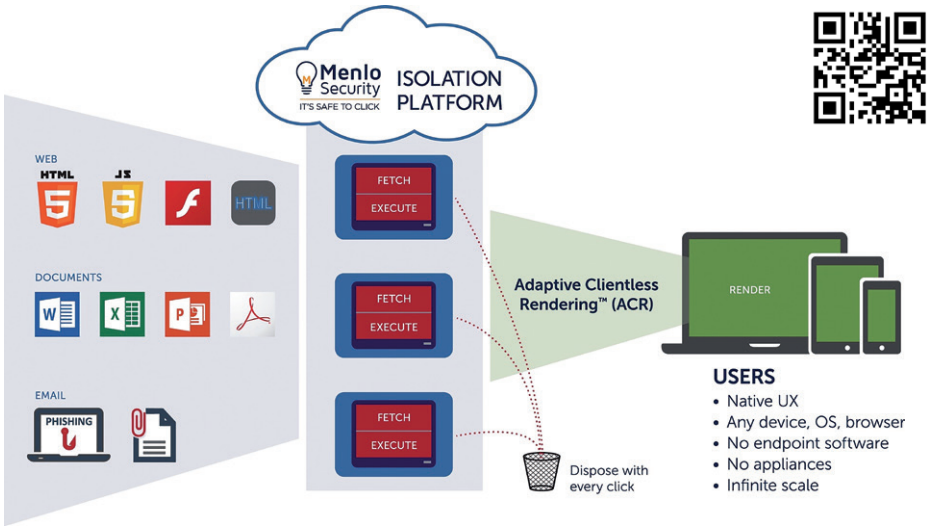
Null Prozent Malware durch Isolation

Der wachsenden Cyber-Bedrohungen Herr zu werden wird immer schwieriger. Ein neuer technischer Ansatz sorgt dafür, dass Schadcode und Phishing-Angriffe den Anwender überhaupt nicht mehr erreichen: Browser-, Dokumenten- und E-Mail-Isolation über eine zentrale Plattform.

Das Cybercrime-Problem nimmt rasant zu, wie der KPMG-Report «Clarity on Cyber Security» im Mai 2017 festhält: Demnach erlitten in den vergangenen 12 Monaten 88 Prozent der befragten Schweizer Unternehmen eine Cyber-Attacke – im Jahr davor waren es erst 54 Prozent. Bisher unbekannte Bedrohungen und unbekannte Schwachstellen spielen dabei zunehmend die Hauptrolle. Die wichtigsten Angriffsvektoren sind Websites mit eingebettetem Schadcode und «bewaffnete» Office- oder PDF-Dokumente sowie Phishing-E-Mails. Schädliche Webinhalte und Phishing machen rund 85 Prozent der Cyber-Risiken aus.

Konventionelle Lösungen zur Abwehr von Cyber-Attacken basieren oft auf der Erkennung bekannter Malware-Signaturen (Detection) und daraus abgeleiteter Merkmale. Bedrohungen, die mit neuen Mechanismen arbeiten, werden so nicht abgefangen. Eine andere Methode ist die Kontrolle aller eingehenden Inhalte durch Ausführung des potenziellen Schadcodes in einer geschützten Umgebung (Sandboxing) – ein rechen- und zeitaufwendiger Vorgang, der vom Prinzip her zudem ebenfalls mit der Erkennung von Schadcode arbeitet.



Die Menlo Security Isolation Platform sorgt dafür, dass Schadsoftware gar nicht zum Anwender gelangt.

Menlo Security Isolation Platform: die Highlights

- Vollständige Isolation der Anwender von jeglicher Malware
- Agentless: keine Software auf dem Client nötig
- Eliminiert Schadcode in JavaScript-, Flash- und Java-Inhalten
- 100-prozentig sichere Isolation: auch Bilder und Fonts werden bereinigt
- Phishing-Schutz durch Read-only-E-Mails
- Schutz vor schädlicher Werbung (Malvertising) und Ransomware
- Erhältlich als Cloud-Service oder als virtuelle Appliance
- Lizenziert pro User und Jahr

Neuartiger Ansatz

Einen völlig neuartigen Weg geht der 2013 gegründete kalifornische Sicherheitsspezialist Menlo Security. Das Ziel ist, dass Schadsoftware erst gar nicht zum Anwender gelangt. Die Menlo Security Isolation Platform isoliert die eingehenden Inhalte (Websites, Dokumente, E-Mails) jeweils in einem Container, einer abgesicherten virtuellen Umgebung, und führt dort den allenfalls enthaltenen aktiven Code aus (JavaScript, Flash, Java). Handelt es sich um Malware, läuft sie innerhalb des Containers und kann keinen Schaden anrichten – der Container wird unmittelbar danach entsorgt.

Der unschädliche Nutzinhalt wird auf Basis des «Document Object Models» (DOM) von HTML als gerenderte Information (Adaptive Clientless Rendering) ohne aktive Elemente an den Anwender übermittelt. So ist gewährleistet, dass der Client von jeglichem Schadcode isoliert ist. Die eigentliche Browser-Verarbeitung findet auf der Isolation Platform statt. Analoges gilt für E-Mails und Dokumente. Auf dem Endgerät muss dazu keine Software installiert werden. Einzig die Definition eines Proxy-Servers ist nötig. Der Anwender arbeitet wie gewohnt mit seinem Browser, der Office-Suite, dem PDF-Reader und dem E-Mail-Client.

Sicherheit ohne Erkennung

Gleichzeitig entfällt die fehleranfällige Analyse, ob es sich um «gute» oder «böse» Inhalte handelt. Die Lösung von Menlo Security kommt ganz ohne Detection aus. Dies hat den Vorteil, dass die zahllosen Security-Alerts, wie sie bei Detection-basierten Lösungen gang und gäbe sind, völlig wegfallen. Das Sicherheitsteam wird entlastet. Auf Wunsch lässt sich die Isolation Platform aber auch mit einem konventionellen Malware-Schutz kombinieren.

Ein weiterer positiver Nebeneffekt: Da der Client nur noch bereinigte Inhalte erhält, die von aktivem Code befreit sind, laden Websites merklich schneller. Der Quellcode der gerenderten Seite ist massiv schlanker als das Original und wird rascher übermittelt. Und der Browser muss keine Berechnungen mehr ausführen.

Weg von der Kloake

Menlo Security liegt mit seiner Lösung ganz auf der Linie von Gartner-Analyst Neil MacDonald: «Es ist Zeit, Ihre Nutzer durch Remote-Browsing von der Internet-Kloake zu isolieren.» Auf Basis der Isolation Platform bietet der Hersteller drei kombinierbare, aber auch einzeln nach Bedarf einzusetzende Dienste an: Web Isolation Service, Document Isolation Service und Phishing Isolation Service. Die Isolation Platform ist als Cloud-Service oder als virtuelle Appliance für den Betrieb vor Ort erhältlich.

Kontakt

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