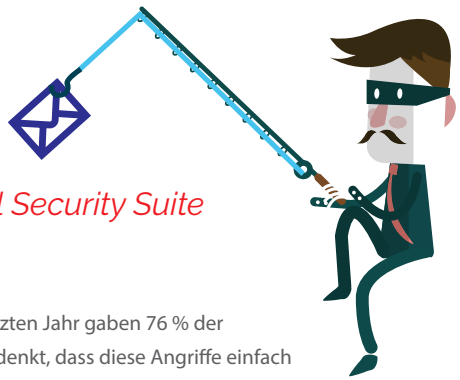
Lassen Sie sich nicht von einem Hacker ködern

Schutz Ihres Unternehmens vor Phishing-Angriffen mit WatchGuard Total Security Suite



Einführung

Phishing-Angriffe sind nach wie vor ein wichtiges Thema für kleine und mittelständische Unternehmen. Allein im letzten Jahr gaben 76 % der Unternehmen an, Opfer eines Phishing-Angriffs geworden zu sein.[1] Was nicht sonderlich verwundert, wenn man bedenkt, dass diese Angriffe einfach durchzuführen und für erfolgreiche Angreifer besonders gewinnbringend sind.

Aber es gibt gute Nachrichten für IT-Administratoren - mit ein wenig Wissen über Phishing und einer mehrschichtigen Verteidigungsstrategie ist es möglich, Ihr Unternehmen vor einem Phishing-Angriff zu schützen.

Was ist Phishing?

Ein Phishing-Angriff liegt vor, wenn ein Krimineller eine E-Mail verschickt, in der er vorgibt, jemand oder etwas zu sein, das er nicht ist, um von den Zielpersonen sensible Daten zu erhalten. Sie verwenden oft gängige Taktiken wie Angst, Neugier oder ein Gefühl der Dringlichkeit, um die Zielperson dazu zu verleiten, einen Anhang zu öffnen oder auf einen bösartigen Link zu klicken.

Was für einen Hacker noch effektiver sein kann, ist ein Spearphishing-Angriff - E-Mails, die spezifische Informationen über die Zielperson enthalten. Angreifer recherchieren ihre Zielperson oft auf Social-Media-Kanälen wie LinkedIn oder sogar auf ihrer Unternehmenswebsite, um die perfekte E-Mail zu erstellen, die sie garantiert zum Klicken bringt.

Verteidigung gegen Phishing-Angriffe

Die erfolgreichsten Anti-Phishing-Programme bestehen aus vier Komponenten: Schutz, Ausbildung, Evaluierung und Berichterstattung. Diese vier Schritte greifen so ineinander, dass Ihre Mitarbeiter als menschliche Schutzschilder genutzt werden, die durch die Technologie aktiviert werden.

Die erste Säule eines jeden Anti-Phishing-Programms besteht darin, Schutz zu bieten, indem man eine Barriere zwischen den nichts ahnenden Computernutzern und den Angreifern errichtet:

- Überwachung und Blockierung des Zugriffs auf bösartige ausgehende DNS-Anfragen, um sicherzustellen, dass Mitarbeiter nicht in der Lage sind, über verdächtige Links auf schlechte Websites zuzugreifen.
- Scan-Tools, die das Verhalten von Dateien überwachen, um sicherzustellen, dass bösartige Dateien nicht durch das Netzwerk gelangen.
- Verwendung von Cloud-Sandboxing-Lösungen, mit denen Sie verdächtige Dateien in einer virtuellen Umgebung öffnen können, um festzustellen, ob sie schädlich sind. Wird festgestellt, dass die Datei bösartig ist, wird sie unter Quarantäne gestellt, um das Netzwerk vor dem Angriff zu schützen.

Außerdem ist es wichtig, Ihre Mitarbeiter regelmäßig über Phishing zu informieren und ihre Klickraten zu bewerten. Es gibt eine Vielzahl von kostenlosen und kostenpflichtigen Schulungsoptionen, einschließlich computergestützter Awareness-Schulungen, Phishing-E-Mail-Simulationsübungen und sogar eines Austausches von Phishing-Schulungsvideos und -Plakaten mit Mitarbeitern. Unternehmen mit gut ausgebildeten Mitarbeitern, die regelmäßig und genau über Phishing-Tests berichten, können eine Anfälligkeitsrate von bis zu 5% aufweisen. [2]

Als Teil der Ausbildung ist es wichtig, dass Ihre Mitarbeiter wissen, wohin sie E-Mails weiterleiten sollen, die sie für verdächtig halten. Dabei geht es häufig um die Weiterleitung der verdächtigen E-Mail an den Helpdesk oder die IT. Diese Phishing-Mails sind Gold wert, wenn es darum geht, zu verstehen, wie und von wem der Angriff durchgeführt wurde. Durch das Sammeln und Studieren von Phishing-Mails können Sie Trends in der Art und Weise erkennen, wie Ihr Unternehmen angegriffen wird (Office 365 Phishing, falsche Rechnungen usw.) und wer die Ziele sind (Vertrieb, F&E, Personal). Der Angreifer hinterlässt Spuren und wir können dies nutzen, um unser Sicherheitsprogramm zu fokussieren und besseren Schutz zu bieten.

1 https://info.wombatsecurity.com/state-of-the-phish

2 https://siliconangle.com/blog/2017/11/30/phishing-attacks-cost-1-6m-average-enterprises-successfully-fighting-back/

Phishing-Schutz von WatchGuard

Jede Organisation hat ihren Anteil an ahnungslosen Computernutzern. Und selbst wenn wahrscheinlich nur ein kleiner Prozentsatz Ihrer Mitarbeiter auf einen unsicheren Link klickt oder einen infizierten Anhang herunterlädt, benötigen Sie die richtigen Sicherheitsdienste. Mit der WatchGuard Total Security Suite können Sie Endbenutzer vor Angriffen schützen und gleichzeitig die Phishing-Ausbildung verbessern.

