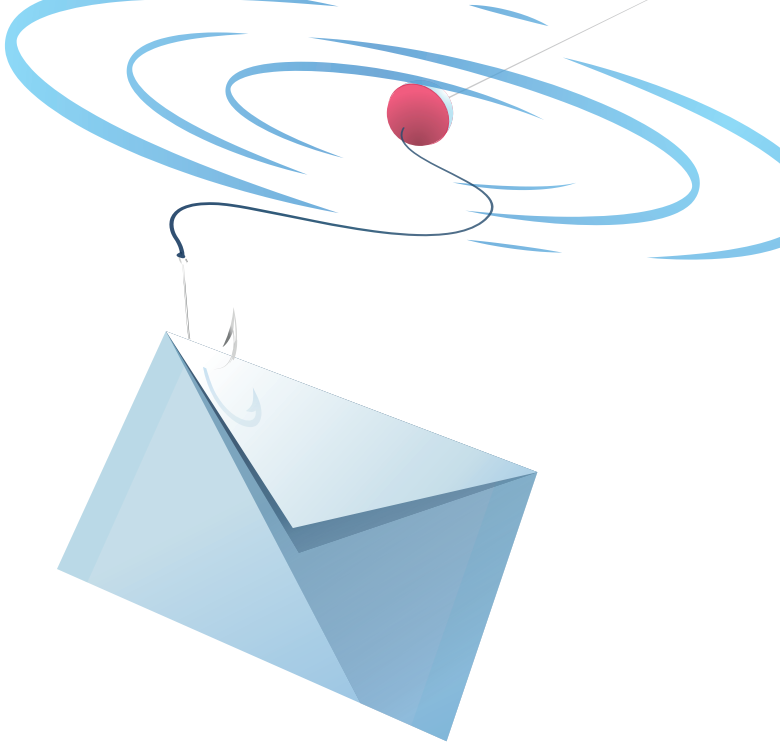
SOPHOS
Cybersecurity made simple.



Phishing: Lassen Sie sich nicht ködern

Phishing ist ein lukratives Geschäft. Gehen Sie Angreifern nicht an den Haken.

Im vergangenen Jahr haben Phishing-Angriffe stark zugenommen, da Angreifer ihre Strategien immer weiter ausfeilen und erfolgreiche Angriffstypen untereinander austauschen. Insbesondere Malware-as-a-Service-Angebote im Dark Web wurden vermehrt genutzt, um die Effizienz und das Volumen von Angriffen zu steigern. 41 % aller Unternehmen verzeichnen bereits täglich Phishing-Angriffe.[1]

In diesem Paper beleuchten wir die Entwicklung von Phishing in den letzten Jahren und erklären, in welchen Formen Phishing-Angriffe auftreten und ablaufen. Außerdem zeigen wir, was wirklich gegen Phishing hilft: eine mehrschichtige Abwehrstrategie, bei der leistungsstarke Sicherheitstechnologien mit effektiven Maßnahmen zur Mitarbeiteraufklärung kombiniert werden.

Sophos-Whitepaper Juni 2018

Mehr als lästiger Spam

Bisher wurde Phishing oft mit Online-Banking-Betrügereien in Verbindung gebracht: Über eine E-Mail locken Kriminelle Sie auf eine Website, die der Anmeldeseite Ihrer Bank zum Verwechseln ähnlich sieht. Hier geben Sie Ihre Zugangsdaten in ein gefälschtes Formular ein und übermitteln die Daten damit direkt an die Hacker.

Hinter Phishing verbirgt sich jedoch viel mehr als gefälschte Bank-Webseiten und Links zu Wunderpillen oder Paketzustellungen: Bei Phishing-Angriffen geht es darum, Ihnen einen Köder vor die Nase zu halten und darauf zu warten, dass Sie „anbeißen" und für die Angreifer wertvolle Informationen liefern.

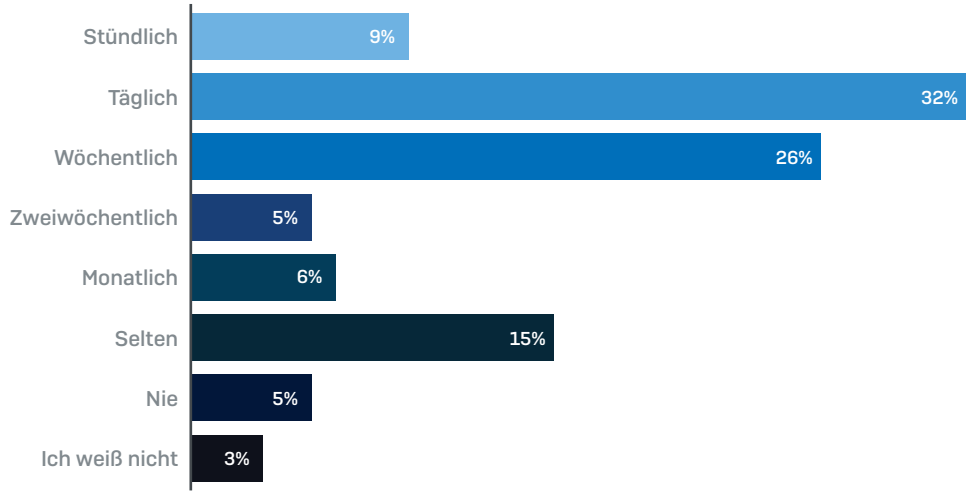
93%
aller Datenpannen gehen von Phishing aus[2]

