100 Prozent sicher surfen dank Isolation

Isolation verspricht einen perfekten Schutz beim Umgang mit Web und E-Mail. Patrick Michel, Principal Consultant beim IT-Security-Distributor BOLL, erklärt, worum es bei diesem innovativen Sicherheitskonzept geht, was die Vorteile sind und welche Anbieter starke Isolationslösungen offerieren.

Was heisst Isolation im Zusammenhang mit Security?
Patrick Michel: Es geht darum, dass beim Zugriff aufs Web und beim Lesen von E-Mails kein Schadcode zum Anwender gelangt. Dazu läuft alles, was sonst im lokalen Browser ausgeführt wird, auf einer Isolationsplattform in einer hochsicheren Umgebung in Form eines virtuellen Containers, in dem ein Browser für den Anwender ausgeführt wird. Dadurch wird der allfällige Schadcode nicht auf dem Client ausgeführt, sondern in einem Isolations-Container. Es wird also gar nicht versucht, Schadcode zu erkennen. Dieser wird stattdessen komplett isoliert. Für das effektive Endgerät wird neuer und sauberer Code gerendert. Bei Dokumenten, die von den Usern heruntergeladen werden, ist die Vorgehensweise eine andere. Den Dokumenten werden gefährliche Script-Funktionen, die in den meisten Fällen ohnehin nicht benötigt werden, entzogen. Bei manchen Lösungen hat der Nutzer jedoch mittels Willensbekundung die Möglichkeit, das Originaldokument trotzdem zu laden.

Welche Bedeutung hat Isolation für die IT-Security?
Isolation bringt einen regelrechten Paradigmenwechsel mit sich. Statt zwischen Gut und Böse zu unterscheiden, wie es herkömmliche, auf Detection basierende Sicherheitslösungen tun, wird der Anwender zu 100 Prozent von sämtlichem potenziell gefährlichen Code isoliert. Der gesamte Web-Traffic sowie Links in E-Mails gehen über die Isolationsplattform. Man kann nach Herzenslust surfen, wohin man will – ohne Angst vor Schadcode. Kurz: Isolation ist ein sehr interessantes Technologiekonzept und adressiert die Schwäche von Detection-Produkten, beziehungsweise ergänzt diese.

Macht Isolation andere Sicherheitssoftware überflüssig?
Mit einer Isolationsplattform spielen URL-Filter aus dem Blickwinkel der Sicherheit keine Rolle mehr. Für andere Zwecke – wie etwa die Blockierung von Inhalten, die im Unternehmen aus anderen Gründen unerwünscht sind – ist Web Filtering natürlich weiterhin nützlich. Für den Benutzer-Web-Traffic stellt sich heute die Frage, wo dieser abgesichert werden soll. In klassischen Architekturen wird dies auf Firewalls oder Secure Web Gateways (Proxies) getan. Im Zeitalter von Cloud und Heimarbeitsplätzen vermehrt auch als Secure Access Service Edge (SASE) Service. Anbieter von Secure-Web- und Secure-E-Mail-Gateway-Lösungen haben damit begonnen, diese mit entsprechenden Isolation-Funktionen oder -Produkten zu ergänzen.

Patrick Michel, Principal Consultant, BOLL

Wie gelangen die «gesäuberten» Inhalte zum Anwender?
Hier gibt es zwei Varianten: Entweder wird die in der Isolationsplattform aufbereitete Website als reines HTML-/CSS-Dokument an den Browser geschickt – man spricht von Clientless Rendering. Dies ist sehr effizient und für die Nutzer völlig transparent; das heisst, die User merken gar nichts von der Isolation. Oder die Inhalte werden in einer Art Terminal Emulation als Pixelstream übermittelt, was aber mehr Ressourcen benötigt, mehr Traffic verursacht und Einbussen bei der Nutzerfreundlichkeit bringt. Manche Anbieter mischen die Ansätze auch. Dabei wird beispielsweise die Pixel-Methode als Fallback-Technologie eingesetzt, wenn die Rendering-Methode Probleme bei der Darstellung verursacht.

Wie steht es um den Reifegrad der Isolationstechnologie?
Es ist zwar ein vergleichsweise junges Konzept, aber die Technologie ist inzwischen erwachsen geworden. Isolation ist keine Nischentechnologie mehr und steht bei Unternehmen und Behörden produktiv im Einsatz. Dies auch in der Schweiz – so zum Beispiel bei Banken, Kernkraftwerken und anderen sicherheitsbewussten Organisationen. Die ursprünglichen Bedenken, dass es zu viele Probleme bei der Darstellung gerenderter Websites geben würde, haben sich nicht bestätigt.

Wer bietet Lösungen auf Basis Isolation an?
Der Pionier war und ist Menlo Security mit seiner Isolation Platform, die Web-Traffic und E-Mail zuverlässig schützt. Heute kommt das Konzept jedoch bei vielen Security-Herstellern zur Anwendung. So etwa bei Fortinet, Proofpoint und Symantec. Bei reinen Cloud-Anbietern wie Zscaler hat Isolation ebenfalls Einzug gehalten – die Technologie ist durch die Akquisition von Appsulate ins Zscaler-Portfolio gestossen. Wenn Branchengrössen innovative Start-ups aufkaufen und deren Technologien in ihre eigenen Lösungen integrieren, ist dies ein deutliches Indiz für die zunehmende Bedeutung einer Technologie.

Und wer hat Ihrer Meinung nach die beste Isolationsplattform?
Aus unserer Erfahrung bei BOLL ist dies ganz klar Menlo Security. Speziell wenn der gesamte Web-Traffic isoliert werden soll. Die Rendering-Technologie von Menlo hat sich in Tests als führend erwiesen. Der Markt spricht immer stärker auf die Isolation-Lösung von Menlo an. So hat das US-Verteidigungsministerium kürzlich einen 199-Millionen-Dollar-Vertrag mit einem Partner von Menlo abgeschlossen. Zudem erweitert Menlo Security sein Lösungsportfolio kontinuierlich. Dies stets auf Basis der Isolationsplattform als Kernelement.

BOLL
IT Security Distribution

BOLL Engineering AG

Jurastrasse 58
5430 Wettingen
Tel. 056 437 60 60

info@boll.ch
www.boll.ch