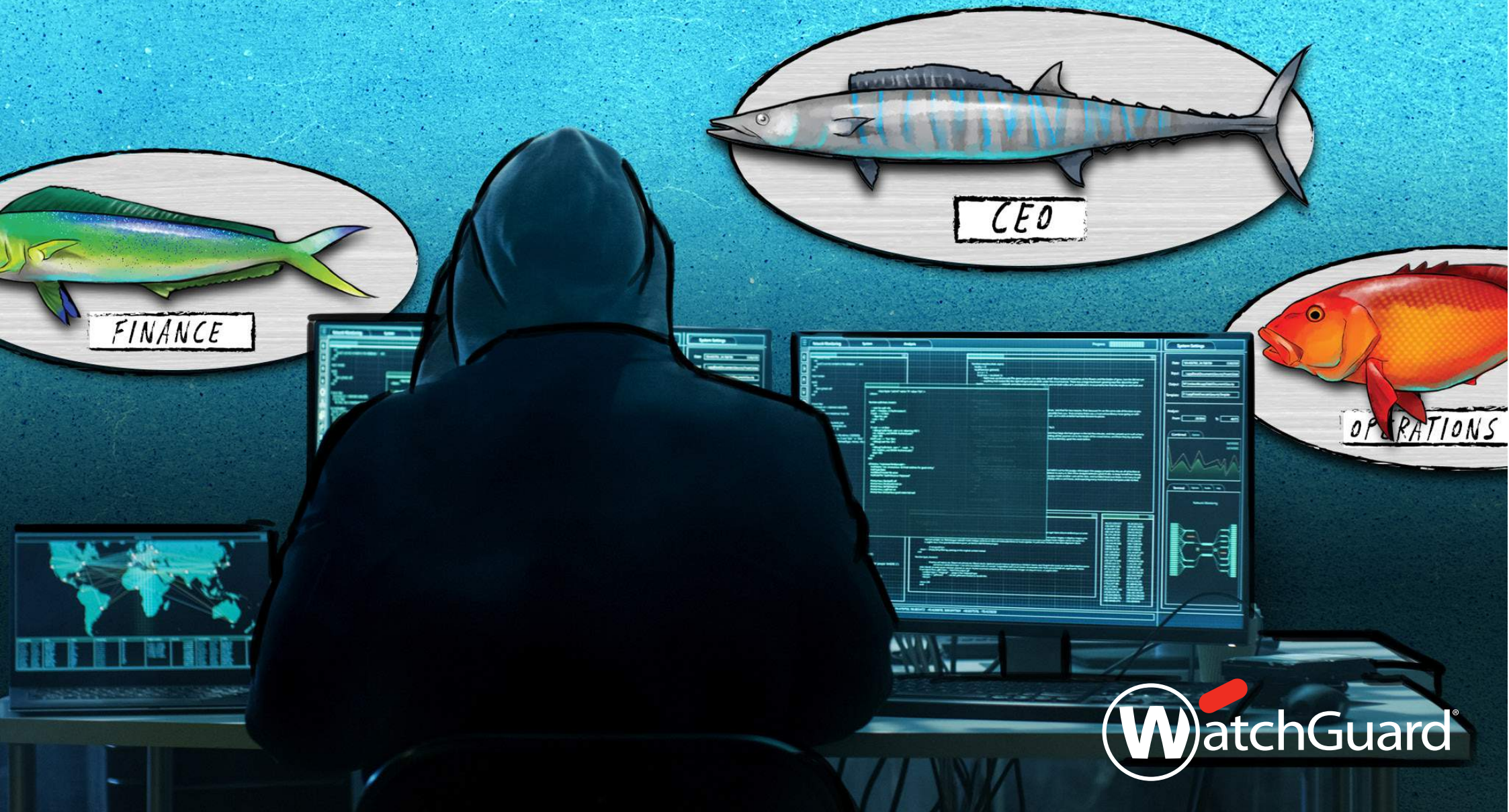
TROPHY PHISHING

Schützen Sie sich vor Hackern



WatchGuard®

INHALTSVERZEICHNIS

WatchGuard®

EINFÜHRUNG

Die weite Verbreitung von Phishing-E-Mails hat einen einfachen Grund – **sie sind von Erfolg gekrönt.**

Nutzer klicken immer noch auf Links und laden Dateien herunter. Warum also sollten Hacker damit aufhören, sie zu senden?