Phishing ist ein lukratives Geschäft

In den letzten Jahren haben Phishing-Angriffe drastisch zugenommen – nicht zuletzt dank Dark Web Services, die kostenlose Phishing-Kits und Phishing-as-a-Service anbieten. Selbst technisch komplett unversierte Angreifer können auf diese Weise komplexe Malware einsetzen, die von echten Cybercrime-Profis entwickelt wurde.

Phishing-Angriffe sind damit mittlerweile alltäglich geworden. 41 % der IT-Mitarbeiter verzeichnen mindestens einmal täglich einen Phishing-Angriff.[3]

Häufigkeit von Phishing-Angriffen

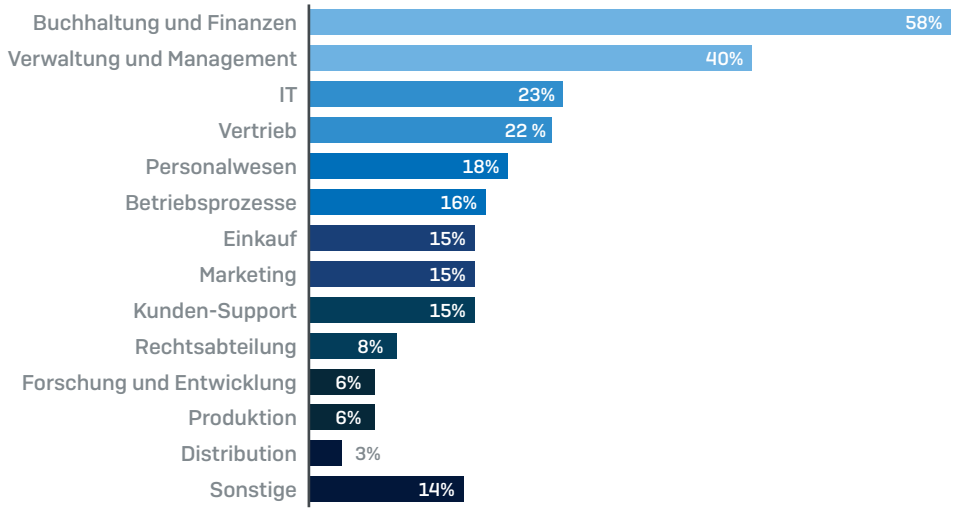


Phishing-Angriffe sind vor allem finanziell motiviert. Aus dem Verizon Data Breach Investigations Report 2018 geht hervor:

- **59 % der Angriffe sind finanziell motiviert.** Dabei erschleichen sich Cyberkriminelle unter anderem Benutzerdaten, die sie dann im Dark Web anbieten. Systeme werden mit Ransomware infiziert oder Hacker geben sich als Führungskräfte aus, um Mitarbeiter dazu zu bringen, Gelder zu transferieren oder wertvolle Daten preiszugeben.
- **41 % der Angriffe haben zum Ziel, sich Zugriff auf Systeme zu verschaffen.** Dabei verschaffen sich die Angreifer beispielsweise Zugang zu Unternehmensnetzwerken, um Daten zu stehlen oder um die Kontrolle über Systeme zu übernehmen.

Da Cyberkriminelle sich in den meisten Fällen finanzielle Vorteile verschaffen möchten, überrascht es wenig, dass sie es besonders auf Mitarbeiter mit Zugriff auf Unternehmensfinanzen abgesehen haben. Dabei werden diese dazu gebracht, Gelder auf von den Tätern kontrollierte Bankkonten zu überweisen. Mitarbeiter, die Unternehmensprozesse verwalten, sowie die IT stehen ebenfalls im Visier von Phishing-Angreifern. So werden Unternehmen immer häufiger Opfer von Ransomware und Erpressungsversuchen.[4]

Am häufigsten von Phishing-Angriffen betroffene Abteilungen



Steigerung von Effizienz und Produktivität

Momentan sind 89 % aller Phishing-Angriffe auf organisiertes Verbrechen zurückzuführen. Da Phishing mittlerweile wie jede andere Geschäftstätigkeit abläuft, haben sich die Angriffsstrategien auf eine Weise verändert, die betriebswirtschaftlichen Grundprinzipien folgt: Wie lassen sich Arbeitsabläufe vereinfachen und effizienter gestalten und wie kann eine Expandierung realisiert werden, um den Umsatz zu steigern?

