LÖSUNGSÜBERSICHT

HP WOLF SECURITY

HP WOLF ENTERPRISE SECURITY

HP SURE CLICK ENTERPRISE

POWERED BY Bromium

BLOCKIEREN SCHÄDLICHER E-MAIL-ANHÄNGE

SICHERES ÖFFNEN ALLER E-MAIL-ANHÄNGE AUS OUTLOOK ODER WEBMAIL, SELBST WENN SIE MALWARE ENTHALTEN

VERMEIDEN RESTRIKTIVER IT-SICHERHEITSRICHTLINIEN, DIE DEN ZUGRIFF AUF E-MAIL-ANHÄNGE EINSCHRÄNKEN

VERBESSERN DER BENUTZERPRODUKTIVITÄT, INDEM MITARBEITERN DAS ÖFFNEN VON E-MAIL-ANHÄNGEN ERMÖGLICHT WIRD

MITARBEITER MÜSSEN E-MAIL-ANHÄNGE ÖFFNEN, UM IHRE AUFGABEN ERLEDIGEN ZU KÖNNEN

Mitarbeiter haben täglich mit E-Mail-Anhängen zu tun, beispielsweise, wenn sie Lebensläufe lesen, Rechnungen bearbeiten, Zustellungsbenachrichtigungen erhalten, Finanzaufstellungen gemeinsam nutzen oder bei rechtlichen Vereinbarungen mit externen Parteien zusammenarbeiten – und sie öffnen diese E-Mail-Anhänge oft, weil sie sicher aussehen. Cyberkriminelle sind sich dieser Sicherheitslücke bewusst und nutzen sie aus.

Heutzutage wird Ransomware häufig über „waffenfähige" Microsoft Office Dokumente oder PDF-Dateien übermittelt, die per E-Mail gesendet werden. Cyber-Kriminelle tun dies, weil es funktioniert. Laut Ransomware-Statistiken aus dem Jahr 2019 haben Unternehmen mehr als 7,5 Milliarden US-Dollar durch Ransomware-Angriffe verloren.[1]

Legitime Anwendungen, von denen vielen ausdrücklich auf der Whitelist, wie z. B. die Microsoft Office Suite, können ebenfalls ausgenutzt werden, um mehrschichtige Schutzmaßnahmen zu umgehen und von einem einzigen kompromittierten Host aus ein ganzes Unternehmen zu übernehmen.

Trotz vielversprechender Weiterentwicklungen bei der Malware-Erkennung, stetiger Verbesserungen bei sicheren E-Mail-Gateways und einer Zunahme von Schulungen zur Sensibilisierung der Benutzer überwinden schädliche E-Mail-Anhänge weiterhin alle Schutzvorkehrungen, was zu Datenschutzverletzungen, Datenverlusten und sogar zur Datenvernichtung führen kann.

Die raffinierte, per E-Mail verbreitete Malware von heute überwältigt ohne große Schwierigkeiten herkömmliche Erkennungs- und Abwehrmechanismen.

Hier einige Zahlen:

- Über 90 % der böswilligen E-Mail-Anhänge haben polymorphe Fähigkeiten.[2]
- 53 % der Viren verbreiten sich über .exe-Dateien aus[3], und 46 % der Hacker, die Malware verbreiten, übertragen diese fast ausschließlich per E-Mail.[3]

PER E-MAIL ÜBERMITTELTE MALWARE IST KOSTENGÜNSTIG, EFFIZIENT UND VERÄNDERT SICH STÄNDIG

Die folgende Schadsoftware wird heute von Cyberkriminellen erfolgreich genutzt:

- **Ransomware:** Verschlüsselt die Daten auf dem PC des Opfers mit einem symmetrischen Schlüssel und zwingt das Opfer dazu, Lösegeld zu zahlen oder ein Reimaging für den Computer durchzuführen. Ransomware ist weit verbreitet und wird in erster Linie über schädliche Dokumente eingeschleust.
- **Makroaktivierte Trojaner:** Legen schädliche Binärdateien auf dem Host ab, der dann die Kommunikation mit den Command-and-Control-Servern herstellt, um weitere Anweisungen zu erhalten und weiteren schädlichen Code herunterzuladen.
- **Dateilose Malware:** Missbraucht Tools wie PowerShell, um Befehle auszuführen, ohne Dateien auf dem Host abzulegen.
- **Schädliche Links:** Diese schädlichen Links, die sich in harmlosen E-Mail-Anhängen verstecken, können leicht durch mehrschichtige Abwehrmechanismen schlüpfen und zu einem Drive-by-Download oder Browser-Exploit führen.

