KURZBESCHREIBUNG DER LÖSUNG

Lassen Sie sich nicht von Hackern erwischen:

Schützen Sie Ihr Unternehmen mit WatchGuard vor Phishing-Angriffen

Einführung

Phishing-Angriffe sind nach wie vor ein wichtiges Thema für mittelständische Unternehmen. Fast 83 % der Unternehmen haben gemeldet, im letzten Jahr 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?

Bei der gängigsten Art von Phishing-Angriff verschickt ein Krimineller eine E-Mail, in der er vorgibt, jemand oder etwas zu sein, der bzw. das er nicht ist, um von den Zielpersonen sensible Daten zu erhalten. Die Angreifer verwenden oft Taktiken, die Angst schüren, Neugier wecken oder ein Gefühl der Dringlichkeit vermitteln, 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 ganz gezielter Spearphishing-Angriff – E-Mails, die spezifische Informationen über die Zielperson enthalten. Angreifer kundschaften ihre Zielpersonen häufig in sozialen Netzwerken wie LinkedIn und Facebook aus, um ein Profil ihres Opfers zu erstellen. Dies hilft ihnen dann dabei, eine maßgeschneiderte Nachricht zu verfassen, die ihre Erfolgschancen verbessert.

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.

Der Schutz vor Phishing erfordert eine mehrschichtige Herangehensweise an die Sicherheit, die darauf abzielt, Benutzer im Internet zu schützen. Diese mehrschichtige Herangehensweise umfasst folgende wichtige Elemente:

- Überwachung und Blockierung bösartiger ausgehender DNS-Anfragen, um sicherzustellen, dass Mitarbeiter nicht in der Lage sind, über verdächtige Links auf bösartige Websites zuzugreifen oder über Command-and-Control-Kanäle zu kommunizieren.
- Scan-Tools, um sicherzustellen, dass bösartige Dateien nicht durch das Netzwerk gelangen, und Endpoint-Security, die Malware erkennen und abwehren kann.
- Cloud-Sandboxing-Lösungen, mit denen Sie verdächtige Dateien in einer emulierten virtuellen Umgebung öffnen können, die einen echten Endpoint nachahmt, um bösartige Absichten zu erkennen.
- Multifaktor-Authentifizierung als Schutz vor Betrug, Identitätswechsel und Diebstahl von Anmeldedaten.

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 gerade einmal 5 % aufweisen.[2]

[1] https://www.proofpoint.com/us/resources/threat-reports/state-of-phish

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-E-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.

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 WatchGuard können Sie Nutzer vor Angriffen schützen und gleichzeitig die Phishing-Ausbildung verbessern.

Schutz vor unüberlegten Klicks

DNS ist die Basis des Internet – es fungiert quasi als Telefonbuch, das Domainnamen in IP-Adressen übersetzt. DNS ermöglicht es dem typischen Benutzer, zu google.com zu navigieren, statt eine numerische IP-Adresse einzugeben. DNS ist fast immer der erste Schritt beim Herstellen einer Verbindung zum Internet und wird von praktisch jedem Gerät verwendet, das eine Verbindung benötigt. Es ist außerdem eines der bevorzugten Werkzeuge von Hackern, die Benutzer austricksen und Datenverkehr zu bösartigen Servern umleiten, indem sie den DNS-Eintrag von legitimen Websites „spoofen".

Als erste Verteidigungsmaßnahme kann jede DNS-Anfrage daraufhin überprüft werden, ob sie bösartig oder legitim ist. So kann verhindert werden, dass sich der riskante Klick eines Nutzers zu einem schwerwiegenden Sicherheitsvorfall entwickelt. Mit den Cloud-basierten DNS-Sicherheitslösungen von WatchGuard werden bösartige DNS-Anfragen automatisch basierend auf aktuellen Bedrohungsinformationen erkannt und blockiert.

WatchGuard bietet zwei Varianten von Schutz auf DNS-Ebene:

- DNSWatch – Das in der Total Security Suite enthaltene DNSWatch bietet Schutz für alle Benutzer, die mit Ihrem Netzwerk verbunden sich und sich hinter einer WatchGuard Firebox befinden.
- DNSWatchGO – Bietet rund um die Uhr Basisschutz vor Phishing und Malware für Benutzer unterwegs.

Beide Produkte bieten Schulungen zur unmittelbaren Förderung des Sicherheitsbewusstseins für Nutzer, wenn diese eine Phishing-Nachricht erhalten. So wird das bereits von Ihnen vermittelte Sicherheitswissen vertieft. 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.