Hacker warten auf den nächsten großen Fisch an der Angel und darauf, dass Sie anbeißen. Dieses eBook behandelt die Hauptziele, auf die Hacker es abgesehen haben, den Köder und die Vorgehensweisen, die sie nutzen, sowie Verteidigungslösungen, die erforderlich sind, um Ihre Mitarbeiter und Kunden zu schützen.

90 %

aller Angriffe beginnen mit einer Phishing-E-Mail.

76 %

der Unternehmen haben gemeldet, im letzten Jahr Opfer eines Phishing-Angriffs geworden zu sein.

(Wombat Security State of the Phish)

LIEBLINGSMETHODEN VON HACKERN

Spear Phishing

Spear Phishing-Angriffe sind deutlich gezielter. Der Hacker muss über sein Opfer informiert sein, bevor er die perfekte E-Mail entwerfen kann.

Executive Whaling

Zielt auf Führungskräfte und Administratoren ab; der Schwerpunkt liegt darauf, Geld von Konten abzuschöpfen oder vertrauliche Daten zu stehlen.

Phishing

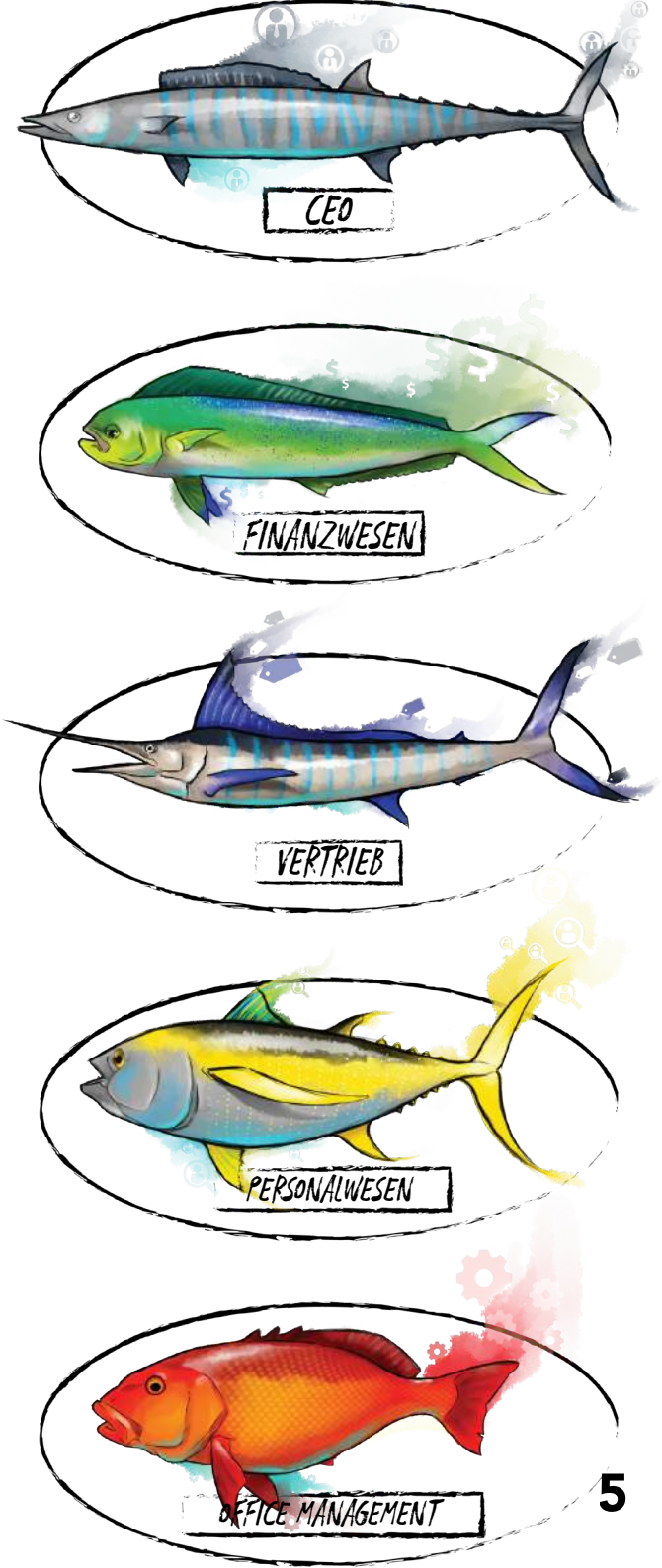
Phishing-E-Mails erfordern einen umfassenden Sweep-Ansatz, um Benutzer anzugreifen und auf sensible Informationen zuzugreifen.

