GIRITECH®

Deutschland · Österreich · Schweiz

Geschützter Web Zugriff

Sichere Daten!

Der Browser gilt schlechthin als das Haupteinfallstor für Schadsoftware. Remote Browser Isolation (RBI) schützt den Endpunkt und damit die über ihn erreichbaren Instanzen.

Allerdings sollte die Betrachtung nicht nur auf potentielle Angriffe von aussen gerichtet sein. Das Risikopotential Datenexfiltration die durch die Möglichkeiten moderner Web Angebote und Browser Features zustande kommen kann, verdient hinreichende Aufmerksamkeit.

Schützen Sie Ihre Endpunkte und Ihre Daten

Im Zuge der digitalen Transformation speichern Organisationen, Unternehmen, Behörden, Bildungseinrichtungen etc. ihre sensibelsten Unternehmensdaten ausserhalb ihres Unternehmens-Netzwerks.

Und es ist nicht nur ein Cloud-basierter Ersatz für die Festplatten von einst. Jede SaaS-App oder jeder Remote-Service verfügt über wertvolle, geschäftskritische Unternehmensdaten, die vor noch nicht allzu langer Zeit auf Unternehmensservern innerhalb eines gesicherten Netzwerkperimeters geschützt gespeichert worden wären.

Wenn wir an Bedrohungen aus dem Internet denken, denken wir an Malware, Ransomware, Phishing, Diebstahl von Anmeldeinformationen und Downloads mit beinhalteter Schadsoftware. Dabei sind Benutzerfehler oft ein wesentliches Glied in der Kausalkette vieler Angriffe.

Völlig legitime und unerlässliche Benutzeraktivitäten können unter gewissen Umständen Unternehmen erheblichen Schaden zufügen. Business-Tools wie SaaS-Lösungen, Cloud-Speicher-Apps, Social-Media-Sites und Browserfunktionen die nachlässig oder böswillig verwendet werden, können zu Datenlecks, Datenverlusten und Datendiebstahl führen.

Mobile Work stellt IT-Sicherheitsteams vor echte Herausforderungen da Benutzer über eine Reihe von Geräten, Browsern und Netzwerken vom Büro, mobil und von zu Hause aus auf Webanwendungen zugreifen. Das Risiko des Datenverlusts ist real und stellt eine allgegenwärtige Gefahr dar, zumal ein Grossteil der Mitarbeiter über nicht verwaltete, persönliche Geräte auf entsprechende Webanwendungen zugreifen.

SaaS- und Webanwendungen bieten Systeme und Sicherheitsvorkehrungen zum Schutz der Kundendaten. Schließlich ist die Gewährleistung der Datensicherheit absolut erfolgskritisch. Trotz gelegentlicher Hacks ist die Wahrscheinlichkeit eines Datenverlusts innerhalb einer SaaS-App eher gering. Viel wahrscheinlicher ist es, dass an den Übergängen zwischen den Systemen Lecks auftreten.

Für die zunehmend digital agierenden Unternehmen entstehen solche Datenlecks über Webbrowser, Endgeräte und die Benutzer selbst. Lecks können durch böswillige Absichten, fahrlässige Offenlegung oder einfach durch begangene Fehler entstehen.

Secure Web Gateways schützen Benutzer vor bekannten Phishing-Sites. Da jedoch die meisten Phishing-Sites nur wenige Stunden aktiv sind, werden viele solcher Sites nie bekannt.
Bei Zero-Trust-Browsing hingegen wird beim Klicken auf einen Link die Ziel-Website auf einem vom Endpunkt isolierten Remote-Browser geöffnet. Ein schreibgeschützter Modus für nicht kategorisierte Websites schützt Benutzer und Organisationen vor ausgeklügelten Methoden zum Diebstahl von Anmeldeinformationen.

GIRITECH®
Deutschland · Österreich · Schweiz

Web-Apps, browserbasierter Zugriff und damit verbundene Risiken

Vier primäre Datenexfiltrationswege vor denen sich Unternehmen schützen müssen.

Datendiebstahl und Unternehmensspionage sind nur einen Klick entfernt, da vertrauliche Daten über den Browser ganz einfach auf persönliche Webspeicherkonten übertragen werden können.

Cloud-Speicherlösungen machen es Benutzern leicht, Bilder und Daten von jedem Gerät aus zu speichern. Benutzer können Unternehmensdaten durch ein einfaches Drag-and-Drop in ihrem eigenen, persönlichen Cloud-Speicher ablegen.