89%
aller Phishing-Angriffe sind auf organisiertes Verbrechen zurückzuführen

Folglich haben sich effizientere Methoden zur Verbreitung von Angriffen entwickelt – mit On-Demand-Phishing-Services, sofort einsatzbereiten Phishing-Kits und neuen Wellen von Angriffstypen wie Business Email Compromise (BEC), die mittels Social Engineering hochwertigere Ziele ins Visier nehmen.

Kostenlose Phishing-Kits

Wünschen Sie sich auch, dass sich Ihre Produkte so gut verkaufen wie das neueste iPhone? Die meisten von uns „leihen" sich gerne Ideen von Freunden, Kollegen oder Wettbewerbern aus, wenn wir feststellen, dass diese Ideen funktionieren, oder? Die Phishing-Community ist da keine Ausnahme. Tatsächlich ist sie sogar besser organisiert.

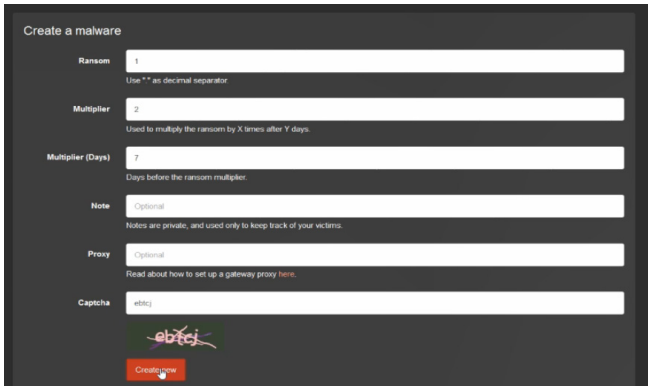
Betrachtet man das Phishing-Ökosystem näher, fällt auf, dass eine große Anzahl von Akteuren Angriffe verüben, jedoch nur sehr wenige Phishing-Angreifer in der Lage sind, selbst ein Phishing-Kit zu entwickeln. Daher werden Phishing-Kits nun vielfach in Dark-Web-Foren und auf Marktplätzen zum Download angeboten. Diese Kits enthalten alles, was ein Angreifer braucht, um gewinnbringende Angriffe zu starten: E-Mails, Webseiten-Code, Bilder usw.

Die Autoren der Kits schlagen Profit aus dem Inumlaufbringen ihrer Kits an weniger versierte Benutzer und können auf zweierlei Art verdienen: Entweder bieten sie kostenlose Kits an, die Backdoors enthalten, mit denen sie alle Daten, die vom Absender gesammelt werden, auch selbst erfassen können, oder sie bieten die Kits zum Kauf an. Besonders teure Kits verfügen mittlerweile sogar über Features wie Bedienfelder zur Nachverfolgung von Kampagnen.

Attacks-as-a-Service

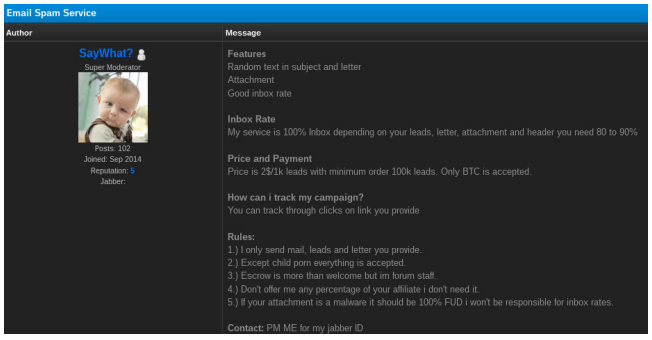
Inzwischen müssen Angreifer nicht einmal mehr selbst Malware entwickeln oder E-Mails verschicken können. As-a-Service- und Pay-as-you go-Lösungen haben Einzug in die meisten Online-Service-Technologien erhalten und Phishing bildet hier keine Ausnahme – das Angreifern zur Verfügung stehende Service-Angebot wächst stetig:

- **Ransomware-as-a-Service** ermöglicht Benutzern, einen Online-Account anzulegen und ein kurzes Webformular auszufüllen, in dem u. a. der Mindestlösegeldbetrag und Zusatzgebühren bei verspäteter Bezahlung festgelegt werden können. Der Service-Anbieter streicht dann einen gewissen Prozentsatz jeder Lösegeldzahlung für sich ein und bietet dem Benutzer ggf. einen Preisnachlass an, wenn dieser den Malware-Code in neue Sprachen übersetzen kann oder das Angriffsvolumen ein bestimmtes Niveau übersteigt.



Satan-Ransomware – ein Online-Service, mit dem Kriminelle innerhalb von Minuten ihren eigenen Virus entwickeln und Windows-Systeme infizieren können.

