HP WOLF ENTERPRISE SECURITY

POWERED BY Bromium®

HP WOLF SECURITY

DIE STADT BONN ERRICHTET EINEN SCHUTZSCHILD GEGEN UNBEKANNTE MALWARE

Der Schutz vertraulicher Daten genießt in der Stadtverwaltung höchste Priorität – und sie schlägt eine innovative Richtung ein. Durch die Entscheidung für die HP Sure Click Lösung schützt die Stadt die Endgeräte ihrer Mitarbeitenden – und somit die vertraulichen Daten von Einwohner:innen – vor zuvor unbekanntem Malwarecode.

Das 72 Meter hohe Rathaus ist der Hauptsitz der Verwaltung der Bundesstadt Bonn. (Quelle: Bundesstadt Bonn)

Herkömmliche Sicherheitstools sind in der kommunalen IT heutzutage Standard. Neue Zero-Day-Attacken, moderne persistente Bedrohungen und Ransomware-Trojaner können damit jedoch nicht zuverlässig entdeckt werden. Grund genug für die Stadtverwaltung Bonn, die Client-Sicherheit zu verbessern. Zwei Aspekte waren hierbei besonders wichtig: Sicherheit beim Surfen sowie bei der E-Mail-Kommunikation. Wenngleich Unternehmen den Empfang von E-Mail-Anhängen oder den Zugriff auf Websites streng regulieren können, ist dies in Stadtverwaltungen aufgrund berechtigter Interessen von Bürger:innen nicht möglich. PDF-Dokumente und ZIP-Archive müssen zugelassen werden; Mitarbeitende müssen in der Lage sein, aus Gründen des Jugendschutzes entsprechende fragwürdige Foren oder Websites zu besuchen. Eine weitere Herausforderung ist die Tatsache, dass aufgrund des umfassenden Aufgabenspektrums von Stadtverwaltungen Hunderte von Anwendungen, Tools und speziellen Prozessen bereitgestellt und betriebsbereit gehalten werden müssen.

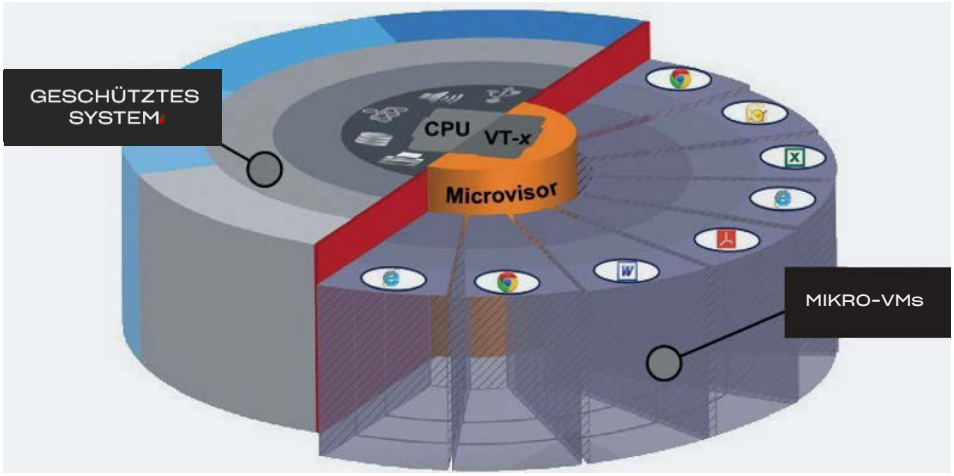
E-MAIL- UND BROWSERSCHUTZ VON EINER QUELLE

Bei der Auswahl einer Client-Sicherheitslösung zog die Stadtverwaltung Bonn anfangs mehrere Anwendungen in Betracht, welche die Schwachstellen von Internet-Browsern schützen und ein sicheres Surfen ermöglichen. Diese Anwendungen lösten jedoch nicht das äußerst wichtige E-Mail-Problem. Schnell wurde klar, dass die Secure Platform von Bromium mit ihrem technischen Konzept der „Isolation statt der Erkennung von Malware-Code mithilfe von Mikrovirtualisierung“ die bestmögliche Wahl war.

Im Rahmen einer kurzen Evaluierungsphase wurden umfassende Funktions- und Leistungstests durchgeführt. Ein zentrales Ergebnis war, dass etwa ein Viertel der ca. 4.000 Computer nicht über die erforderliche Ausstattung für einen nahtlosen Einsatz der Bromium Lösung verfügten. Schließlich entschied sich die Stadtverwaltung für eine schrittweise Einführung der Secure Platform in Kombination mit dem Austausch älterer Hardware sowie der Einführung von Windows 10.

