Schutz vor ausgefeilten E-Mail-Bedrohungen

Zahlreiche Cyberattacken beginnen per E-Mail. Mit einer integrierten Kombination von Antivirus/Antispam-E-Mail-Gateway und neuen Sandboxing-Technologien haben auch hochentwickelte Angriffsmethoden viel weniger Chancen.

Auch wenn für die geschäftliche Kommunikation vermehrt Instant Messaging zum Einsatz kommt: E-Mail ist und bleibt das meistgenutzte Kommunikationsmedium, vor allem für den Verkehr mit externen Kommunikationspartnern. Davon profitieren auch Cyberkriminelle, die mit immer ausgefeilteren und gezielteren Attacken operieren.

Die Fortinet-Appliances FortiMail und FortiSandbox maximieren die E-Mail-Security nachhaltig.

Advanced Threat Protection

Solche hochentwickelten Bedrohungen laufen oft in mehreren Schritten ab und beginnen fast immer mit dem Versand von E-Mails mit schadcodebehafteten Anhängen oder eingebetteten Links, die auch zu gefälschten oder mit Malware infizierten Websites führen. So funktionieren zum Beispiel die in den Schlagzeilen häufig vermeldeten «Ransomware»-Attacken, die dem Nutzer ein Lösegeld abverlangen, um die durch den Schadcode verschlüsselten Daten wieder zu entsperren. Typisch ist, dass diese Angriffe häufig durch kurzfristige Mutationen von klassischen Antivirus-Scan-Technologien nicht erkannt werden. Hier braucht es neue Ansätze, um auch noch unbekannten oder eben mutierten Schadcode sofort zu erkennen.

Neben einer Sensibilisierung der Mitarbeitenden – Stichwort: «keine verdächtigen Attachments öffnen» – ist demnach eine Sicherheitsinfrastruktur nötig, die auch unbekannte und komplexe Angriffsmethoden erkennt und Attacken zeitnah abwendet. Das beste Mittel dazu ist «Sandboxing»: Das Verhalten potenziell schädlicher Objekte wird als Erstes im Detail in einer virtuellen Umgebung untersucht. So lassen sich Systemänderungen, Exploitversuche, Verweise auf infizierte Websites, nachfolgende Downloads, Botnet-Kommunikationen und andere schädliche Aktivitäten erkennen. Falls die Analyse ergibt, dass schädliches Verhalten vorliegt, wird ein Fingerabdruck des Schädlings in Form eines Hashwerts des untersuchten Objekts gespeichert. So lässt sich die Bedrohung später ohne Verzögerung erneut identifizieren. Denn die Sandbox-Analyse ist aufwendig und kann pro Datei mehrere Minuten dauern.

FortiMail und FortiSandbox: die Highlights

- Integrierte Lösung mit Mail-Gateway und Sandbox
- Erkennt und neutralisiert bekannte und unbekannte Bedrohungen
- Hohe Schutzrate, hohe Effizienz
- Flexible Deployment-Optionen
- Keine Kosten pro User oder pro Mailbox
- Sandbox auch mit Firewalls und Client-Schutz von Fortinet integrierbar

Mail-Gateway und Sandbox im Verbund

Den besten und effizientesten Schutz vor E-Mail-basierten Bedrohungen, der zudem technisch elegant umsetzbar ist, bietet eine integrierte Lösung mit einem E-Mail-Gateway und einer Sandbox wie im Fall von FortiMail und FortiSandbox: Der E-Mail-Gateway FortiMail untersucht jede eingehende Meldung mit verschiedenen Filtermechanismen wie Antispam und Antivirus auf bekannte Malware. Durch den Einsatz eines vollwertigen Mail Gateways wird die Mailserver-Kommunikation entschlüsselt, sodass auch verschlüsselte E-Mail-Transport-Kommunikation analysiert werden kann. Erkannte Schädlinge stellt der Gateway unter Quarantäne und verhindert somit das Ausliefern solcher E-Mails an den Empfänger. Alle weiteren potenziell schädlichen Inhalte werden an die Sandbox übergeben. Erst wenn von dort grünes Licht kommt, gelangt das E-Mail zum unternehmensinternen Mail-Server. FortiSandbox übergibt zudem die Hash-Signaturen der neu als schädlich erkannten Objekte an das weltweite FortiGuard Threat-Protection-Netzwerk, worüber innert sehr kurzer Zeit auch andere Kunden von dem hochaktuellen Schadcodeschutz profitieren. FortiSandbox erkannte in unabhängigen Tests von NSS Labs 97,3% der Sicherheitsverletzungen, dank der mehrschichtigen Sandbox-Analyse von Fortinet überwiegend innerhalb von einer Minute.

FortiMail ist als Hardware-Appliance in sieben Leistungsstufen für Organisationen aller Grössen oder als virtuelle Appliance erhältlich. FortiSandbox gibt es in zwei Modellen, die 8 beziehungsweise 28 virtuelle Umgebungen parallel bewältigen und sich von Leistung und Kosten her vornehmlich für grössere Unternehmen eignen. Die für die Analyse benötigten Windows- und Office-Lizenzen sind im Lieferumfang enthalten. Auch FortiSandbox ist optional als virtuelle Appliance für 4 bis 54 virtuelle Umgebungen verfügbar. KMU können die Sandbox-Funktionalität als Cloud-Service direkt vom FortiMail-Gateway aus nutzen.

Kontakt

BOLL
IT Security Distribution

BOLL Engineering AG
Jurastrasse 58, 5430 Wettingen
Telefon 056 437 60 60
info@boll.ch
www.boll.ch