HP WOLF ENTERPRISE SECURITY

POWERED BY Bromium®

SCHLIESSEN SIE IHRE GRÖSSTE SICHERHEITSLÜCKE ENDGÜLTIG

IHR UNTERNEHMEN IST VON DATENSCHUTZVERLETZUNGEN NUR EINEN KLICK ENTFERNT

DER GRÖSSTE VORTEIL FÜR ANGREIFER IST DAS VERHALTEN IHRER NUTZER

Mehr als 70 % der Datenschutzverletzungen in Unternehmen werden durch PC-Nutzer ausgelöst.[1] Das Einfallstor dafür sind zu mehr als 99 % E-Mails, das Web, Chats oder USB-Medien.[2] Und 99 % dieser Vorfälle sind nur durch Nutzeraktionen möglich, das heißt, sie ereignen sich, weil Nutzer auf etwas klicken oder auf bösartiges Phishing hereinfallen.[3]

Mit HP Sure Click Enterprise[4] hingegen können Sie über E-Mails, Web, Chats und USB-Medien verursachte Datenschutzverletzungen mühelos verhindern. Die Anwendung stellt ein virtuelles Sicherheitsnetz für PC-Benutzer bereit, das auch dann schützt, wenn unbekannte Bedrohungen andere Schutzmaßnahmen umgehen können. Hardware-gestützte Virtualisierung isoliert risikobehaftete Inhalte, um Nutzer-PCs, Daten und Anmeldeinformationen zu schützen, und macht Malware unschädlich, während die IT-Abteilung verwertbare Bedrohungsdaten erhält, um die Sicherheitslage des Unternehmens zu verbessern.

Die derzeit verfügbaren HP-Features zielen auf sechs Bedrohungsvektoren ab:
Für das Unternehmen:

- Webnavigation
- Microsoft Office-Anwendungen
- PDF-Dateien
- E-Mail:
- Collaboration-Tools
- Anwendungen

Angriffe auf diese Komponenten öffnen die Türen für Ransomware, dateilose Malware, den Diebstahl von Anmeldedaten, infizierte ausführbare Dateien und mehr.

Im Versuch, sich gegen diese Risikovektoren zu wehren, haben Unternehmen Kontrollen in ihren Clouds, Netzwerken und an Endgeräten eingeführt, unter anderem mit Cloud CASB, Antivirenprogrammen für Clouds und Netzwerke, Sandboxing und Sicherheitsanalysen. Für die Endgeräte wurden Antivirenprogramme, Anwendungs-Whitelists sowie , Lösungen für die Endgeräteerkennung und Reaktion (EDR) eingeführt. Zum Schutz vor diesen Bedrohungsvektoren und den daraus folgenden Konsequenzen setzen Unternehmen von der Cloud bis zum Endgerät im Durchschnitt 60 Kontrollpunkte ein.

Trotz all dieser Kontrollen zum Schutz der Endgeräte – und damit des Unternehmens – sind sie dennoch von Datenschutzverletzungen weiterhin nur einen Klick entfernt. Denn die Technologie hat eine Wirksamkeit zwischen 90 % und 95 %, darum treten Datenschutzverletzungen weiterhin auf. Um die Lücke der verbleibenden 5 %-10 % zu schließen, empfiehlt Gartner Schulungen für besseres Sicherheitsbewusstsein, was für eine allgemeine Sensibilisierung im Unternehmen sicher nützlich ist, aber nicht vor Profi-Hackern schützt.

Unternehmen sind nur einen Klick von Datenschutzverletzungen entfernt und der Grund dafür ist die Beziehung zwischen Endanwendern und schädlichen Inhalten. Wissenschaftlich betrachtet, insbesondere nach der Kausalitätstheorie, führt ein Ereignis (Ursache) zum Eintreten eines anderen Ereignisses (Wirkung). Übertragen auf die Cybersicherheit – und im Einzelnen auf Sure Click Enterprise – ist die Ursache ein menschlicher Fehler des Nutzers und die Wirkung die Konsequenz seines fatalen Klicks.

Eliminieren wir nun die Ursache, also das menschliche Fehlerpotenzial, aus der Umgebung, werden ALLE Wirkungen ebenfalls eliminiert. Denn das Eintreten dieser Wirkungen ist vom menschlichen Verhalten abhängig, mit dem der Nutzer Angreifern Tür und Tor zum Unternehmen öffnet.

Sure Click Enterprise beseitigt die Ursache aus der Gleichung. Sure Click Enterprise verarbeitet jede Nutzeraufgabe (z. B. das Öffnen eines E-Mail-Anhangs) in einer isolierten, hardwaregestützten virtuellen Mikromaschine (Mikro-VM). Dadurch kommt die Malware über die Aktion, mit der sie angekommen ist, nicht hinaus, sodass sie weder den Computer des Benutzers noch andere Geräte im Netzwerk infizieren kann. Wenn der Vorgang abgeschlossen ist, wird die Mikro-VM zusammen mit der Malware zerstört. Und das Beste daran: Die Nutzerproduktivität wird in keinster Weise beeinträchtigt, weil Nutzer nichts zusätzlich tun müssen, um sich von Sure Click Enterprise vor Bedrohungen schützen zu lassen.

IHR ENDGERÄT

HP Sure Click Enterprise zur Anwendungsisolierung hält Malware und lauernde Angreifer zuverlässig von den PCs Ihrer Nutzer und Ihrem Netzwerk fern.

Ist die Ursache beseitigt, gibt es: nichts zu stehlen > kein Ziel > keine Schleichwege mehr. Mit dem Ausschluss des menschlichen Fehlerpotenzials nehmen Sie dem Angreifer seine Eintrittskarte. Das ist so, als würden

70 % DER ANGRIFFSFLÄCHE EINFACH VERSCHWINDEN.

SETZEN SIE MIT HP WOLF ENTERPRISE SECURITY CYBERANGRIFFEN EIN ENDE, ENDGÜLTIG.

HP wendet für die Endgerätesicherheit Zero-Trust-Grundsätze an und schützt so seine Kunden auch vor den jeweils neuesten Bedrohungen, mit zuverlässiger, Hardware-gestützter Technologie für Isolation und Eindämmung.

Als Bestandteil der HP Wolf Enterprise Security-Dienste schützt HP Sure Click Enterprise vor gefährlichen Klicks. Mit den Hardware-gestützten Mikro-VMs und modernster Hypervisor-Technologie werden E-Mails, Anwendungen und Browser isoliert und so die Nutzer-PCs, ihre Identität sowie das Netzwerk zuverlässig gesichert.

Mit seiner einfachen Bereitstellung und der erweiterten, hochgradig zuverlässigen Threat Intelligence, die keine zusätzliche Infrastruktur vor Ort und keinen Erwerb weiterer Software erfordert, eignet sich HP Sure Click Enterprise besonders für Unternehmen und Behörden, die auf ein höheres Schutzlevel angewiesen sind.

[1] https://www.rapid7.com/resources/rapid7-efficient-incident-detection-investigation-saves-money/

[2] HP Threat Intelligence-Daten

[3] https://www.proofpoint.com/us/resources/threat-reports/human-factor

[4] HP Sure Click Enterprise ist separat erhältlich und erfordert Windows 8 oder Windows 10. Microsoft Internet Explorer, Google Chrome, Chromium und 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.

---

c07907109, Juni 2021