- **Phishing-as-a-Service** ermöglicht Benutzern, gegen entsprechende Bezahlung Phishing-Angriffe in ihrem Auftrag versenden zu lassen – über globale Botnets, um verdächtige IP-Bereiche zu vermeiden. Benutzern wird sogar garantiert, dass sie nur für tatsächlich zugestellte E-Mail-Nachrichten zahlen müssen, ähnlich wie bei seriösen E-Mail-Marketing-Services.



Beispiel für Spam-Versand-Service mit Preisen pro an aktiven Posteingang gesendeter E-Mail inklusive Tracking für Klickraten.

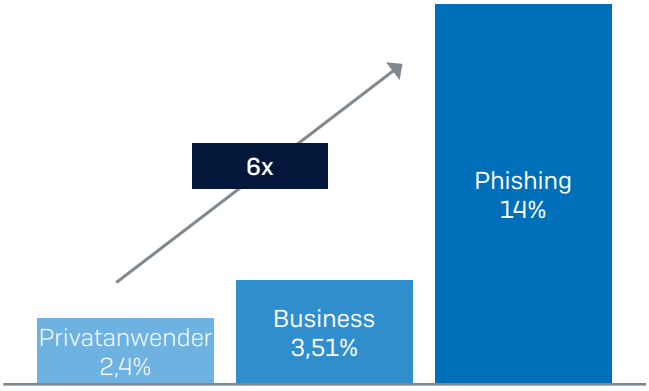
Solche Services haben wie bereits beschrieben zu einer Explosion von Phishing-Angriffen geführt, da jeder beliebige Angreifer nun auch ohne technisches Know-how in der Lage ist, Angriffe zu starten.

Wie Marketing, nur besser

Besonders beunruhigend: Diese Dark-Web-Services sparen Angreifern Zeit, sodass diese sich noch stärker darauf konzentrieren können, ihre Kampagnen noch perfider zu machen und ihre Strategien weiter zu optimieren.

Mit diesen Strategien erzielen die Angreifer Ergebnisse, bei denen die meisten Vertriebs- und Marketing-Teams vor Neid erblassen würden: Tatsächlich werden Phishing-E-Mails derzeit mit sechsmal höherer Wahrscheinlichkeit geöffnet als reguläre Marketing-E-Mails.5

Klickraten von Phishing-E-Mails



Der Zeitgewinn für Forschung und Entwicklung auf Seiten der Angreifer hat Phishing-Bedrohungen einen neuen Entwicklungsschub beschert. Business Email Compromise (BEC)-Angriffe nehmen drastisch zu – eine gefährliche neue Form von Phishing-Angriffen, die Angreifern noch höhere Einnahmen verspricht, indem hochwertige Unternehmensziele ins Visier genommen werden.

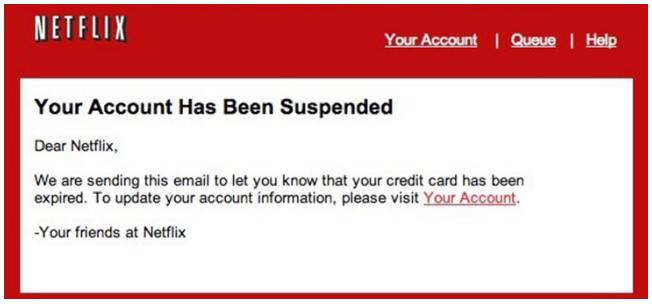
Wie Phishing funktioniert

Wie bereits erwähnt, verbirgt sich hinter Phishing mehr als nur gefälschte Bank-E-Mails und Benachrichtigungen über Paketzustellungen. Es geht darum, Benutzer dazu zu verleiten, Angreifern etwas für sie Wertvolles zu übermitteln. Was als simples „Phishing" begann, hat sich mittlerweile in drei „Angriffszweige" unterteilt: klassisches Phishing, Massen-Phishing und Spear-Phishing sowie „Business Email Compromise"-Angriffe, eine Untergruppe von Spear-Phishing.

Massen-Phishing

Diese Angriffe sind im Wesentlichen opportunistisch. Sie nutzen den Markennamen eines Unternehmens, um die Kunden der Marke auf gefälschte Websites zu locken. Hier werden die Kunden dazu gebracht, ihre Kreditkartennummern, Zugangsdaten und andere persönliche Informationen preiszugeben. Diese Daten werden von den Angreifern dann gewinnbringend weiterverkauft.

