10 Anzeichen dafür, dass Ihr Endpunktschutz veraltet ist und Sie ein Upgrade brauchen

Die anhaltende Zunahme gefährlicher Cyberangriffe zeigt, dass gängige Schutzmaßnahmen nicht mit den modernen Bedrohungen Schritt halten. Wie steht es um Ihr Unternehmen? Ist es umfassend geschützt? Anhand der folgenden zehn Warnsignale können Sie feststellen, ob Ihre aktuelle Endpunktsicherheit noch ausreichend ist.

BlackBerry.
Intelligent Security. Everywhere.

1. Sie verwenden nach wie vor signaturbasierte Sicherheitsprodukte.

Bis vor Kurzem konnte neue Malware noch von einzelnen Unternehmen erkannt, katalogisiert und blockiert werden. Anhand des einzigartigen Datei-Hash, auch bekannt als Signatur, konnten schädliche Dateien identifiziert und an der Ausführung gehindert werden. Aktuell hingegen veröffentlichen Angreifer pro Tag etwa 1.200 neue Malware-Varianten.[1] Allein die schiere Anzahl dieser Bedrohungen reduziert die Wirksamkeit eines signaturbasierten Sicherheitsansatzes erheblich.

2. Ihre mobilen Geräte sind angreifbar.

Die Hacker haben sich schnell auf den Trend zur Mobilität eingestellt. Mobile Geräte werden gerade zum Hauptziel von Phishing-Angriffen. Bis zu 83 % davon finden über Textnachrichten oder mobile Anwendungen[2] statt. Außerdem sind mobile Geräte heiße Kandidaten für Datenverluste, die wiederum zu Imageschäden, Gesetzesverstößen und Bußgeldern führen können.

3. Sie führen noch immer regelmäßig Systemprüfungen durch.

Herkömmliche Antivirensoftware (AV) ist auf ressourcenintensive Systemprüfungen angewiesen, um Malware zu entdecken. Zwar können Sie diese Scans planen, auf Anforderung oder nach Signatur-Updates durchführen, doch sind die negativen Auswirkungen auf die Systemleistung unbestreitbar.[3] Wenn Ihre Sicherheitslösung nach wie vor Systemüberprüfungen braucht, ist es Zeit für ein Upgrade.

Jeden Tag werden 450.000 neue Malware-Varianten und potenziell schädliche Anwendungen entdeckt.[4]

4. Ihre neuen Rechner arbeiten sehr langsam.

Viele Unternehmen verwenden Sicherheitsmodelle, bei denen die neuen Lösungen auf den bestehenden aufbauen. Mit der Zeit belastet die Anhäufung der Sicherheitsebenen die Systemressourcen und reduziert die Performance erheblich.[5] Sind Ihre PCs sehr langsam, sollten Sie eine modernere Endpunktlösung in Betracht ziehen.

5. Sie verwenden für die Verwaltung Ihrer AV einen lokalen Server.

Wenn Sie Ihre Antivirensoftware nicht über die Cloud verwalten können, ist es womöglich Zeit für ein Update. Denken Sie daran, dass viele Lösungen eine ständige Internetverbindung benötigen, um effektiv zu sein. Achten Sie darauf, dass Ihre Antivirenprogramme auch dann funktionieren, wenn die Anwender offline sind.

6. Sie verschwenden zu viel Zeit mit der Verwaltung Ihrer Antivirenprogramme.

Jede Minute, die Sie und Ihr IT-Team mit der Verwaltung Ihrer AV verbringen, ist verlorene Zeit. Wenn Ihre aktuelle Lösung ein Zeitfresser ist, sollten Sie neue Optionen in Betracht ziehen. Nutzen Sie Ihre kostbare Zeit lieber für zukunftsweisende Strategie-Projekte, die den Schutz Ihres Unternehmens verbessern.

7. Sie verbringen zu viel Zeit damit, Fehlalarme abzuarbeiten.

Durch fortschreitende Sensitivität der Lösungen hat sich auch die Zahl der False Positives erhöht. Wenn verhaltensbasierte Identifizierung, Sandboxing, hostbasierte Intrusion Prevention und URL-/Reputationsfilterung zu viel Ihrer Zeit mit Fehlalarmen verschwenden, sollten Sie handeln.

8. Sie erkennen Lücken in Ihrem Endpunktschutz.

Mit Ihrer Lösung können Sie ältere Geräte gut schützen. Mobile Geräte, IoT- und eingebettete Systeme hingegen nicht. Wenn Sie Ihre aktuelle Lösung nicht oder nur begrenzt an neue Technologien und Trends anpassen können, sollten Sie zeitnah über einen zukunftsfähigen Schutz nachdenken.

9. Ihre Endpunktsicherheit arbeitet rein reaktiv.

Ihr Endpunktschutz beschränkt sich auf Reaktionsmaßnahmen, die nach einem erfolgreichen Angriff erfolgen? Wenn Ihre Endpunktlösung Zero-Day-Malware nicht erkennen kann und Ihnen keine präventiven Taktiken zur Verhinderung von Sicherheitsverletzungen anbietet, sollten Sie nach einer zeitgemäßen Lösung suchen.

10. Sie müssen Ihr Betriebssystem aktualisieren, damit es mit Ihrem Antivirenprogramm kompatibel ist.

Es ist nicht unüblich, dass aus technischen Gründen geschäftskritische Systeme an bestimmte Betriebssysteme gebunden sind und nicht aufgerüstet werden können. Entscheiden Sie sich daher für eine skalierbare, zukunftsfähige Sicherheitslösung, die auch auf älteren Systemen läuft. Dies spart Kosten und vereinfacht Ihren Security Stack.

BlackBerry.
Intelligent Security. Everywhere.

Wenn eines der genannten Warnsignale auf Ihr Endpunktkonzept zutrifft, ist es Zeit für eine neue, zukunftsweisende Lösung. BlackBerry® Protect bietet Ihnen einen umfassenden, präventiven Sicherheitsansatz, Threat Prevention und Schutz vor ausgefeilten Bedrohungen dank fortschrittlicher Cylance®-KI. Mehr dazu erfahren Sie unter www.blackberry.com/protect.

[1] Malware Statistics For 2020 And What To Expect, PixelPrivacy, 2020, https://pixelprivacy.com/vpn/guides/guide-malware-statistics-and-facts/

[2] Raphael, JR, „8 mobile security threats you should take seriously in 2020", CSO, 25. Feb. 2020, https://www.csoonline.com/article/3241727/8-mobile-security-threats-you-should-take-seriously-in-2020.html?page=2

[3] McDunnigan, Micah „Do Firewalls & Virus Programs Slow Down the Computer?", Houston Chronicle, 2018, smallbusiness.chron.com/firewalls-virus-programs-slow-down-computer-63186.html

[4] AV-TEST, Total Malware, 16. Jan. 2022, https://www.av-test.org/en/statistics/malware/

[5] Korolov, Maria „The dark side of layered security", CSO, 13. Nov. 2015, www.csoonline.com/article/3004856/data-protection/the-dark-side-of-layered-security.html

MKTG-20-0570 | 011512