Social Engineering

Eine Vorgehensweise, um Daten von Social-Media-Seiten zu sammeln und so Einblicke zur Gestaltung von E-Mails zu erhalten.

HAUPTZIELE IN UNTERNEHMEN

Jeder Bereich in Ihrem Unternehmen ist ein Fisch, der einem Hacker an den Haken gehen kann. Die beste Möglichkeit, sich zu schützen, ist, den Köder zu kennen, den der Hacker verwendet, und Ihre Mitarbeiter so zu schulen, dass sie diese Bedrohungen erkennen, wenn sie mit ihnen in ihrem Posteingang konfrontiert sind. Erfahren Sie mehr über die Top 5-Ziele in Ihrem Unternehmen und die Köder, die Hacker nutzen.



WatchGuard

ZIEL: CEO

Es ist sehr einfach für Hacker, Informationen über ein Unternehmen zu sammeln. Wenn sie auf der Unternehmensseite oder Social-Media-Seiten wie LinkedIn suchen, finden sie problemlos die Namen und E-Mail-Adressen der Mitarbeiter aus der Finanz- oder Rechtsabteilung. Eine einfache E-Mail mit einer imitierten E-Mail-Adresse von einem Mitarbeiter der Rechtsabteilung und einer Betreffzeile zu einem drohenden Gerichtsverfahren sorgt dafür, dass selbst ein CEO auf jeden beliebigen Link klickt.

CEO

Köder:

Von der Rechtsabteilung: „Wir werden verklagt.“

ZIEL: FINANZWESEN

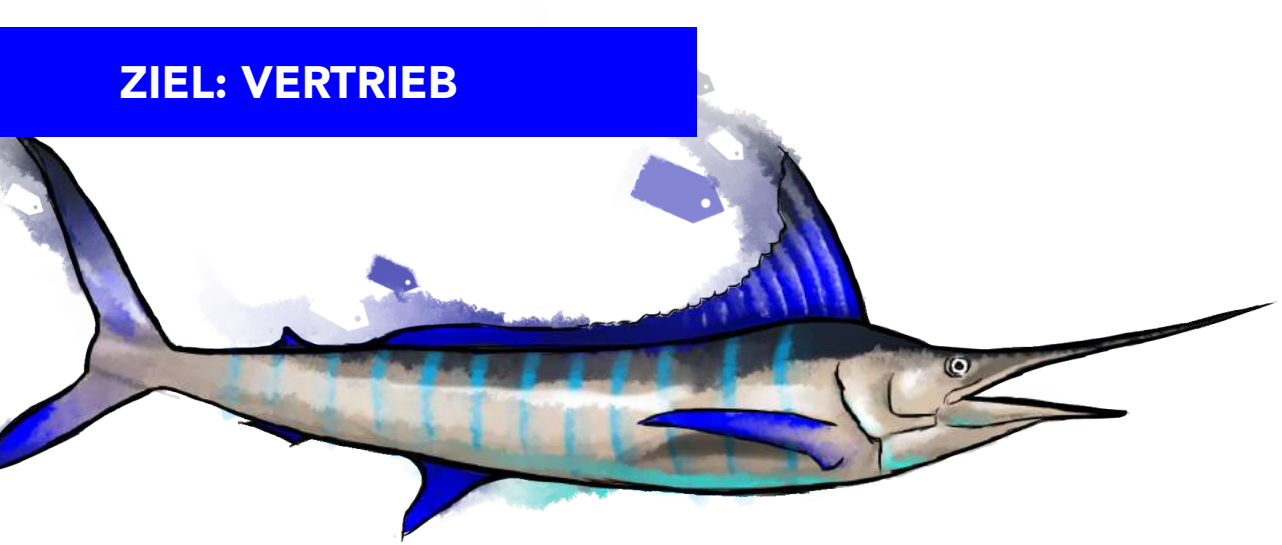
Wenn der CEO Sie bittet, etwas zu tun, ist es in der Regel in Ihrem Interesse, die Aufgabe auszuführen (in angemessenem Rahmen). Warum sollten Sie es also als Mitarbeiter der Finanzabteilung hinterfragen, wenn der CEO Sie bittet, Geld zu überweisen? Hacker wissen dies. Daher imitieren sie oft eine E-Mail vom Chef, damit der Mitarbeiter schnell reagiert. Wenn dieser den Köder schluckt und auf den Link für die Überweisung klickt, übermittelt er dem Hacker direkt Kontoinformationen.