- Nimmt Einzelpersonen ins Visier
- In der Regel Konsumenten von Produkten oder Dienstleistungen einer Marke
- Unpersönlicher, explosionsartiger Massenversand
- Schwerpunkt auf Diebstahl personenbezogener Daten (z. B. Zugangsdaten)

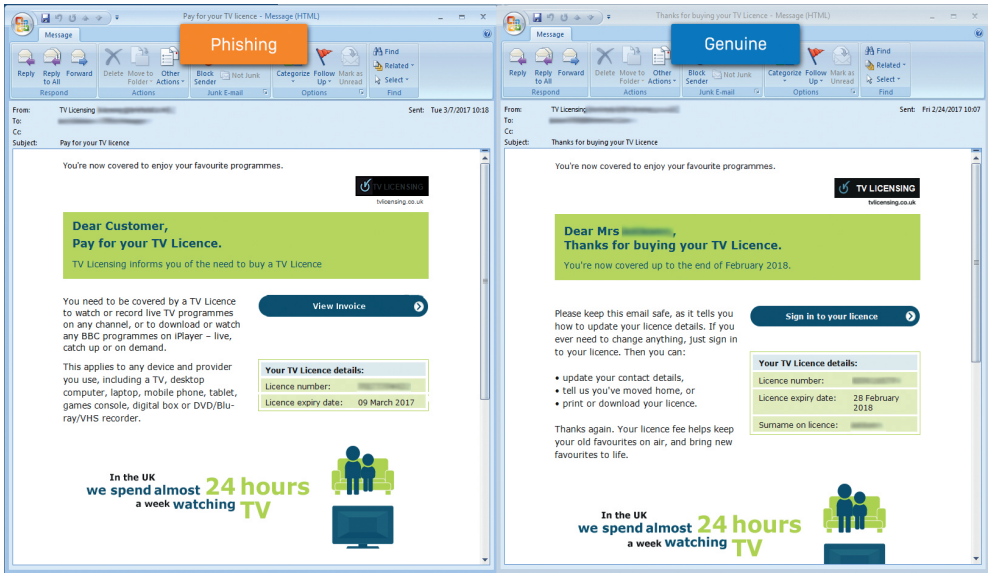


Ein typisches Beispiel für Massen-Phishing

Spear-Phishing

Beim Spear-Phishing geben E-Mails vor, von einem bestimmten Absender oder aus vertrauter Quelle zu stammen. Sie werden gezielt an ausgewählte Einzelpersonen in Unternehmen gesendet und sollen die Empfänger zu konkreten Handlungen bewegen, z. B. dazu, Geld auf ein Bankkonto zu überweisen.

- Nehmen gezielt bestimmte Unternehmen ins Visier
- In der Regel eine Einzelperson oder bestimmte Gruppe in einem Unternehmen
- Gefälschte (täuschend echt erscheinende) E-Mail-Adressen, um Benutzer zu täuschen
- Geben sich als vertraute Quellen und oder Führungskräfte aus



Echte und Phishing-E-Mail sind sich oft zum Verwechseln ähnlich, wie in diesem überzeugenden „UK TV License"-Beispiel.

Spear-Phishing-Angriffe nehmen immer mehr zu, und Cyberkriminelle gehen dabei immer gewiefter und effektiver vor. Laut einer aktuellen Umfrage unter 330 IT-Experten wurden bereits bei 55 % der Befragten die Identitäten von Führungskräften für Spear-Phishing-Angriffen missbraucht.[6]

Mittlerweile werden bei noch gezielteren Untergruppen von Spear-Phishing mittels Social Engineering Zieldaten gesammelt und die Konversionen erhöht. Diese sind als „CEO Fraud", „Whaling" und seit neuestem als „Business Email Compromise (BEC)" bekannt.

Business Email Compromise

Bei „Business Email Compromise"-Angriffen werden keine Absender-Adressen gefälscht, sondern E-Mail-Accounts von Mitarbeitern kompromittiert. Solche Angriffe sind für Enduser weit schwerer zu erkennen.

- Nimmt gezielt Unternehmensdaten, Zugangsdaten und Finanzen eines Unternehmens ins Visier
- Nachdem Angreifer ein Unternehmen ins Visier genommen haben, machen sie Einzelpersonen in diesem Unternehmen ausfindig, indem sie Daten von Websites wie Facebook und LinkedIn sammeln. Auf Grundlage dieser Informationen erstellen sie anschließend individuell zugeschnittene, täuschend echt wirkende Phishing-E-Mails.
- Der Angreifer isoliert anschließend diese Einzelperson, indem er vorgibt, dass die E-Mail-Nachricht von einem hochrangigen Mitarbeiter stammt, und erhöht den Druck, indem er die Nachrichten vermehrt kurz vor Feierabend oder am Ende der Arbeitswoche verschickt.

Im Gegensatz zu Massen- oder Spear-Phishing-Kampagnen zielen diese Angriffe in der Regel auf die Finanzen eines Unternehmen ab. Und anders als bei Angriffen aus den vergangenen Jahren, bei denen potenziellen Opfern PDF-Anhänge mit Empfänger-Kontoverbindungen geschickt wurden, werden solche Informationen bei BEC-Angriffen zurückgehalten, bis eine positive Antwort vom Opfer eingegangen ist. Schließlich ist das betrügerische Konto bei einem Angriff der größte Kostenfaktor für den Angreifer und es besteht immer die Gefahr, dass ein Empfänger den Betrug bemerkt und ihn an die Behörden meldet.

