Advertorial

Maximale Sicherheit beim Surfen

Über die Menlo Isolation Platform können sich die Mitarbeitenden des Kernkraftwerks Gösgen sicher im Web bewegen.

Das Kernkraftwerk Gösgen schützt den Zugang zum World Wide Web durch Browser-Isolation auf höchstmöglichem Niveau. So ist garantiert, dass keinerlei Schadcode bis zu den Endgeräten der Mitarbeitenden vordringt.

In einem Kernkraftwerk ist eine ausserordentlich hohe Sicherheit der IT unabdingbar. Dies betrifft insbesondere auch die Nutzung des World Wide Web: Links zu schädlichen Websites in Phishing-E-Mails und Drive-by-Infections sind die meistgenutzten Angriffsvektoren der Cyberkriminellen. Im Kernkraftwerk Gösgen (KKG) legt man deshalb schon seit Jahren Wert auf den sicheren Zugang zum Web. Mit einer selbst konfigurierten Lösung auf Basis von VMware Thinapp wurde der Browser virtualisiert, sodass der Web-Traffic und damit auch möglicher Schadcode ausschliesslich in der virtuellen Umgebung in Erscheinung trat und die PCs der Mitarbeitenden nicht direkt erreichen konnte.

Bisherige Lösung zunehmend unbefriedigend

Thinapp wird allerdings vom Hersteller VMware nur gelegentlich mit Unterstützung für die aktuellsten Browserversionen aktualisiert, während fast im Wochentakt eine neue Ausgabe des im KKG genutzten Firefox-Browsers erscheint. Manuela Schweizer, im KKG für die Technik von IT Security und Netzwerk zuständig, hält dazu fest: «Wir sind immer mehr ins Hintertreffen geraten. Und der Aufwand für die Paketierung von Firefox für das virtuelle Deployment war beträchtlich. Deshalb suchten wir eine neue Lösung, die mit der Entwicklung der Browser mithält und den Arbeitsaufwand reduziert.»

Da kam es gelegen, dass BOLL Engineering im Sommer 2018 auf François Gasser, den IT-Sicherheitsbeauftragten des KKG, zukam und ihm die Menlo Isolation Platform vorstellte. Das Interesse war sofort geweckt: «Es war schon bei der ersten Demonstration klar, dass wir genau solch eine Lösung wollten – wenn das Konzept in der Praxis wirklich funktioniert, ist Browser-Isolation eine geniale Lösung für sämtliche Sicherheitsprobleme beim Surfen», zeigt sich Gasser überzeugt.

