CHECK POINT THREAT EXTRACTION

CHECK POINT THREAT EXTRACTION

Frei von Malware ohne Zeitverzögerung

Die Vorteile

- Präventiver Schutz vor bekannten und unbekannten Bedrohungen in E-Mail-Dokumenten oder Web-Downloads
- Bereitstellung Malware-freier Dokumente ohne Verzögerungen
- Flexibler Schutz für individuelle Anforderungen im Unternehmen

Die Funktionen

- Schutz für Microsoft Office- und PDF-Dokumente
- aktive Entfernung von schadhaften oder ausführbaren Inhalten in Dokumenten
- Konvertierung der rekonstruierten Dateien in das PDF-Format für maximale Sicherheit oder Erhaltung des Original-Formats – je nach Sicherheitsrichtlinie im Unternehmen
- Rekonstruktion der Dateien in rund einer Sekunde
- frei konfigurierbare Sicherheits-optionen
- Einfacher Zugriff auf die Original-Dateien (falls gewünscht)

[1] Check Point Security Report 2014

DIE IST-SITUATION

Dokumente stellen heute eines der größten Sicherheitsrisiken für Unternehmen dar. Im vergangenen Jahr haben 84 Prozent aller Unternehmen schadhafte Dokumente heruntergeladen.[1] Mitarbeiter müssen jedoch in verschiedensten Funktionen wie Personal, Einkauf, etc. regelmäßig Dokumente von Bewerbern, Kunden oder Anbietern öffnen, denn das ist Teil ihrer beruflichen Aufgabenstellung. Zudem müssen sie Dokumente aus dem Internet herunterladen, wenn sie beispielsweise Marktanalysen durchführen, sich über aktuelle Technologien und Produkte informieren oder neue Mitarbeiter suchen. Viele Angestellte denken dabei jedoch nicht über die Folgen nach, wenn sie diese Dokumente öffnen, und setzen ihre Unternehmen Risiken wie Bedrohungen, Trojanern oder darin eingebetteter Malware aus.

Unternehmen müssen Schutzmechanismen implementieren, um sich vor den Risiken, die durch schadhaften Code in Dokumenten entstehen, abzusichern. Der herkömmliche Ansatz, sich vor infizierten Dokumenten zu schützen, indem sie nach Malware suchen und diese abwehren, schafft jedoch keine ausreichende Sicherheit. Antivirus-Lösungen sind schnell, sie können jedoch nur bekannte Malware aufdecken – und dies schützt nicht vor Zero-Day-Malware-Infektionen. Zero-Day-Lösungen erkennen auch neue, bisher unbekannte Malware und Advanced Persistent Threats (APTs). Diese Ansätze erfordern jedoch Zeit und setzen das Netzwerk möglicherweise Risiken aus, sofern Sicherheitsvorfälle nicht unmittelbar entdeckt und blockiert werden. Ein neuer Ansatz ist notwendig, um die Bedrohungen adressieren und die Malware eliminieren zu können bevor diese bis zu den Mitarbeitern durchzudringen.

DIE LÖSUNG

Check Point Threat Extraction nutzt einen neuen Ansatz, um Malware, die in E-Mail-Dokumenten oder Web-Downloads enthalten ist, zu entfernen. Threat Extraction bietet vollständige Sicherheit, da möglicherweise schadhafte oder ausführbare Inhalte entfernt werden und ausschließlich Malware-freie Dokumente an die Mitarbeiter weitergeleitet werden – und das ohne zeitliche Verzögerungen.

Threat Extraction eliminiert Bedrohungen aus Microsoft Office- und PDF-Dokumenten, indem die Software schadhafte Inhalte wie Makros, eingebettete Objekte und Dateien oder externe Links entfernt. Mitarbeiter erhalten rekonstruierte Dokumente, die ausschließlich als sicher bestätigte Elemente enthalten.

Mit Threat Extraction können Unternehmen Malware-freie Dokumente ohne Zeitverzögerung bereitstellen.

DOKUMENTE FREI VON MALWARE

Regelmäßig genutzte Dokumente können riskante Inhalte bergen wie beispielsweise eingebundene Makros oder eingebettete Links, die dazu genutzt werden können, Computer und Netzwerke zu infizieren. Mit Check Point Threat Extraction werden die Bedrohungen eliminiert, indem die schädlichen Elemente entfernt und die Inhalte mit ausschließlich sicheren Bestandteilen rekonstruiert werden. So erhalten die Empfänger Malware-freie Dokumente.