BEC-Angriffe sind meist schwerer zu erkennen, weil Angreifer die Phishing-E-Mails in diesem Fall über kompromittierte E-Mail-Accounts versenden.

Anzeichen erkennen

Vielleicht kommt Ihnen Folgendes bekannt vor: Sie erhalten eine gefälschte Rechnung über ein Flugticket, das angeblich mit Ihrer Kreditkarte bezahlt wurde, und werden aufgefordert, eine Datei im Anhang zu öffnen, falls Sie der Zahlung widersprechen möchten. Hierbei handelt es sich um Massen-Phishing.

30%
aller Phishing-Mails werden geöffnet

Genau wie die angeblich von Paketdiensten stammenden Nachrichten, in denen behauptet wird, dass Sie Ihre Firmenadresse bestätigen müssen, damit Ihnen eine Sendung zugestellt werden kann.

Spear-Phishing ist weitestgehend identisch, der Unterschied besteht lediglich darin, dass der „Köder" spezifischer ist. Oder, im Fall von BEC-Angriffen, enthält die Nachricht eventuell keine schädlichen Links oder Anhänge, sondern fordert Sie dazu auf, einen Geldbetrag zu überweisen, um die E-Mail glaubwürdiger erscheinen zu lassen.

Generell können Sie davon ausgehen: Wenn eine betrügerische E-Mail mit „Sehr geehrter Kunde," beginnt, handelt es sich um Phishing. Wenn Sie mit Ihrem Namen angesprochen werden, handelt es sich um Spear-Phishing. Und sollte die Nachricht von der echten E-Mail-Adresse Ihres Chefs stammen, haben Sie es mit einem Business Email Compromise (BEC)-Angriff zu tun.

Viele Spear-Phishing-Angriffe sind noch weitaus individualisierter. Gut vorbereitete Kriminelle kennen eventuell Ihre Stellenbezeichnung, Ihre Durchwahl, den Kiosk, zu dem Sie in der Mittagspause gerne gehen, Ihre Freunde, den Namen Ihres Chefs, den Namen Ihres Ex-Chefs oder sogar den Namen des Lieferanten, von dem Ihr Unternehmen seine Kaffeebohnen bezieht.

Und wie Sie sich wahrscheinlich vorstellen können, ist Phishing umso erfolgreicher, je mehr Informationen die Angreifer über ihre potentiellen Oper haben. Je mehr Informationen Angreifer über Ihr Unternehmen sammeln konnten, desto glaubwürdiger können sie ihre Phishing-Mails gestalten.

Die Quellen für diese Informationen sind vielfältig:

- Erfolgreiche Angriffe in der Vergangenheit (z. B. mit datenstehlender Malware)
- Vertrauliche Unternehmensdokumente, z. B. Telefonverzeichnisse und Organigramme, die in Suchmaschinen auftauchen
- Ihre privaten Seiten und die Seiten des Unternehmens in sozialen Netzwerken
- Verärgerte ehemalige Mitarbeiter
- Von anderen Kriminellen im Dark Web erworbene Daten

Ihnen fallen wahrscheinlich noch viele weitere Methoden ein, mit denen Daten, die eigentlich vertraulich bleiben sollten, in Umlauf geraten können. Im Wesentlichen geht es um Folgendes: Wenn Sie und Ihre Mitarbeiter diese Methoden durchschauen, ist die Gefahr, dass Sie auf eine Phishing-E-Mail hereinfallen, deutlich geringer.

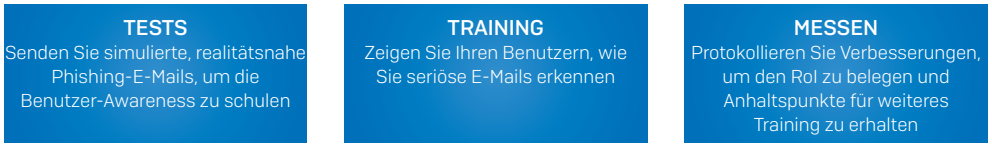
Der Kampf gegen Phishing

Es gibt verschiedenste Formen von Phishing-Angriffen, jedoch leider keine Wunderwaffe, um Ihr Unternehmen vor Phishing-Angriffen zu schützen. Die einzig wirksame Methode ist eine mehrschichtige Abwehr gegen Phishing-Angriffe, bei der leistungsstarke Sicherheitstechnologien mit effektiven Maßnahmen zur Mitarbeiteraufklärung kombiniert werden. Bei Sophos empfehlen wir allen Unternehmen ein an drei Ebenen ansetzendes Konzept:

1. Aufklärung

Im Kampf gegen Phishing sind Ihre Benutzer das schwächste Glied. Im Durchschnitt dauert es nämlich nur 16 Sekunden, bis jemand auf eine Phishing-E-Mail klickt [Quelle: Verizon 2018 Data Breach Investigation Report].

