Angriffsziel Browser: Gefahren vermeiden

Aktuelle Daten zeigen, dass 91% der Cyberangriffe über das Internet und/oder E-Mail erfolgen. Bei 40% der webbasierten Malware handelt es sich um Zero-Day-Bedrohungen, die nicht als schädlich bekannt sind und nicht durch signaturbasierte Scans erfasst werden. Deshalb ist es unverzichtbar, Anwender und Anwenderinnen vom Internet zu isolieren.

Browser sind echte Alleskönner. Neben der klassischen Internetnutzung haben sie sich weltweit als clientseitige Kommunikationsplattform etabliert. Aktive Inhalte sorgen für hohen Komfort und unterstützen dabei, verschiedenste Prozesse automatisiert auszulösen. Doch diese Durchdringung der Unternehmensprozesse birgt beträchtliche Sicherheitsrisiken, wie die Gefahr einer Endpunkt-Kompromittierung, oft in Verbindung mit Ransomware-Angriffen, der ungewollte Abfluss von Daten, die Speicherung sensibler Informationen im Cache oder die Offenlegung des Standorts als Angriffsvektor in das Firmennetzwerk. Deshalb sorgen präventive Konzepte für die Neutralisierung solcher Übertragungswege.

Attacken über das Internet

Programmierfehler in Webseiten sind so allgegenwärtig, dass Browser sie standardmäßig ignorieren, um das Benutzererlebnis nicht zu beeinträchtigen. Zugleich wird nicht bekannten Zertifizierungsstellen vertraut die wiederum anderen unbekannten Stellen vertrauen. Was technisch sinnvoll erscheint, sorgt sicherheitsseitig für ein Web-Ökosystem, das angreifbar ist.

Cyberangriffe über Browsersessions können auf verschiedene Weisen erfolgen. Bei Drive-by-Angriffen genügt das bloße Aufrufen einer Webseite, um über Schwachstellen im Browser und aktive Javascript-Unterstützung unbemerkt Schadcode einzuschleusen. Kommt der Code zur Ausführung, verfügt er über alle Rechte des jeweiligen Anwenders.

Ein wesentlicher Nutzungsaspekt des Browsers ist der Download verschiedenster Dateien. Sei es der schnell benötigte Gerätetreiber, die attraktiv erscheinende Freeware oder die gesuchte Musterlösung eines Problems, in den meisten Fällen ist die Datenquelle unbekannt. So ist weder die Integrität der Datei gesichert, noch ersichtlich, ob sie Schadcode enthält.

Webseiten können zur Preisgabe von Informationen (Phishing) verleiten und durch aktive Komponenten die Kontrolle über den Endpunkt mit Benutzerrechten übernehmen.
Der Schutz vor webbasierter Malware ist wichtig, jedoch sind Browser auch eine Schwachstelle beim Thema Daten-Exfiltration, dem unberechtigten Kopieren oder Übertragen schützenswerter Unternehmensdaten. Es ist einfach und ohne tiefreichende Kenntnisse möglich, interne Dateien auf Webspeicher, Social-Media Seiten und Hostingportale hochzuladen. Dabei ist es unerheblich, ob der Datenverlust versehentlich oder beabsichtigt zustande gekommen ist.