Erfolgreiche Proofs of Concept

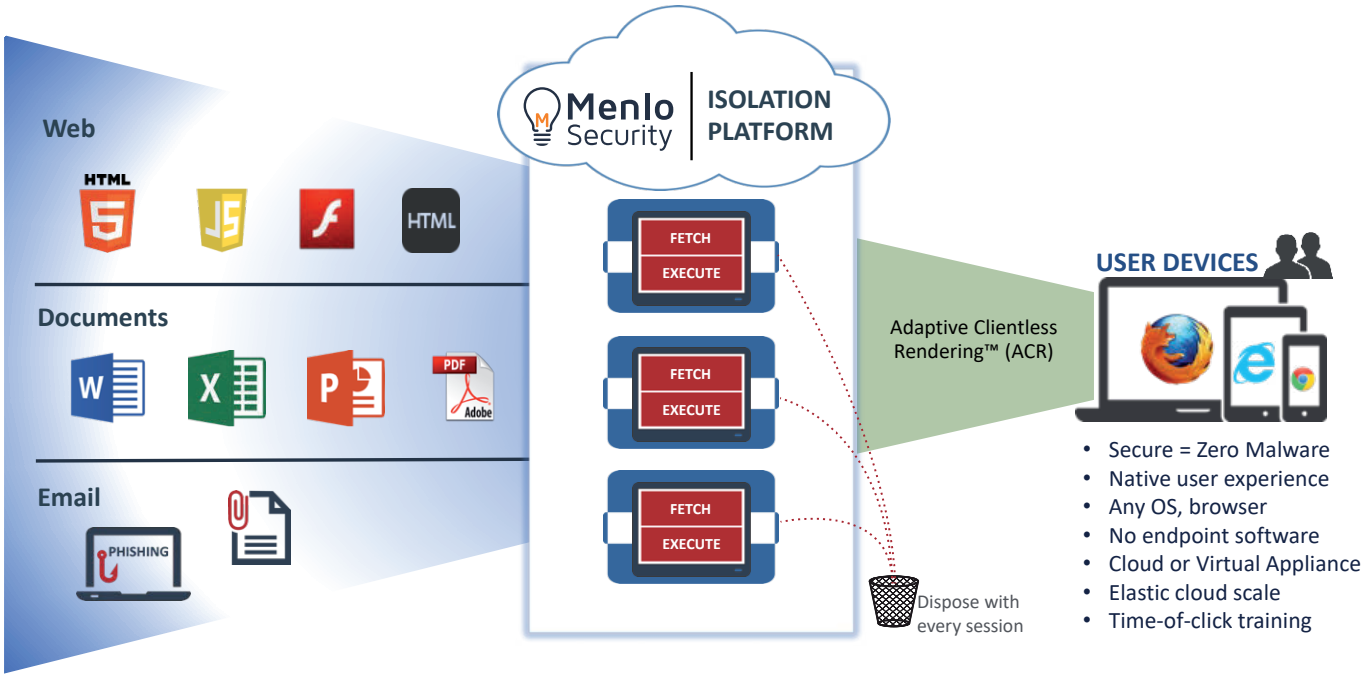
Dass die Isolation funktioniert, wurde anhand eines Proof of Concept ziemlich schnell deutlich. Der BOLL-Partner BNC Business Network Communications AG stellte dem KKG einen Test-Account der Cloud-Variante der Menlo Isolation Platform zur Verfügung. François Gasser nutzte die Lösung als erster Teilnehmer selbst. Sein Fazit: «Praktisch alle Websites wurden anstandslos dargestellt – es gab viel weniger Probleme als erwartet.» Einzig bei wenigen, besonders komplexen Webformularen sei es zu Einschränkungen gekommen.

Parallel zur Menlo Isolation Platform evaluierte das KKG eine zweite Lösung, die ebenfalls auf dem Prinzip Isolation basiert. Doch diese erwies sich in einigen Punkten als weniger ausgereift. «Bei der Menlo-Lösung lässt sich zum Beispiel direkt aus dem Logfile eine Exception generieren und Probleme können so rasch behandelt werden. Die andere Lösung bietet diesen Komfort nicht.» Das KKG entschied sich demnach gegen Ende 2018 für die Menlo Isolation Platform und für BNC als Beratungs- und Implementa-

Vorteile der Menlo Isolation Platform für das KKG

- Umfassende Sicherheit für alle Mitarbeitenden beim Web-Zugang
- Arbeitsaufwand für Konfiguration und Paketierung des Browsers entfällt
- Einfache Update- und Rollback-Funktion über GUI
- Kontinuierliche Aufzeichnung des Surfverhaltens
- Support für Streaming
- Browserkonfiguration via PAC-File
- Rollenbasierte Zugriffskontrolle

Auf einen Blick: *Kunde:* Kernkraftwerk Gösgen-Däniken AG, 4658 Däniken / www.kkg.ch *Reseller:* BNC Business Network Communications AG, 8600 Dübendorf / www.bnc.ch



tionspartner. «BNC kannten wir bisher nicht», hält Manuela Schweizer fest, «aber die Chemie hat von Anfang an gestimmt. Die technischen Details und die Umsetzung haben wir Hand in Hand erarbeitet. Das hat rasch Vertrauen geschaffen.»