FINANZWESEN

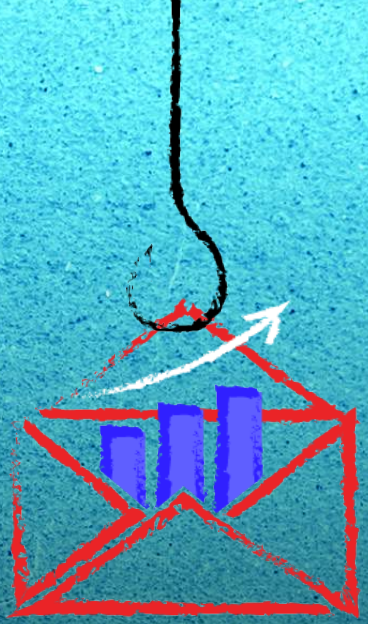
Köder:

Vom CEO:
„ÜberweisenSie bitte diesen Betrag!“

ZIEL: VERTRIEB



Über Vertriebsmitarbeiter werden E-Mails und Telefonanrufe von potenziellen und bestehenden Kunden abgefangen. Sie reagieren sofort auf jede E-Mail, die sie erhalten und zum nächsten großen Deal führen könnte. Es ist kinderleicht für Hacker, die Daten von Vertriebsmitarbeitern zu ermitteln (beispielsweise über LinkedIn), und sie können relativ sicher sein, dass alle E-Mails, die sie senden, zumindest geöffnet werden. Der Diebstahl von Anmeldedaten dieser Benutzer bietet Zugriff auf Kundenlisten, Preistabellen und vertrauliche Informationen zu Geschäftsabschlüssen. Zudem sind weitere Phishing-Angriffe auf Mitarbeiter der Finanz-, Management- und Account-Teams möglich, die den Nachrichten von Vertriebsmitarbeitern vertrauen. Bei dieser Art des Phishing gehen viele Fische an den Haken!



VERTRIEB

Köder:

Von einem potenziellen Kunden:
„Ich bin an einem Geschäftsabschluss interessiert!“

ZIEL: PERSONALWESEN

Unabhängig von den Standardverfahren erhalten Mitglieder der Personalabteilung in der Regel Lebensläufe per E-Mail. Sie öffnen zwar wahrscheinlich nicht jede E-Mail, Hacker wissen jedoch, dass das Team der Personalabteilung E-Mails bei entsprechender Gestaltung öffnet und Anhänge herunterlädt. Dann hat der Hacker Zugriff auf sensible Mitarbeiterinformationen, einschließlich Sozialversicherungsnummern, Adressen, Telefonnummern und sogar die Daten von Notfallkontakten. Oder auf Gesundheits- oder Rentendaten, was ihm beim nächsten Hack gegen Ihr Unternehmen hilft.

