



HÖCHSTMÖGLICHE SICHERHEIT BEIM SURFEN

Über die Menlo Isolation Plattform 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

» BNC kannten wir bisher nicht, 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. «

MANUELA SCHWEIZER

Technik IT Security und Netzwerk,
Kernkraftwerk Gösgen



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 Implementationspartner. «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.»



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 wurden 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.

» Schon bei der Demonstration wurde klar: Browser-Isolation ist eine geniale Lösung für sämtliche Sicherheitsprobleme beim Surfen. «

FRANÇOIS GASSER

IT-Sicherheitsbeauftragter, Kernkraftwerk Gösgen

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 – ins-



ÜBER DAS KKG

Das Kernkraftwerk Gösgen (KKG), das erste Schweizer Kernkraftwerk der 1000-Megawatt-Klasse, nahm im November 1979 den kommerziellen Betrieb auf. Seither wurden mehrere Modernisierungsprojekte zur weiteren Erhöhung der Sicherheit durchgeführt. Die Anlage erzeugt mittlerweile acht Milliarden Kilowattstunden Strom pro Jahr und deckt damit etwa 13 Prozent des schweizerischen Stromverbrauchs. Das KKG beschäftigt gegen 550 Mitarbeiterinnen und Mitarbeiter. An der Kernkraftwerk Gösgen-Däniken AG, welche die Anlage betreibt, sind die fünf Partner Alpiq, Axpo, Stadt Zürich, CKW und ewb beteiligt. Die Geschäftsleitung liegt in den Händen der Alpiq.



ÜBER BNC

Die BNC Business Network Communications AG, gegründet im Jahr 1998, ist mit über 60 Mitarbeitenden an den Standorten Bern, Zürich und Lausanne ein bedeutender Schweizer IT-Infrastruktur-Dienstleister. BNC entwirft, implementiert und verwaltet individuelle Lösungen und Services in den Bereichen Networks, Security und Cloud & Data Center und berät und unterstützt mittlere und grössere Unternehmungen und Organisationen sowie IT-Service-Provider. Mit den Professional, Support und Managed Services von BNC können diese nicht nur mit dem raschen Technologiewandel Schritt halten, sondern auch einen Wettbewerbsvorteil daraus ziehen.

STARKE PARTNER

KUNDE

Kernkraftwerk Gösgen-Däniken AG
4658 Däniken
www.kkg.ch



RESELLER

BNC Business Network Communications AG
8600 Dübendorf
www.bnc.ch



DISTRIBUTOR

BOLL Engineering AG
5430 Wettingen
www.boll.ch