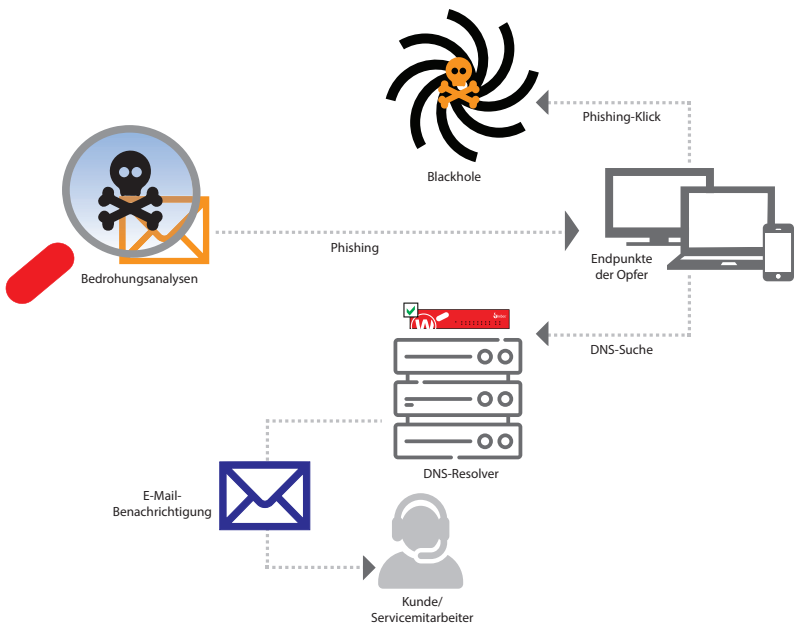
WatchGuard Gateway AntiVirus scannt Dateien und Datenverkehr durch die Firebox, um bekannte Malware und Riskware zu identifizieren. Wenn eine Bedrohung anhand des Signaturabgleichs erkannt wird, wird die Verbindung blockiert oder die Datei entfernt. Dadurch werden die Mitarbeiter davor geschützt, dass bösartige Anhänge im Rahmen eines Phishing-Angriffs den Endbenutzer erreichen können, der auf eine Gelegenheit zum Klicken wartet.

Bei Zero-Day-Bedrohungen, die Ihr Netzwerk erreichen, führt WatchGuard APT Blocker die Datei in einer Cloud-Sandbox-Umgebung aus und analysiert ihr Bedrohungspotenzial. Bösartige Dateien werden unter Quarantäne gestellt, und die Systemadministratoren werden über die Bedrohung informiert.

Aber wie können Sie ahnungslose Computerbenutzer schützen?

WatchGuard DNSWatch nutzt die Erkennung auf DNS-Ebene, um eine zusätzliche Sicherheitsebene zu schaffen, um Malware-Infektionen zu erkennen und zu stoppen. Bösartige DNS-Anfragen werden automatisch erkannt und blockiert und leiten die Benutzer an einen sicheren Ort statt an den Angreifer weiter. Die Personal Touch-Komponente dieses Dienstes liefert detaillierte Berichte über die erkannte und blockierte Infektion.

Das Beste daran ist, dass der Benutzer, der die Anfrage stellt, auf eine sichere Seite weitergeleitet wird, die ergänzende Informationen zu Ihrer bereits absolvierten Phishing-Ausbildung enthält. Ihre Mitarbeiter an ihre Schulung zu erinnern, wenn sie gerade auf einen Link oder eine Anlage geklickt haben, ist der effektivste Weg, dies in Zukunft zu verhindern. Verbunden mit dieser Schulung ist eine Nachricht von Ihnen, die den Benutzer möglicherweise dazu auffordert, Sie anzurufen oder die E-Mail weiterzuleiten, auf die er gerade geklickt hat. Im Moment sind die Benutzer viel empfänglicher für Ratschläge, sodass sich die Möglichkeit bietet, neue Sicherheitsfunktionen wie die Multi-Faktor-Authentifizierung oder die Aktivierung eines Passwortmanagers zu aktivieren.



Über WatchGuard

WatchGuard® Technologies gehört zu den führenden Anbietern im Bereich Netzwerksicherheit. Mehr als 80.000 Unternehmen weltweit vertrauen auf die ausgeklügelten Schutzmechanismen auf Enterprise-Niveau, wobei dank der einfachen Handhabung insbesondere kleine bis mittlere sowie dezentral aufgestellte Unternehmen von WatchGuard profitieren. Neben der Zentrale in Seattle im US-Bundesstaat Washington unterhält WatchGuard Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum. Weitere Informationen finden Sie unter WatchGuard.de.

Wenn Sie mehr über WatchGuard, unsere Werbeaktionen und Updates erfahren möchten, folgen Sie uns auf Twitter @WatchGuard, auf Facebook oder auf unserer Seite auf LinkedIn. Lesen Sie auch unseren InfoSec-Blog Secplicity. Darin wird einfach und nachvollziehbar beschrieben, wie Sie den neuesten Bedrohungen am besten begegnen. Hier geht's zum Blog: www.secplicity.org

Deutschland, Österreich, Schweiz: +49 700 92229333 INTERNATIONALER VERTRIEB +1.206.613.0895 www.watchguard.de

Teilenr. WGCE67085_042018