Lösungsübersicht

EINDÄMMUNG VON PHISHINGANGRIFFEN

SICHERES ÖFFNEN VON LINKS, EINSCHLIESSLICH SCHÄDLICHER LINKS

VERMEIDEN RESTRIKTIVER IT-SICHERHEITSRICHTLINIEN, DIE DEN BENUTZERZUGRIFF AUF GETEILTE URLs EINSCHRÄNKEN

SCHUTZ VOR PHISHINGLINKS DANK NATIVER BROWSERLEISTUNG UND BENUTZERFREUNDLICHKEIT

PHISHINGLINKS UMGEHEN WEITERHIN MEHRSCHICHTIGE ABWEHRMECHANISMEN

Trotz der Weiterentwicklungen von Antiphishingtechniken und Mitarbeiterschulungen werden Phishingangriffe immer beliebter. Das liegt daran, dass sie so gut funktionieren. Schließlich müssen Mitarbeiter auf Links klicken, um ihre Arbeit erledigen zu können, und Social Engineering erschwert das Identifizieren von Phishinglinks.

Phishinglinks sind besonders effektiv, weil es zahlreiche böswillige und kurzlebige Websites gibt. Ihr Inhalt wird oft geändert, um eine genaue Kategorisierung zu verhindern. Erschwerend kommt hinzu, dass einige Mitarbeiter schnell und unüberlegt auf Links klicken und ihre E-Mail- und Chatclients geöffnet lassen, wodurch eine sofortige Möglichkeit für Cyberkriminelle geschaffen wird.

EINE KOSTENGÜNSTIGE UND EFFEKTIVE MÖGLICHKEIT, SCHÄDLICHE NUTZLASTEN EINZUSCHLEUSEN

Schädliche Phishinglinks werden ständig weiterentwickelt und nehmen viele Formen an:

- **Spear-Phishing:** Gezielte Betrugsversuche, die sich an Einzelpersonen richten, indem sie deren Namen, Rollen oder Arbeitsprozesse enthalten.
- **Whaling:** Richtet sich an Führungskräfte von Unternehmen und wird häufig in Form von rechtlichen Hinweisen, Kundenbeschwerden oder Themen der Geschäftsleitung geschrieben.
- **Social Engineering:** Getarnt als Appelle an die Bereitschaft des Menschen, Vertrauen zu haben und hilfsbereit zu sein.
- **Unbeabsichtigte Infektion:** Teilen von Nachrichten oder Links von sozialen Netzwerken, die kompromittiert wurden.

Phishingangriffe werden in unterschiedlicher Weise ausgeführt:

- Phishinglinks in E-Mail-Nachrichten
- Schädliche Links in harmlosen E-Mail-Anlagen
- Gezielte Links oder Nachrichten auf Social-Media-Plattformen
- Geteilte Links in Chatprogrammen

HP SURE CLICK ENTERPRISE, UNTERSTÜTZT VON BROMIUM, VERWENDET ANWENDUNGSISOLIERUNG ZUM SCHUTZ DES HOSTS VOR PHISHINGBEDROHUNGEN

HP Sure Click Enterprise verwendet virtualisierungsbasierte Sicherheit, um Organisationen vor Phishingbedrohungen zu schützen, indem jeder geteilte Link in einer geschützten Mikro-VM-Browserregisterkarte geöffnet wird.

Durch hardwaregestützte Isolierung wird jede Browserregisterkarte in einem eigenen sicheren Container ausgeführt, vollständig isoliert vom Host und von allen anderen Browserregisterkarten, um eine Kreuzkontamination zu verhindern. Beim Schließen der Browserregisterkarte wird der Mikro-VM zusammen mit jeder Bedrohung beendet. Die vollständige Malware-Angriffskette wird an den HP Sure Click Enterprise-Controller gesendet und für alle anderen HP Sure Click Enterprise-Geräte in Ihrem Netzwerk freigegeben, wodurch die Infrastruktur weiter abgesichert und die gesamte Angriffsfläche verkleinert wird.

ANWENDUNGSISOLIERUNG: SCHÜTZEN BEREITS VOR DER ERKENNUNG

Phishingbedrohungen eindämmen

Öffnen Sie alle Links auf einer isolierten Mikro-VM-Browserregisterkarte. Kommt Malware zum Einsatz, wird sie eingedämmt, sodass der Host und das Netzwerk nicht gefährdet sind. Mitarbeiter können jetzt sorglos darauf klicken.

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. Vermeiden Sie Reimaging, Rebuilds und Notfallkorrekturen.

Echtzeitinformationen zu Sicherheitsbedrohungen freigeben

Adaptive Intelligenz identifiziert und stoppt ausweichende Angriffe, gibt Echtzeit-Risikodaten für Ihr Netzwerk frei und bietet eine vollständige Angriffskettenanalyse (Kill Chain-Analyse) für Ihr SOC.

Dauerhaften Schutz durch hardwaregestützte Sicherheit erreichen

Nur HP Sure Click Enterprise verwendet virtualisierungsbasierte Sicherheit, um eine hardwaregestützte Anwendungsisolierung zu ermöglichen. Schützen Sie sich vor unbekannten Bedrohungen und polymorpher Malware, die selbst durch die fortschrittlichsten Erkennungstools schlüpfen können.

92 % der Organisationen schulen Endbenutzer in der Erkennung und Vermeidung von Phishingangriffen.

- Wombat Security[1]

Phishing verleitet Benutzer zur Installation von C2- und Keylogger-Software, um Anmeldeinformationen zu erfassen, die zum Authentifizieren bei und zum Herausfiltern von Daten aus Organisationen verwendet werden.

- Verizon DBIR 2017[2]

Weitere Informationen unter https://www.hp.com/enterprisesecurity

1. https://www.wombatsecurity.com/press/press-releases/annual-state-phish-report-wombat-security-showssimulated-phishing-and-training
2. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

© Copyright 2020. HP Development Company, L.P. Änderungen vorbehalten. Neben der gesetzlichen Gewährleistung gilt für HP Produkte und Dienstleistungen ausschließlich die Herstellergarantie, die in den Garantieerklärungen für die jeweiligen Produkte und Dienstleistungen explizit genannt wird. Aus den Informationen in diesem Dokument ergeben sich keinerlei zusätzliche Gewährleistungsansprüche. HP haftet nicht für technische bzw. redaktionelle Fehler oder fehlende Informationen. Microsoft, Windows und das Windows Logo sind Marken bzw. eingetragene Marken der Microsoft Corporation in den USA und/oder anderen Ländern. Adobe® ist eine Marke von Adobe Systems Incorporated. Intel, Core und Xeon sind Marken der Intel Corporation oder ihrer Tochtergesellschaften in den USA und anderen Ländern. AMD und Ryzen sind Marken von Advanced Micro Devices, Inc.