HP WOLF SECURITY

HP WOLF ENTERPRISE SECURITY

# HP SURE CLICK ENTERPRISE

POWERED BY Bromium

## DIEBSTAHL VON ZUGANGSDATEN VERHINDERN

DIEBSTAHLVERSUCHE VON ANMELDEINFORMATIONEN VON UNSICHEREN WEBSITES BLOCKIEREN

SICHERE WEBSITE-BESUCHE OHNE ANGST VOR ANGRIFFEN

RESTRIKTIVE IT-SICHERHEITSRICHTLINIEN BESEITIGEN, DIE DEN BENUTZERZUGRIFF EINSCHRÄNKEN

## GESTOHLENE ANMELDEDATEN SIND DER SCHLÜSSEL ZU ERFOLGREICHEN DATENDIEBSTÄHLEN

Phishing-Angriffe sind heute die häufigste Ursache für Cybersecurity-Verstöße in Unternehmen, und die Anmeldedaten von Mitarbeitern sind ein bevorzugtes Ziel für böswillige Angriffe. Das liegt daran, dass sie der Schlüssel sind, um viele der anderen Sicherheitsprotokolle zu entsperren, die zum Schutz Ihres Unternehmens eingerichtet wurden. Die richtige Kombination aus Benutzernamen und Passwort ist häufig alles, was zwischen einem Cyberkriminellen und dem wertvollen geistigen Eigentum eines Unternehmens steht.

Spear-Phishing ist besonders effektiv, weil es zumeist ein positives Verhalten ausnutzt – den Wunsch einer Person, die Sicherheitsrichtlinien einzuhalten, indem sie genau die Anmeldedaten bereitstellt oder aktualisiert, die sie eigentlich schützen soll. Es ist auch schwierig zu blockieren, weil böswillige Websites zahlreich und kurzlebig sind. Ihr Inhalt wird oft geändert, um eine genaue Kategorisierung zu verhindern.

## PHISHING BLEIBT DIE HÄUFIGSTE UND EFFEKTIVSTE CYBERBEDROHUNG FÜR IHR UNTERNEHMEN

**Schädliche Phishing-Bedrohungen werden ständig weiterentwickelt und können viele Formen annehmen:**

- **Spear-Phishing:** Gezielte Betrugsversuche, die sich gegen Einzelpersonen richten, indem sie deren Namen, Rollen oder Arbeitsprozesse enthalten
- **Whaling:** Richtet sich gegen Führungskräfte von Unternehmen und hat häufig die Form von rechtlichen Hinweisen, Kundenbeschwerden oder Geschäftsleitungsinformationen
- **Social Engineering:** Tarnt sich als Appell an die Vertrauens- und Hilfsbereitschaft der menschlichen Natur
- **Unbeabsichtigte Infektion:** Teilen von Nachrichten oder Links aus sozialen Netzwerken, die kompromittiert wurden

**Phishing-Angriffe werden in unterschiedlicher Weise ausgeführt:**

- Phishing-Links in E-Mail-Nachrichten
- Zielgerichtete Links oder Nachrichten auf Social-Media-Plattformen
- Geteilte Links in Chatprogrammen

## HP SURE CLICK ENTERPRISE[1] VERHINDERT DEN DIEBSTAHL VON ANMELDEDATEN, INDEM BENUTZER VOR DER FREIGABE VON ANMELDEDATEN AUF BÖSWILLIGEN UND UNSERIÖSEN WEBSITES GEWARNT UND DIESE BLOCKIERT WERDEN

Sure Click Enterprise[1] stoppt den Diebstahl von Zugangsdaten durch das Verhindern der Möglichkeit, Passwörter auf Websites einzugeben, mit deren Hilfe Zugangsdaten gestohlen werden können, wenn ein Benutzer auf einen Phishing-Link in einer E-Mail, einem Chat-Client, einer PDF-Datei oder einer anderen Datei geklickt hat. Wenn ein Benutzer eine Website besucht und zur Eingabe seiner Anmeldedaten aufgefordert wird, nutzt Sure Click Enterprise den HP Threat Intelligence Service, um im Hintergrund eine Seriositäts- und Domain-Analyse durchzuführen, um die Sicherheit der Website zu erkennen. Bei einwandfreien, bekanntermaßen sicheren Websites kann der Benutzer seine Anmeldedaten wie gewohnt und ohne Behinderungen durch die Software eingeben.

Handelt es sich bei der Seite jedoch um eine Phishing-Seite, wird ein Warnfenster über der Seite angezeigt, sobald der Benutzer versucht, sein Passwort einzugeben, und so die Erfassung der Zugangsdaten verhindert. Die Software kann dahingehend konfiguriert werden, dass der Benutzer entweder das Browserfenster sicher schließen oder die Seite mit inaktivierten Feldern zur Datenerfassung anzeigen kann.

Bei Seiten mit niedriger Reputation werden die Benutzer gewarnt, die Seite genau zu prüfen und keine Zugangsdaten einzugeben, bis die Seite für den Benutzer als sicher eingestuft wurde. Administratoren können auswählen, ob die Eingabe von Benutzerdaten auf diesen Seiten blockiert wird oder ob die Benutzer fortfahren können, wodurch die Seite anschließend der Liste der zuverlässigen Seiten auf diesem Benutzer-PC hinzugefügt und die Warnung bei zukünftigen Besuchen nicht mehr angezeigt wird, um unnötige Einschränkungen der Produktivität zu vermeiden. Alle Aktionen, die auf bekanntermaßen böswilligen und unseriösen Websites durchgeführt werden, werden aufgezeichnet und an den Sure Click Controller gemeldet, damit die IT-Abteilung den Status der Bedrohung und des Benutzerverhaltens überprüfen kann.

## ZUGANGSDATENSCHUTZ: VERSTÖSSE DURCH PHISHING-ANGRIFFE VERMEIDEN

### DEN DIEBSTAHL VON ZUGANGSDATEN DURCH PHISHING-ATTACKEN VERHINDERN

Verringern Sie das Risiko, dass Ihre Mitarbeiter auf Phishing-Betrügereien hereinfallen.
Sure Click Enterprise blockiert die Eingabe von Anmeldedaten auf bekanntermaßen böswilligen Websites und warnt die Benutzer vor potenziell riskantem Verhalten auf allen Websites mit niedriger Reputation.

### 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 keine Ressourcen mehr aufgrund falsch-positiver Ergebnisse verschwendet werden. Sie vermeiden Reimaging, Rebuilds und Notfallkorrekturen.

### INFORMATIONEN ZU SICHERHEITSBEDROHUNGEN IN ECHTZEIT TEILEN

Adaptive Intelligenz identifiziert und stoppt ausweichende Angriffe, teilt Echtzeit-Risikodaten über Ihr Netzwerk und bietet 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.

**67 % ALLER SICHERHEITSVERLETZUNGEN WERDEN DURCH DEN DIEBSTAHL VON ZUGANGSDATEN VERURSACHT**

– Verizon DBIR 2020[2]

**DATENSCHUTZV-ERLETZUNGEN MIT GESTOHLENEN ZUGANGSDATEN KOSTEN DIE UNTERNEHMEN WELTWEIT DURCHSCHNITTLICH 3,86 MILLIONEN DOLLAR PRO VORFALL, IN DEN USA SOGAR BIS ZU 8,36 MILLIONEN DOLLAR.**

– IBM Cost of a Data Breach Report 2020[3]

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

1. 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.
2. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2020/
3. https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/



4AA7-7469DEE, April 2021, Rev. 2

HP WOLF SECURITY