktualisiert werden müssen. Außerdem können Sie so auch sicherstellen, dass regelmäßig Back-ups wertvoller Daten erstellt werden.

6. Suchen Sie nach aktiven Angreifern in Ihrem Netzwerk

Cyberkriminelle sind heute raffinierter denn je und setzen bei ihren Ransomware-Angriffen auf hinterlistige Verfahren. Unternehmen benötigen Tools, mit denen sie detaillierte Fragen stellen können, um komplexe Bedrohungen und aktive Angreifer zu erkennen. Sobald Bedrohungen und Angreifer aufgespürt wurden, benötigen Unternehmen auch Tools, mit denen sie schnell geeignete Gegenmaßnahmen ergreifen können.

Technologien innerhalb Ihrer Endpoint-Lösung wie EDR (Endpoint Detection and Response) bieten diese Funktionalität. Aktivieren Sie daher EDR-Funktionen, sofern diese vorhanden sind.

7. Schließen Sie Sicherheitslücken mit Hilfe von Experten

Ransomware ist für Hacker nur das „Finale" einer langen Kette von Aktionen. Um Ransomware bereitzustellen, sind Hacker bereits in Ihr Netzwerk eingedrungen und haben möglicherweise ohne Ihr Wissen Daten abgeschöpft – manchmal sogar Monate vor dem eigentlichen Angriff.

Technologien allein reichen oft nicht aus, um diese Eindringlinge zu stoppen. Ein einfacher Vergleich als Beispiel: Mit einer Überwachungskamera können Sie sehen, wie Diebe in Ihre vier Wände gelangen, aber nur mit Sicherheitspersonal können Sie einen Diebstahl verhindern. Dieses Prinzip gilt auch für die Cybersecurity. Die beste Methode, um sich wirklich effektiv vor diesen Eindringversuchen zu schützen, besteht darin, Ihre mehrschichtige Sicherheit um menschliche Expertise zu erweitern.

Managed Detection and Response(MDR)-Services spielen hier eine entscheidende Rolle. Durch die Kombination Ihrer internen IT- und Security-Teams mit einem externen Bedrohungsexperten-Team lassen sich Bedrohungen wesentlich schneller und effektiver bekämpfen.

Sophos Intercept X Advanced with EDR

Mit Sophos Intercept X Advanced mit EDR erhalten Sie alle Funktionen, die Sie benötigen, um Ihr Unternehmen vor Ransomware-Angriffen zu schützen.

Mit der Anti-Ransomware-Technologie von Intercept X erkennen Sie schädliche Verschlüsselungsprozesse und stoppen diese, bevor sie sich im Netzwerk ausbreiten können. Anti-Exploit-Technologien stoppen die Bereitstellung und Installation von Ransomware, Deep Learning blockiert die Ausführung von Ransomware, und CryptoGuard verhindert unbefugte Datei-Verschlüsselungen bzw. setzt betroffene Dateien in ihren sicheren Ursprungszustand zurück.

Außerdem trägt Sophos EDR dazu bei, dass Ihre Threat-Hunting-Aktivitäten und IT Operations in Ihrer gesamten Umgebung reibungslos funktionieren. Mit Sophos EDR kann Ihr Team detaillierte Fragen stellen, um komplexe Bedrohungen, aktive Angreifer und potenzielle IT-Schwachstellen zu identifizieren und anschließend schnell geeignete Gegenmaßnahmen zu ergreifen. So können Sie Angreifer in Ihrem Netzwerk aufspüren, die sich bislang unauffällig verhalten haben, aber nur auf eine gute Gelegenheit warten, um Ransomware zu installieren.

Sophos Managed Threat Response (MTR)

Mit dem 24/7 MDR-Service Sophos Managed Threat Response ergänzen Sie Ihre mehrschichtige Sicherheitsstrategie um menschliche Expertise. Ein Expertenteam sucht in Ihrem Auftrag proaktiv nach potenziellen Bedrohungen und überprüft diese. Bei entsprechender Genehmigung durch den Auftraggeber ergreifen die Experten Maßnahmen, um Bedrohungen auszuschalten, einzudämmen und unschädlich zu machen, und geben konkrete Ratschläge, um die Ursache wiederholt auftretender Vorfälle zu bekämpfen.

Fazit

Obwohl Ransomware inzwischen in die Jahre gekommen ist, werden wir wohl auch in Zukunft nicht von neuen Varianten verschont bleiben. Vielleicht werden wir Ransomware nie vollständig eliminieren können. Wenn Ihr Unternehmen jedoch die in diesem Dokument beschriebenen Best Practices für den Endpoint-Schutz einhält, stehen Ihre Chancen gut, dass Sie vor neuesten Bedrohungen geschützt bleiben.

Zusammenfassung:

1. Aktivieren Sie alle Richtlinien und stellen Sie sicher, dass alle Funktionen eingeschaltet sind
2. Überprüfen Sie regelmäßig Ihre Ausschlüsse
3. Aktivieren Sie MFA in Ihrer Sicherheitskonsole
4. Stellen Sie sicher, dass jeder Endpoint geschützt und auf dem neuesten Stand ist
5. Setzen Sie Sicherheitsvorgaben durch
6. Suchen Sie nach aktiven Angreifern in Ihrem Netzwerk
7. Schließen Sie Sicherheitslücken mit Hilfe von Experten

Testen Sie Sophos Intercept X kostenlos unter www.sophos.de/endpoint

Weitere Informationen über Sophos MTR finden Sie unter www.sophos.de/MTR

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

200702 WPDE (NP)

SOPHOS