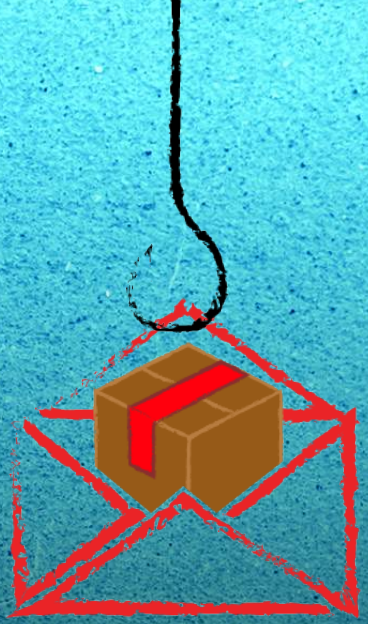
PERSONAL-WESEN

Köder:

Von einem zukünftigen Mitarbeiter:
„Stellen Sie mich ein!“

ZIEL: FACILITY MANAGEMENT

Versandanhänge für UPS- und DHL-Bestellungen sind eine weitere gängige Methode, wie Angreifer Zugriff zu Ihrem Unternehmen erhalten. Die Teammitglieder des Office Managements (oder selbst andere Mitarbeiter, die oft Sendungen empfangen) erhalten diese Arten von E-Mails mit einem Anhang, der wichtige Versandinformationen enthält. Betreffzeilen wie „verloren gegangenes Paket“ oder „Problem mit der Lieferung“ wecken mit Sicherheit ihre Aufmerksamkeit. Hacker wissen, dass E-Mails mit großer Wahrscheinlichkeit geöffnet, Links geklickt oder Anhänge heruntergeladen werden, selbst wenn keine Sendung erwartet wird.



FACILITY MANAGEMENT

Köder:

Von einem Versandunternehmen:
„Ihr Paket ist verloren gegangen“

SICHERHEITSLÖSUNGEN

Sie können sich vor diesen Phishing-Angriffen in ruhigere Gewässer flüchten. Wenn Sie über die richtigen Verteidigungsmechanismen verfügen, sind Ihre Mitarbeiter und Kunden geschützt. WatchGuard bietet ein robustes Portfolio an Sicherheitslösungen, um dafür zu sorgen, dass Sie auf jeder Ebene und gegen jeden Angriffstyp geschützt sind.

WATCHGUARD TOTAL SECURITY SUITE

Mehrstufiger Schutz im gesamten Unternehmen.

Oft sind verschiedene Bereiche Ihres Unternehmens auf unterschiedliche Weise von Phishing-Angriffen betroffen. Dies erfordert Schutz auf jeder Ebene Ihres Unternehmens vor bekannten, unbekannten und sogar versteckten Bedrohungen. WatchGuard Total Security Suite schützt Ihr Unternehmen vor Phishing-Angriffen, egal, ob sie bösartige Links oder Anhänge beinhalten. Im Folgenden erfahren Sie wie:

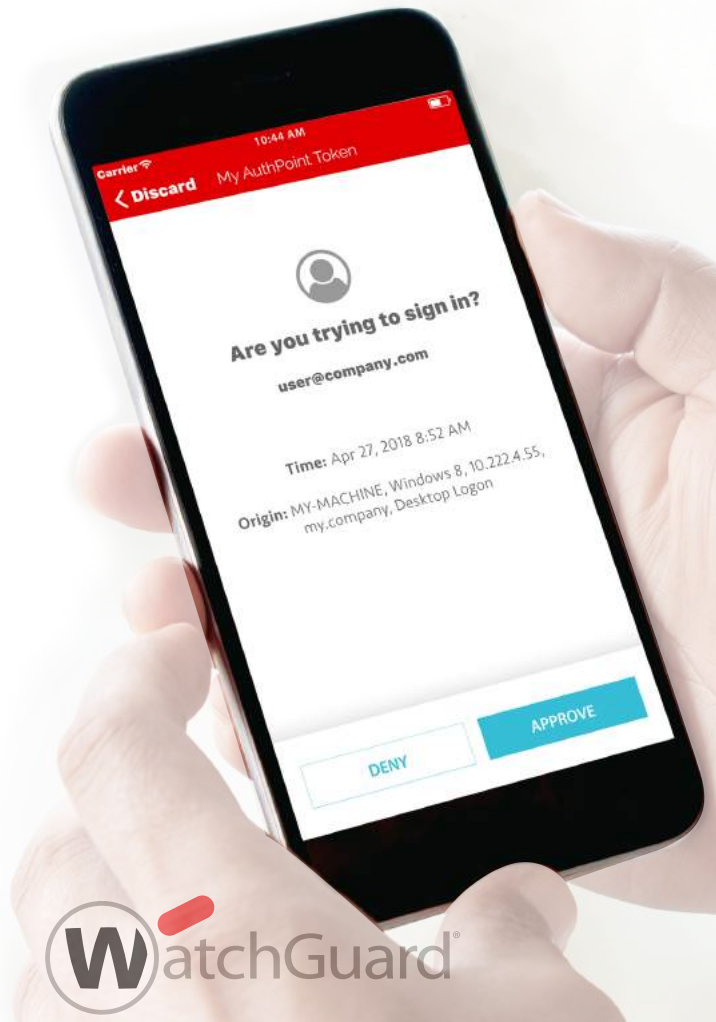
WatchGuard DNSWatch überwacht den DNS-Traffic und blockiert den Zugriff auf bekannte bösartige Websites. Wenn ein Benutzer eine Phishing-E-Mail erhält und auf den Link klickt, wodurch er auf eine bösartige Website verwiesen wird, schreitet DNSWatch ein, um sicherzustellen, dass der Benutzer nicht auf die gefährliche Website zugreift. Als Bonus leitet dieser Service Benutzer auf eine sichere Seite um, die sie erneut auf die Warnsignale von Phishing-E-Mails hinweist.