BEREITSTELLUNG OHNE ZEITVERZÖGERUNGEN

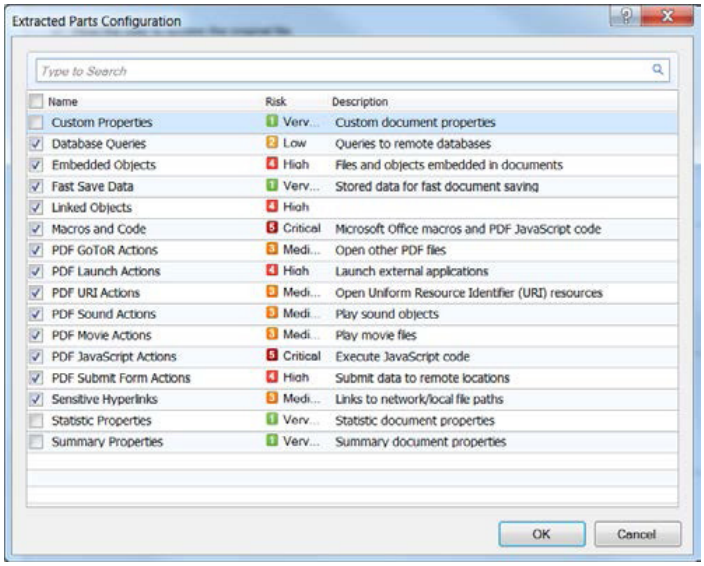
Im Gegensatz zu anderen Technologien für die Bedrohungserkennung, die Zeit für die Suche und Identifikation von Bedrohungen benötigen bevor sie diese blockieren können, eliminiert Threat Extraction alle Risiken präventiv und gewährleistet so die Bereitstellung sicherer Dokumente ohne Zeitverzögerungen.

SCHUTZ FÜR ALLE GÄNGIGEN DATEITYPEN

Check Point Threat Extraction unterstützt alle gängigen Dateitypen, die heute in Unternehmen genutzt werden. Dies umfasst Microsoft Office Word-, Excel-, Power Point- sowie Adobe PDF-Dokumente. Administratoren können auswählen, welche dieser Dateitypen sie mit Threat Extraction überprüfen möchten, wenn die Dateien per E-Mail oder über einen Web-Download in das Unternehmensnetzwerk gelangen.

FLEXIBLE OPTIONEN FÜR DIE SICHERHEIT

Threat Extraction bietet Unternehmen die Flexibilität, die Schutzoptionen für ein Dokument auszuwählen, die am besten für ihre betrieblichen Anforderungen geeignet sind. Um optimalen Schutz zu erzielen, empfiehlt Check Point, alle Dokumente zu rekonstruieren und in das PDF-Format zu konvertieren. Alternativ können Unternehmen auch das Original-Format des Dokuments erhalten und die Inhalte, die möglicherweise eine Bedrohung darstellen, entfernen. Diese Option ermöglicht es Administratoren, unterschiedliche Arten von Inhalten zu entfernen – seien es risikoreiche Makros, eingebettete Dateien oder externe Links.



EINFACHE BEREITSTELLUNG

Installiert als zusätzliches Software-Blade auf dem Gateway, ist Threat Extraction im Mail-Transfer-Agent-Modus in das E-Mail-Netzwerk integriert. Threat Extraction kann sowohl für das gesamte Unternehmen als auch für einzelne Mitarbeiter, Domänen oder Abteilungen genutzt werden. Administratoren können – je nach Anforderung – einzelne User und Gruppen einbinden und so eine sehr granulare Konfiguration für das Unternehmen vornehmen.

SYNCHRONISIERT MIT THREAT EMULATION

Threat Extraction und Threat Emulation bieten im Zusammenspiel noch besseren Schutz. Threat Extraction liefert Malware-freie Dokumente ohne Zeitverzögerung. Threat Emulation analysiert das Original-Dokument in einem isolierten Bereich, der sogenannten “Sandbox”, um so unbekannte Bedrohungen zu erkennen. Threat Emulation führt eine Analyse durch und schafft so Transparenz über alle Bedrohungen und Attacken.

Threat Extraction lässt sich auf zwei Arten konfigurieren: Threat Extraction leitet das rekonstruierte Dokument entweder unmittelbar an den Empfänger weiter oder wartet auf die Rückmeldung von Threat Emulation bevor entschieden wird, ob das Dokument rekonstruiert werden soll oder nicht. Zudem wird der Zugriff auf die Original-Datei nur erlaubt, wenn Threat Emulation diese als Schadcode-frei erklärt.

BUNDLES FÜR DEN OPTIMALEN SCHUTZ

Mit NGTX können Unternehmen sowohl die Schutzmechanismen von Threat Extraction nutzen als auch von zusätzlichen Funktionen wie IPS, Application Control, URL Filtering, Antivirus, Anti-Bot und Anti-Spam profitieren. Dieser umfassende Schutz bewahrt Mitarbeiter davor, schadhafte Dateien herunterzuladen, risikoreiche Websites zu besuchen oder Bots ausgesetzt zu werden – noch bevor ein Schaden entstehen kann.

TECHNISCHE SPEZIFIKATIONEN

Funktion	Beschreibung
Unterstützte Dateitypen	Microsoft Office 2003-2013, Adobe PDF
Bereitstellungsoptionen	• MTA – das Gateway empfängt alle eingehenden E-Mails und leitet diese nach der Überprüfung weiter • WebAPI – sendet die Dateien für die Rekonstruktion an die Engine • Web Browser Extension – unterstützt die Rekonstruktion von Download-Dateien
Leistung	Verringerung des Durchsatzes um ~1% pro 8.000 Mitarbeiter 1 GB Speicher erforderlich
Versionen und Betriebssysteme	ab R77.30 für die SecurePlatform oder GAiA