Für Benutzer die zu schnell die Auswahl „Tab schließen“ betätigen, sind Browser-Caches die Rettung. Ein erneutes öffnen des geschlossenen Tabs bringt verlorene Daten zurück.

Kommt das Device abhanden oder wird gehackt ist es jedoch problematisch, wenn vertrauliche Daten aus Web- oder Cloud-SaaS-Anwendungen noch im Cache des Devices sind. Umso mehr, wenn das Gerät nicht verwaltet wird und die IT keine Möglichkeit hat, Daten - einschließlich Webbrowserdaten – auf dem Device remote zu löschen.

Soziale Medien sind ein wichtiges Marketing Instrument und zur Imagepflege. Andererseits macht die Leichtigkeit des Veröffentlichens Social-Media-Kanäle auch riskant. Benutzer können vertrauliche Daten oder Bilder teilen, ohne zu berücksichtigen, dass die von ihnen geteilten Elemente nur für den internen Gebrauch bestimmt sind – oder deren Veröffentlichung sogar beabsichtigen.

Clevere Social-Engineering-Taktiken verleiten dazu Inhalte zu teilen, die für Angriffe auf ihre Organisationen verwendet werden könnten.

Kopieren ist einfach. Sei es der Ausdruck in eine PDF Datei, das schnelle kopieren der Bildschirmanzeige mittels einem einfachen [Strg]+[P] oder [Alt]+[Druck] Befehls oder die Übertragung von Dateiinhalten über das Clipboard.

Wertvolle Daten aus unternehmensinternen Web- und Cloud-Apps können so unbemerkt zum Schaden des Unternehmens exfiltriert werden.

Bis zur Offenlegung vertraulicher Informationen oder entsprechender Lösegeldforderungen ist es dann oft nur noch ein kleiner Schritt.

Ericom ZeroTrust Web Access verhindert Exfiltration

Der Schutz vor dem Hochladen vertraulicher oder proprietärer Daten in soziale Medien oder Cloud-Speicher via Browser ist eine Herausforderung. Es geht letztlich darum, den Upload „innerer“ Daten über das Internet nach außen zu verhindern.

Zero Trust Browsing schützt Benutzer vor unbekannten Bedrohungen, bösartigen Websites und vor allem vor schlimmen Auswirkungen unterlaufener Fehler.

Ericom ZeroTrust Web Access Shield ist eine fortschrittliche Remote-Browser-Isolationslösung, die Malware, Ransomware und andere Bedrohungen von den Endpunkten und vom Unternehmensnetz-werk fernhält.
Es sichert auf transparente Weise die Internetnutzung, „entschärft“ Phishing-Sites, sorgt für sichere Dateidownloads und reduziert Risiken, Kosten und Betriebsbelastung für das IT-Personal.

Zur Lösung dieser Aufgaben dienen:

- Richtlinienbasierte Einschränkungen für Browser-Druckfunktionen, Screenshots und Clipboard Unterstützung für alle oder ausgewählte Sites und/oder Benutzer

- Richtlinienbasierte Einschränkung von Datei-Uploads und Drag-and-Drop auf alle oder ausgewählte Websites für alle oder ausgewählte Benutzer

So kann beispielsweise eine öffentliche Verwaltung das Hochladen von Dateien auf Social-Media-Websites für die meisten Benutzer deaktivieren, während es der Unternehmenskommunikation erlaubt wird, Updates durch Uploads (z.B. Pressemeldungen) zu veröffentlichen.

Die Möglichkeit Inhalte hochzuladen kann auch auf nur bestimmte interne Verzeichnisse und zu explizit freigegebene Social-Media-Sites beschränkt werden. Der Ausdruck von Browser-Tabs kann beispielsweise nur für C-Level-Führungskräfte oder andere vertrauenswürdige Personen erlaubt sein.

Folgende Aspekte sollten bei der Beurteilung von RBI Lösungen betrachtet werden:

- Unterstützung vorhandener Browser Infrastruktur
- Ressourcenbedarf für die benötigte Anzahl Sessions / Tabs mit stabiler Nutzungsperformance
- Skalierbarkeit
- Richtlinienbasierende Data Loss Prevention Funktionen
- Integrationspotential (SIEM, SAML)
- Unterstützung von Web-Meeting Plattformen