Verteidigung gegen Betrug, Identitätswechsel und Diebstahl von Anmeldedaten

Verloren gegangene Anmeldedaten haben sich als eine der effektivsten Methoden für Hacker erwiesen, in ein Netzwerk einzudringen. Ein Angreifer erhält damit vollen Zugriff auf Unternehmensressourcen und kann sogar die Identität ihres Opfers annehmen, um noch mehr Schaden anzurichten. Angesichts der Verbreitung von Malware zum Stehlen von Anmeldedaten und den viel zu häufig anzutreffenden schlechten Angewohnheiten in Bezug auf die Erstellung von Passwörtern reichen Benutzername und Passwort als Schutz alleine nicht mehr aus.

WatchGuard AuthPoint ermöglicht es Ihnen, den Zugriff auf Ressourcen, Konten und Informationen mit Multifaktor-Authentifizierung zu steuern. AuthPoint fügt im Vergleich zur einfachen Authentifizierung mit Benutzername und Passwort eine zusätzliche Nachweisebene hinzu. Anmeldungen mit AuthPoint erfolgen über ein Mobiltelefon und fordern zur Authentifizierung eines Benutzers etwas an, das Sie wissen (Passwort), haben (Mobiltelefon) und sind (Fingerabdruck, biometrische Daten). AuthPoint wird über die Cloud bereitgestellt und ermöglicht es so, das Risiko schwacher oder gestohlener Passwörter zu beseitigen.

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

Abwehren von Malware, die Anmeldedaten stiehlt

Malware, die Anmeldedaten stiehlt, oder Malware, die versucht, Benutzernamen und Passwörter zu stehlen, kommt häufig zu Einsatz und gehört stets zu den Top 10 der Malware-Bedrohungen, mit denen das durchschnittliche Unternehmen konfrontiert ist.[3] Die Erkennung und Abwehr dieser und anderer Malware-Bedrohungen ist mit einer Signatur-basierten Antivirus-Lösung alleine einfach nicht möglich.

WatchGuard bietet mehrere Sicherheitslösungen zur Erkennung und Abwehr von Malware:

- **Gateway AntiVirus und IntelligentAV** – Wenn ein Benutzer über Ihr Netzwerk verbunden ist, scannen WatchGuard Gateway AntiVirus und das KI-basierte IntelligentAV Dateien und Datenverkehr auf dem Weg durch Ihre Firebox, um Malware und Riskware zu identifizieren. Wenn eine Bedrohung 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.
- **APT Blocker** – Für schwer fassbare und Zero-Day-Bedrohungen, die Ihr Netzwerk erreichen – wie z. B. solche in ganz gezielten Spearphishing-Angriffen – bietet WatchGuard APT Blocker eine zusätzliche Schutzschicht. WatchGuard APT Blocker führt die Datei in einer Cloud-Sandbox aus und analysiert ihr Bedrohungspotenzial. Bösartige Dateien werden unter Quarantäne gestellt, und die Systemadministratoren werden über die Bedrohung informiert.
- **ThreatSync** – ThreatSync ist die Cloud-basierte Engine von WatchGuard zur Korrelation und Bewertung von Bedrohungen. Sie verbessert die Erkennung von und Reaktion auf Gefahren innerhalb der gesamten Umgebung vom Netzwerk bis zum Endpunkt. Wenn Malware erkannt wird, grenzt ThreatSync den Host ab, stellt die Datei unter Quarantäne, bricht zugehörige Prozesse ab und löscht den Registrierungsschlüssel.

[3] https://www.watchguard.com/wgrd-about/press-releases/new-security-research-reveals-password-inadequacy-top-threat-need-mfa

Über WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Netzwerksicherheit, sicheres WLAN, Multifaktor-Authentifizierung und Network Intelligence. Beinahe 10.000 Vertriebspartner und Dienstanbieter im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Dienste des Unternehmens, um mehr als 80.000 Kunden zu schützen. Die Philosophie von WatchGuard ist es, Sicherheit auf Enterprise-Niveau für Unternehmen jeder Größenordnung und Art zu realisieren. Das macht WatchGuard insbesondere für mittelständische und sowie dezentral aufgestellte Unternehmen zum idealen Anbieter. 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

Mit diesem Dokument werden keine ausdrücklichen oder implizierten Gewährleistungen gegeben. Änderungen vorbehalten. Zukünftige Produkte, Funktionen oder Funktionalitäten werden zur Verfügung gestellt, sofern und sobald sie verfügbar sind. ©2019 WatchGuard Technologies, Inc. Alle Rechte vorbehalten. WatchGuard, das WatchGuard-Logo, Firebox, DNSWatch, IntelligentAV und ThreatSync sind Marken bzw. eingetragene Marken von WatchGuard Technologies, Inc. in den USA und/oder anderen Ländern. Alle weiteren Markennamen sind das Eigentum ihrer jeweiligen Inhaber. Teilenr. WGCE67085_093019