BROMIUM LÖSUNG BASIERT AUF ISOLATION STATT ERKENNUNG

Das zentrale Merkmal der Bromium Lösung ist, dass nicht das aktive Detektieren von Malwarecode Priorität genießt, sondern eher das effektive Vermeiden seiner Auswirkungen. Dies erfolgt durch Isolation aller riskanten Benutzeraktivitäten mithilfe von Mikro-Virtualisierung. Kernelemente hierbei sind ein speziell mit Blick auf Sicherheitsaspekte entwickelter Xen-basierter Hypervisor sowie die integrierten virtuellen Features aller aktuellen CPU-Generationen.



Die Lösung von Bromium führt anschließend Aufgaben stets in virtuellen Instanzen aus, wenn diese Gefahren bergen können, beispielsweise bei der Beurteilung einer Website, beim Öffnen eines E-Mail-Anhangs oder beim Zugriff auf die Daten auf einem USB-Laufwerk. Hier werden alle einzelnen Aufgaben auf eigenen Mikro-VMs ausgeführt und streng vom tatsächlichen Betriebssystem sowie dem angebundenen Netzwerk getrennt, wodurch ein Kompromittieren der Endgeräte und des IT-Netzwerks der Stadtverwaltung verhindert wird.

Bromium stellt ein virtuelles Sicherheitsnetz für PC-Anwender:innen bereit, das auch dann schützt, wenn unbekannte Bedrohungen andere Schutzmaßnahmen umgehen können. Hardware-gestützte Virtualisierung isoliert risikobehaftete Inhalte, um Nutzer-PCs, Daten sowie Anmeldeinformationen zu schützen, und macht Malware unschädlich, während die IT-Abteilung verwertbare Bedrohungsdaten erhält, um die Sicherheitslage des Unternehmens zu verbessern.

„Bromium bot mit dem Lizensierungs- und Service-Modell die technisch beste und kosteneffektivste Lösung“, sagte Dirk Schumacher, Leiter der Spezialabteilungs-IT-Sicherheit und IT-Strategie der Personal- und Organisationsabteilung der Bundesstadt Bonn.

ÜBER HP SURE CLICK ENTERPRISE

HP Sure Click Enterprise[1] basiert auf der branchenführenden Containment-Technologie der ehemaligen Bromium Inc. und bietet ein virtuelles Sicherheitsnetz für PC-Benutzer, das auch dann funktioniert, wenn unbekannte Bedrohungen andere Schutzmechanismen umgehen. Hardware-gestützte Virtualisierung isoliert risikobehaftete Inhalte, um Nutzer-PCs, Daten sowie Anmeldeinformationen zu schützen, und macht Malware unschädlich, während die IT-Abteilung verwertbare Bedrohungsdaten erhält, um die Sicherheitslage des Unternehmens zu verbessern. HP Inc. ging 2016 eine formelle OEM-Beziehung mit Bromium Inc. ein und begann mit der Auslieferung der Bromium Containment-Technologie, die als HP Sure Click[2] vermarktet wird, auf Millionen von Geräten der Enterprise-Klasse. Nach der formellen Übernahme von Bromium Inc. Ende 2019 benannte HP die Bromium Secure Platform in HP Sure Click Enterprise um – das heutige Top-Produkt des HP Wolf Enterprise Security Portfolios.[3]

Weitere Informationen finden Sie unter www8.hp.com/us/en/security/enterprise-pc-security.html

1 HP Sure Click Enterprise erfordert Windows 10 und Microsoft Internet Explorer; Edge, Google Chrome, Chromium oder Firefox werden unterstützt. Zu den unterstützten Anhängen gehören u. a. Microsoft Office (Word, Excel, PowerPoint)- und PDF-Dateien, wenn Microsoft Office bzw. Adobe Acrobat installiert ist.

2 HP Sure Click erfordert Windows 10. Ausführliche Informationen finden Sie unter https://bit.ly/2PrLT6A_SureClick.

3 HP Wolf Enterprise Security erfordert Windows 10. HP Sure Click Enterprise unterstützt die Browser Microsoft Internet Explorer, Edge, Google Chrome, Chromium sowie Firefox und isoliert Anhänge von Microsoft Office (Word, Excel, PowerPoint) und PDF-Dateien, wenn Microsoft Office oder Adobe Acrobat installiert ist. HP Protected App unterstützt derzeit RDP-Sitzungen, Citrix® ICA-Sitzungen und Chromium-basierte Browser.

4AA7-7797DEE, Rev. 1, Juni 2021