- Damit Ihre Benutzer Phishing nicht schutzlos ausgeliefert sind, ist die Aufklärung und Schulung von Mitarbeitern zur Erkennung und Vermeidung von Phishing-E-Mails unbedingt erforderlich. Ein effektives **Phishing-Simulations- und Trainingsprogramm** sollte an drei Ebenen ansetzen:



2. Vor der Zustellung

58 % aller E-Mails sind Spam, und 77% aller Spam-Mails enthalten schädliche Dateien[6]. Aus diesem Grund ist ein **sicheres E-Mail-Gateway** im Kampf gegen Phishing unabdingbar – Phishing-E-Mails werden so abgefangen, bevor sie Ihren Posteingang erreichen. Folgende Technologien sollte eine effektive Anti-Phishing-Lösung enthalten:

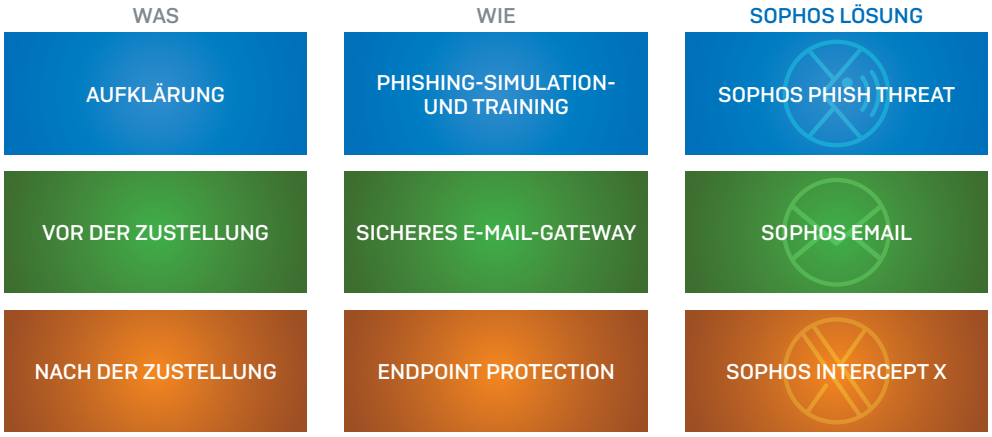
- **Anti-Spam:** Dank weltweiter, leistungsstarker Spam-Traps erreichen schädliche E-Mail Ihre Benutzer gar nicht erst.
- **Sender-Reputation:** IP-Reputation Filterung zum Abfangen unerwünschter E-Mails am Gateway.
- **Authentifizierung: des Absenders:** Erkennen von Absender-Spoofing, Header-Anomalien und verdächtigen E-Mail-Inhalten.
- **Sandboxing:** Ausführen verdächtiger E-Mails außerhalb des Netzwerks.
- **Blockierung schädlicher URLs:** Filtern schädlicher Links zum Schutz vor verzögerten Bedrohungen.

3. Nach der Zustellung

- Der letzte Schutzmechanismus greift nach der Zustellung – wenn Benutzer auf schädliche Links klicken oder infizierte Anhänge aufrufen. Entscheiden Sie sich für eine **Endpoint Security**-Lösung, die sowohl traditionelle als auch neuartige Technologien nutzt:
- **Deep Learning:** Verhindert, dass unbekannte Bedrohungen im Unternehmensnetzwerk ausgeführt werden.
- **Anti-Exploit:** Sorgt dafür, dass Angreifer Schwachstellen in legitimer Software nicht ausnutzen können.
- **Anti-Ransomware:** Stoppt eine unbefugte Verschlüsselung Ihrer Unternehmensdaten.

Was bietet Ihnen Sophos?

Sophos bietet Ihnen eine einzigartige Lösung: Umfassenden Schutz gegen Phishing inklusive Trainings und detaillierten Informationen - alles ganz einfach verwaltet über eine zentrale Konsole.



Sophos Phish Threat schult und testet Ihre Mitarbeiter durch automatische Angriffssimulationen, qualitativ hochwertige Security-Awareness-Trainings und aussagekräftige Reporting-Daten. Und es funktioniert: Im Schnitt sind Kunden bereits nach vier Phish-Threat-Test-E-Mails um 31 % weniger anfällig für Phishing. Überzeugen Sie sich selbst und testen Sie Sophos Phish Threat kostenlos unter www.sophos.de/phish-threat.

Dank **Sophos Email** können Sie Ihrem Posteingang wieder vertrauen. Die Lösung stoppt Phishing-Betrüger, die E-Mail-Adressen bekannter Kontakte fälschen. Durch die Kombination aus SPF, DKIM und DMARC-Authentifizierung sowie Header-Analyse werden legitime E-Mails zugestellt und gefälschte blockiert. Erfahren Sie mehr und testen Sie Sophos Email kostenlos unter www.sophos.de/email.