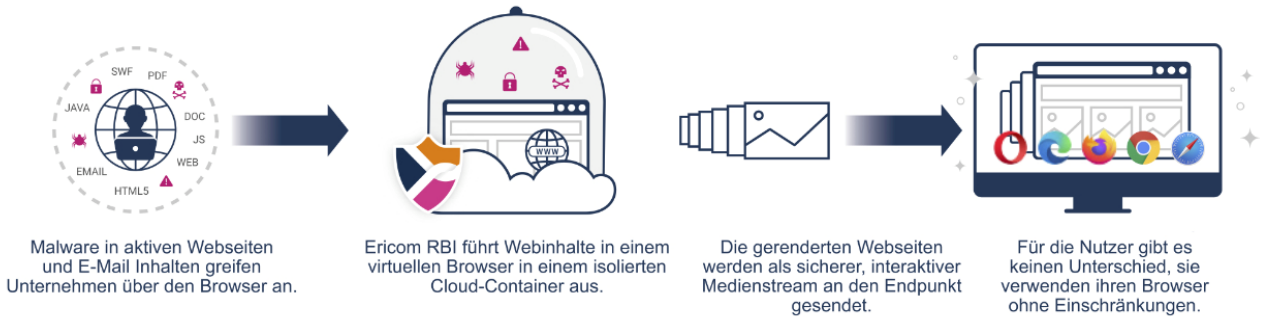
DNS-Negativliste genügt nicht

Ein Ansatz besteht darin, dass die Firewall per DNS-Negativliste den Zugang zu entsprechend kategorisierten Webseiten sperrt. Damit wird ein gewisses Schutzniveau erreicht, das aber lediglich auf Ja/Nein-Entscheidungen basiert. Dieses Verfahren hilft nicht, wenn vertrauenswürdige Webseiten ihrerseits kompromittiert wurden und zur Verteilung von Schadsoftware beitragen.
Die Kategorisierung von Webseiten wiederum ist vielschichtig und unterliegt einer hohen Dynamik. In der Praxis kann es durchaus gewollt sein, den Zugriff auf eine Webseite mit mittlerem Risikopotential zu ermöglichen (bei entsprechend wirksamen Schutzmaßnahmen), jedoch alle Webseiten mit hohem Gefährdungspotenzial zu blockieren.

Sicherheit durch Browser Isolation

Die international ausgezeichnete RBI-Lösung des israelischen Herstellers **Ericom Software** löst alle Anforderungen folgendermaßen:

- Jede Web-Session findet in einem vom Intranet isolierten Container in der Cloud statt. Die Anwender nutzen dafür weiterhin die im Unternehmen eingeführten Webbrowser. Diese werden lediglich um eine Proxy-Adresse und ein Sicherheitszertifikat erweitert.
- Jeder geöffnete Browser-Tab erzeugt einen eigenen Container, der nach Sitzungsende rückstandsfrei zerstört wird.
- Besuchte Webseiten haben keine Kenntnis der Nutzer-IP-Adresse. Übermittelt wird ausschließlich die IP des jeweiligen Cloud-Knotens (z. B. Frankfurt).
- Unabhängig von der Quellcodegröße der Originalseite, genügen wenige Zeilen HTML-Code für die Kommunikation zwischen Client und Container. Aktive Inhalte der besuchten Seiten erreichen den Endpoint nicht. Werbe-Blocker sorgen für eine fokussierte Internet Nutzung.
- Audio- und Bilddaten werden gerendert an den Browser des Nutzers übertragen. Zusätzlich ist ein Streaming-Modus für Webkonferenzen verfügbar. Als Pionier bei der Beschleunigung von Remoteübertragungen liefert Ericom ein hoch skalierbares, äußerst performantes System, das auch den Abruf von Videodaten problemlos unterstützt.
- Die Kategorisierung von URLs, Domänen und IP-Adressen, sowie deren Bewertung hinsichtlich des jeweiligen Risikopotentials (hoch, mittel, gering) ermöglicht Regelwerke für Webseiten, Multi-Domänen und Kategorien.
- Unter anderem sind Zugriffsbeschränkungen (Read-Only Modus), Clipboard-Restriktionen und Regeln für Up- und Downloads möglich. Dateitransfer kann erlaubt oder verboten werden -oder eine mehrstufige Überprüfung, inklusive einer leistungsfähigen CDR-Funktion, durchlaufen. Diese analysiert den Inhalt einer Datei und entfernt eventuell vorhandene Malware bevor die bereinigte Datei dem Client bereitstellt wird.



Fazit

Ericom Remote Browser Isolation schützt Ihre Endpunkte, Ihr LAN und Ihre Daten, ohne dass Sie dabei auf die Nutzung wichtiger Webservices verzichten müssen. Die Plattform vermeidet die lokale Installation und Administration von Hardware-Instanzen und bietet eine von der Anzahl Benutzer / Sessions unabhängige, konstante Nutzungsqualität. Durch die Verlagerung der Schutzmaßnahmen vom Endgerät in den isolierten Browser in der Cloud werden 100% der Malware-basierten Angriffe gestoppt, die über kritische Web- und E-Mail-Vektoren erfolgen.