WatchGuard APT Blocker untersucht verdächtige Dateien im Netzwerk und Host in einer virtuellen Umgebung, um festzustellen, ob sie bösartigen Inhalt enthalten. Ist dies der Fall, werden sie in Quarantäne gestellt. Dies stellt sicher, dass alle Phishing-E-Mails mit Anhängen vor dem Öffnen auf dem Benutzergerät untersucht und als bösartig identifiziert werden.

WatchGuard Threat Detection & Response (TDR) bietet Schutz vor Ransomware-Angriffen. Wenn ein Mitarbeiter eine Phishing-E-Mail mit Ransomware erhält, erkennt die Host Ransomware Prevention (HRP)-Komponente von TDR die Bedrohung und wehrt sie ab, bevor die Dateiverschlüsselung stattfindet.

WATCHGUARD AUTHPOINT

Schutz vor dem Diebstahl von Anmeldedaten



Wenn ein Hacker Zugriff zu Ihrem Unternehmen erhält und eine Möglichkeit findet, Anmeldedaten zu stehlen, müssen Sie sicherstellen, dass er trotz der Anmeldedaten nicht weit kommt. Multifaktor-Authentifizierung (MFA) erfordert ein Passwort, eine biometrische Verifizierung oder ein Security Token für den Zugriff.

WatchGuard AuthPoint™ trägt zum einen dazu bei, das mit dem Verlust oder Diebstahl von Anmeldedaten einhergehende Risiko von Datensicherheitsverletzungen zu reduzieren. Gleichzeitig erfolgt die Bereitstellung vollständig über die Cloud, was die Einrichtung und Verwaltung selbst bei begrenzten personellen Möglichkeiten stark vereinfacht. AuthPoint geht über die herkömmliche Zwei-Faktor-Authentifizierung (2FA) hinaus, indem innovative Methoden der positiven Benutzeridentifizierung genutzt werden – wie beispielsweise bei unserem Ansatz, die „DNA" des Smartphones zu überprüfen. Unser umfangreiches Ökosystem aus Integrationen von Drittanbietern bedeutet zudem, dass Kunden AuthPoint-Schutz durchgängig einsetzen können, um auf das Netzwerk, VPNs, Cloud-Anwendungen usw. zuzugreifen – wo immer es gerade nötig ist. WatchGuard AuthPoint verhindert, dass Hacker, die Passwörter gestohlen haben, auf ihre Daten und Anwendungen zugreifen.

SCHÜTZEN SIE IHR UNTERNEHMEN • SCHÜTZEN SIE IHRE RESSOURCEN • SCHÜTZEN SIE IHRE MITARBEITER

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.

Globale Hauptgeschäftsstelle USA
Tel: +1.800.734.9905
E-Mail: sales@watchguard.com

Hauptgeschäftsstelle Mitteleuropa
Tel: +49 (700) 9222 9333
E-Mail: germanysales@watchguard.com

Hauptgeschäftsstelle APAC-Ozeanien Singapur
Tel: +65.3163.3992
E-Mail: inquiry.sea@watchguard.com

Teilenr. WGCE67116_080118