Sophos Intercept X schützt dank einer Kombination traditioneller und neuartiger Next-Gen-Technologien vor verschiedensten Ransomware-Angriffen und Malware. Das neuronale Deep-Learning-Netzwerk untersucht Millionen Malware-Samples, um unbekannte Bedrohungen proaktiv zu erkennen. Überzeugen Sie sich selbst unter www.sophos.de/intercept-x

Mit Sophos Central können Sie den gesamten Phishing-Schutz über eine einzige Web-Plattform verwalten:

- Zeit- und ressourcensparende Verwaltung über eine zentrale Konsole
- Kein Server-Management nötig dank webbasierter Plattform
- Zugriff jederzeit und überall
- Die Produkte sind perfekt aufeinander abgestimmt – Sie müssen keine zusätzlichen Konfigurationen vornehmen, damit die Produkte gut miteinander funktionieren

Sie können mit einem Produkt beginnen und bei Bedarf weitere hinzufügen.

Zehn Alarmzeichen für Phishing

Die folgenden zehn Alarmzeichen können Ihnen helfen, Phishing frühzeitig zu erkennen:

4. **Irgendetwas stimmt einfach nicht.** Kommt Ihnen eine bestimmte E-Mail-Nachricht irgendwie verdächtig vor? Klingt es zu gut, um wahr zu sein? Vertrauen Sie Ihrem Instinkt.
5. **Allgemeine Anreden.** Anstatt Sie direkt anzusprechen, werden in Phishing-E-Mails häufig allgemeine Anreden wie „Sehr geehrter Kunde" verwendet. Mit diesen unpersönlichen Anreden sparen die Cyberkriminellen Zeit.
6. **Links zu vermeintlich seriösen Websites, auf denen Sie aufgefordert werden, sensible Daten einzugeben.** Diese gefälschten Websites sehen oft täuschend echt aus. Überlegen Sie also lieber zweimal, ob Sie Ihre personenbezogenen oder vertraulichen Daten wirklich preisgeben möchten.
7. **Unaufgefordert zugesendete E-Mails mit spezifischen Informationen zu Ihrer Person.** Informationen wie Stellenbezeichnung, vorherige Anstellung oder persönliche Interessen können aus sozialen Netzwerken wie LinkedIn zusammengetragen werden und sollen Phishing-E-Mails überzeugender machen.
8. **Verunsichernde Texte.** Die Angreifer arbeiten oft mit Texten, die Sie verunsichern sollen (z. B. behaupten sie, dass Ihr Account gehackt wurde), damit Sie schnell und unüberlegt handeln und Informationen preisgeben, die Sie ansonsten für sich behalten würden.
9. **Grammatik- oder Rechtschreibfehler.** Fehler sind oft ein eindeutiger Hinweis auf Phishing. Auch ein ungewöhnlicher Satzbau sollte bei Ihnen die Alarmglocken läuten lassen.
10. **Angebliche Dringlichkeit.** „Wenn Sie nicht innerhalb von 48 Stunden antworten, wird Ihr Account gesperrt." Phishing-Angreifer versuchen, Sie zeitlich unter Druck zu setzen, damit Sie unüberlegt handeln und Fehler begehen.
11. **„Sie sind der Hauptgewinner!"** Solche Phishing-E-Mails sind weit verbreitet, aber leicht zu erkennen. Eine ähnliche, kompliziertere Variante fordert Sie auf, an einer Umfrage teilzunehmen (bei der Sie Ihre personenbezogenen Daten offenlegen) und verspricht Ihnen als Gegenleistung einen Preis.
12. **„Verifizieren Sie Ihren Account."** Diese E-Mails ahmen echte E-Mails nach und fordern Sie auf, Ihren Account zu bestätigen. Achten Sie immer auf Anzeichen von Phishing und hinterfragen Sie stets, warum Sie um eine Verifizierung gebeten werden – die Wahrscheinlichkeit ist hoch, dass Sie getäuscht werden sollen.
13. **Cybersquatting.** Häufig kaufen und „horten" Cyberkriminelle Website-Namen, die bekannten Websites ähneln in der Hoffnung, dass Benutzer die falsche Website besuchen, z. B. www.google.com vs. www.g00gle.com. Nehmen Sie sich immer einen Moment Zeit, um die URL zu prüfen, bevor Sie Ihre persönlichen Daten eingeben.

1, 3, 4, 6 Quelle: Phishing Temperature Check, Freeform Dynamics in Zusammenarbeit mit The Register und Sophos, 2017

2 Quelle: Verizon 2018 Data Breach Investigations Report

5 Quelle: Verizon 2016 DBIR & Experian Email Benchmark Report Q4 2016

6 Quelle: SophosLabs, 2017

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

© Copyright 2018. Sophos Ltd. Alle Rechte vorbehalten.
Eingetragen in England und Wales, Nr. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, GB
Sophos ist die eingetragene Marke von Sophos Ltd. Alle anderen genannten Produkt- und Unternehmensnamen sind Marken oder eingetragene Marken ihres jeweiligen Inhabers.

31.05.2018 WP-DE (3017-DD)

SOPHOS