Produktive Isolationsplattform On-Premises

Für das KKG kam die produktive Nutzung der cloudbasierten Isolationsplattform jedoch aus Datenschutzgründen nicht infrage. In einem zweiten Proof of Concept kam deshalb die On-Premises-Variante zum Einsatz. Manuela Schweizer setzte mit Unterstützung durch BNC einen Management-Server und einen Isolation-Node als virtuelle Appliances auf. Nun wurde die gesamte IT-Abteilung in den Test einbezogen, ergänzt durch ausgewählte Nutzer aus den Fachabteilungen des KKG – insgesamt konnten rund 30 Mitarbeitende die Lösung auf Herz und Nieren prüfen. Allfällige Probleme sollten auf einer Liste im Intranet gemeldet werden. «In den ersten Tagen blieb die Liste völlig leer, und zum Schluss der fast zweimonatigen Testphase umfasste sie vielleicht zehn Einträge», resümiert der IT-Sicherheitsbeauftragte den klaren Erfolg des zweiten PoC.

Seit Ende Februar 2019 surfen nun alle rund 550 Mitarbeitenden des KKG plus eine Reihe Externer produktiv über die Menlo Isolation Platform. Die Performance ist nach einigem anfänglichen Fine-Tuning überzeugend. Aktuell betreibt das KKG neben dem Management-Server vier Isolation Nodes, die für die aufwendigen Aufgaben der Ausführung von aktivem Code und das Rendering der bereinigten Version der Webinhalte zuständig sind. Das Load Balancing übernimmt die bestehende IT-Infrastruktur des KKG.

Unkomplizierte Einführung

Die Mitarbeitenden wurden per Intranet-News über die neue Plattform informiert. Eine Schulung war unnötig: Die Nutzer merken von der dahinterstehenden Technik überhaupt nichts. Auf den Endgeräten muss kein Agent oder spezieller Browser installiert werden. Einzig die Umstellung vom bisherigen virtualisierten Browser auf den lokal auf den Clients installierten Firefox-Browser war mit etwas Aufwand und einigen Problemen verbunden.

Manuela Schweizer freut sich über den zeitsparenden Update-Mechanismus, der sich über ein Webinterface bedienen lässt. Auch alle weiteren Administrationsaufgaben lassen sich über diese Web-Oberfläche intuitiv erledigen. «Und wenn es einmal Probleme mit einer neuen Firmware geben sollte, ist genauso einfach ein Rollback durchgeführt.»

Während früher jedes potenzielle Malware-Problem einzeln auf die Gefährlichkeit hin untersucht werden musste, kann sich François Gasser nun beruhigt zurücklehnen, denn dank Isolation kommt garantiert kein Schadcode beim Websurfen mehr auf die Clients. Die Mitarbeitenden können gefahrlos auch auf Websites zugreifen, die früher gesperrt werden mussten. «Das erleichtert die Arbeit stark. Wir geniessen die Sicherheit, die wir mit der Menlo Isolation Platform erreicht haben.»

Menlo Isolation Platform

Die Menlo Isolation Platform nimmt alle eingehenden Webinhalte entgegen und führt sämtlichen aktiven Code wie Javascript und Flash in einer abgeschotteten virtuellen Umgebung aus. Eine allfällige Infektion findet zwar statt – dies jedoch in einem «Käfig», aus dem der Schadcode nicht ausbrechen kann. Die ursprünglichen Inhalte werden sofort nach der Ausführung «entsorgt». Der Nutzer beziehungsweise dessen Endgerät erhält über einen Proxy-Service eine gerenderte, von aktivem Code befreite Version. Scripts sind entfernt, Flash-Videos automatisch ins MP4-Format umgewandelt. Dazu muss auf dem Endgerät keine Client-Software installiert werden – der Nutzer arbeitet mit dem üblichen Browser mit gewohntem Komfort und gewohnter Geschwindigkeit.

Leistungsmerkmale

- Vollständige Isolation der Anwender von jeglicher Malware
- URL Filtering
- Adaptive Clientless Rendering: keine Software auf dem Client nötig, Surferlebnis wie gewohnt
- Eliminiert Schadcode in JavaScript-, Flash- und Java-Inhalten
- 100-prozentig sichere Isolation: auch Bilder und Fonts werden bereinigt
- Schutz vor schädlicher Werbung (Malvertising), Drive-by-Infections und Ransomware
- Erhältlich als Cloud-Service oder virtuelle Appliance
- Lizenziert pro User und Jahr