HP SURE CLICK ENTERPRISE SETZT AUF ANWENDUNGSISOLIERUNG, UM MALWARE ZU ERFASSEN, DIE IN E-MAIL-ANHÄNGEN VERSTECKT IST

Es stellt den Anwendern ein virtuelles Sicherheitsnetz vor bekannten und unbekannten Bedrohungen bereit, indem es risikobehaftete Inhalte isoliert und verwertbare Erkenntnisse zur Stärkung der Sicherheitslage im Unternehmen liefert. Mit virtualisierungsbasierter Sicherheit öffnet HP Sure Click Enterprise E-Mail-Anhänge (wie Microsoft Office-Dokumente und PDF-Dateien) auf einem isolierten virtuellen Mikrocomputer (Virtual Machine, VM). Die Malware kann gestartet und ausgeführt werden, hat aber niemals Zugriff auf das Endgerät oder das Netzwerk. Die Malware ist im Wesentlichen im Mikro-VM-Container gefangen, wodurch sie für den Benutzer unschädlich gemacht wird, und wird entsorgt, sobald der Benutzer den E-Mail-Anhang schließt.

Dadurch, dass Malware vollständig ausgeführt werden kann, ändert sich die Helpdesk-Kultur: Endbenutzer sind stolz darauf, eine Malware-Erkennung zu melden, statt sich über IT-Sicherheitseinschränkungen zu beschweren.

ANWENDUNGSISOLIERUNG: SCHUTZ BEREITS VOR DER ERKENNUNG

E-MAIL-ANHÄNGE ABSCHOTTEN

Alle E-Mail-Anhänge werden in einer isolierten Mikro-VM geöffnet. Kommt Malware zum Einsatz, wird sie eingeschlossen. Sie kann nicht auf den Host zugreifen. Das Netzwerk ist nicht gefährdet.

IT-SICHERHEIT OPTIMIEREN UND KOSTEN SENKEN

Durch die High-Fidelity-Warnungen von HP Sure Click Enterprise können Sie die Selektierungszeit drastisch verkürzen und dafür sorgen, dass aufgrund falsch-positiver Ergebnisse keine Ressourcen mehr verschwendet werden.
Sie vermeiden Reimaging, Rebuilds und Notfallkorrekturen.

INFORMATIONEN ZU SICHERHEITSBEDROHUNGEN IN ECHTZEIT TEILEN

Adaptive Intelligenz erkennt und blockiert evasive Angriffe, teilt Echtzeit-Risikodaten über Ihr Netzwerk und liefert eine vollständige Angriffskettenanalyse (Kill Chain Analysis) für Ihr SOC.

DAUERHAFTEN SCHUTZ MIT HARDWAREGESTÜTZTER SICHERHEIT ERZIELEN

Nur HP Sure Click Enterprise nutzt virtualisierungsbasierte Sicherheit zum Erzielen einer hardwaregestützten Anwendungsisolierung Unsere Lösung schützt Sie sogar vor bisher unbekannten Bedrohungen und polymorpher Malware, die selbst durch fortschrittlichste Erkennungstools schlüpfen können.

46 % DER HACKER, DIE MALWARE VERBREITEN, TUN DIES FAST AUSSCHLIESSLICH PER E-MAIL[3]

- Verizon DBIR 2020[3]

AKTUELLE STATISTIKEN ÜBER COMPUTERVIREN ZEIGEN, DASS SICH 53 % DER VIREN ÜBER .EXE-DATEIEN VERBREITEN.

- Checkpoint 2020[3]

„DAS IST EIN GROSSARTIGES PRODUKT UND SEHR EFFEKTIV FÜR DIE SICHERHEIT UNSERES UNTERNEHMENS.“

– IT Systems Analyst Global 500 Banking Company[4]

Weitere Informationen finden Sie unter **https://www.hp.com/enterprisesecurity**

1. 34 Shocking 22 Shocking Ransomware Statistics for Cybersecurity in 2021 (2019) – SafeAtLast.co
2. Top 10 Email Malware Threats | eSecurity Planet /
3. A Not-So-Common Cold: Malware Statistics in 2021 | DataProt
4. TechValidate. https://www.techvalidate.com/tvid/813-0A2-81D
5. 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.

4AA7-7467DEE, April 2021, Rev. 2

HP WOLF SECURITY