Phishing

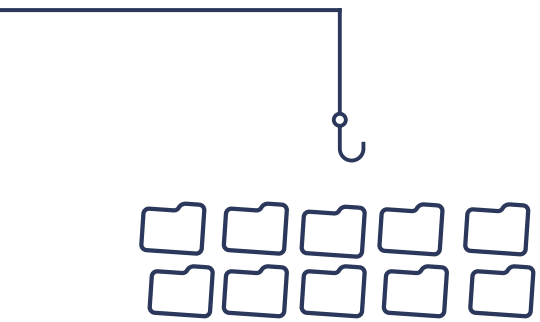
Lassen Sie sich nicht täuschen

datenschutz nord
GRUPPE

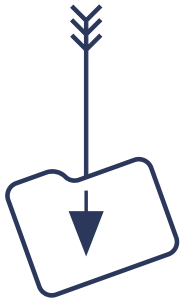
Phishing – Sicherheitsrisiken erkennen

Der Schaden, den die deutsche Wirtschaft durch Phishing-Angriffe jährlich erleidet, steigt stetig. Nahezu jedes Unternehmen und beinahe jeder Mitarbeiter in Deutschland waren bereits Phishing-Attacken ausgesetzt. Von der Installation von Schadsoftware über das Ausforschen sensibler Interna bis hin zum Abfluss von Geldern können die Folgen vielfältig ausfallen. Phishing ist eine erfolgreiche Methode von Angreifern, um mit geringem Aufwand Zugriff auf die Daten Ihres Unternehmens zu erlangen. Hierzu wird versucht, den Nutzer per E-Mail zu täuschen, um sensible Daten preiszugeben. Das Ausnutzen des „menschlichen Faktors“ mit seinen Instinkten, die auf Angst, Neugierde, Vertrauen und „Helfen wollen“ basieren, bildet die Basis für die anschließende Bedrohung. Mit dem Passwort ist es für den Angreifer dann sehr einfach, Zugriff auf das Netzwerk Ihres Unternehmens zu erlangen und sich darin zu bewegen – meist völlig unbemerkt. Diese Art von Angriff umgeht die traditionellen Sicherheitsmaßnahmen, die die Perimeter des Netzwerks schützen aber keinen Schutz für das Innere bieten.

Die häufigsten Vorgehensweisen bei einem Angriff:



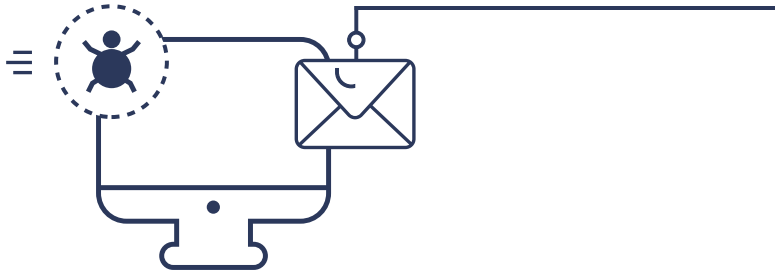
Phishing –
Ungezielter Angriff



Spear Phishing –
Gezielter Angriff

Wie funktioniert Phishing?

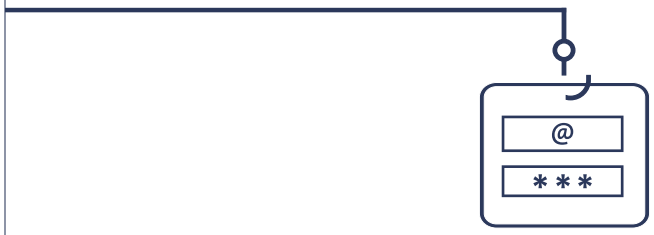
Bei einem Phishing-Angriff versucht der Angreifer Passwörter, Anmeldeinformationen und Daten zu stehlen oder auch, viel perfider, einen Virus zu installieren, um die notwendigen Zugangsdaten zu erlangen. Typischer Weise wird dafür eine E-Mail an das potenzielle Opfer gesendet.



Welche Taktiken werden angewandt?

Hat der Empfänger nun eine Phishing-Mail erhalten, wird im Text versucht, ihn dazu zu bringen, auf einen Link zu klicken, der auf eine gefälschte Seite leitet. Hier sollen dann Name und Passwort eingegeben werden, wodurch der Angreifer zukünftig direkten Zugriff auf sämtliche Daten erhält. Oder, im anderen Fall, wird eine E-Mail mit einem Anhang versendet, der dann direkt eine Malware aktiviert.

Ihr interner Workflow gibt Aufschluss darüber, an welcher Stelle Sie welche Schutzmaßnahmen ergreifen müssen.



Welche Branchen werden als Absender genutzt?

Einer Untersuchung von MarkMonitor Inc. Zufolge ist der Versand gefälschter E-Mail hauptsächlich in den folgenden Branchen gestiegen:

Quelle: Phishing Activity Trends Report, 4th Quarter 2018

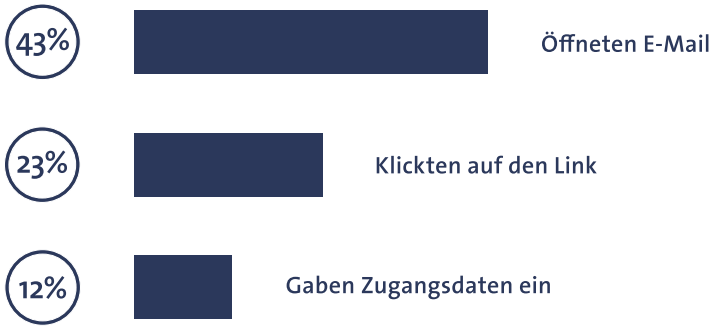
In den meisten Fällen werden Absender gewählt, die vertrauensvoll erscheinen und zu denen die meisten Anwender einen Bezug haben. Angeführt wird die Liste von Microsoft, gefolgt von Paypal, Netflix, facebook, DHL und Dropbox. Mit einem einzigen Satz von Microsoft-Anmeldeinformationen können Hacker auf eine Fundgrube vertraulicher Dateien, Daten und Kontakte zugreifen, die in Office 365 Anwendungen gespeichert sind. PayPal-Anmeldeinformationen bieten den Angreifern eine sofortige Amortisation ihrer Aufwände und Netflixkonten sind wertvoll wegen der darin gespeicherten Kreditkarteninformationen.

Was wird am meisten geklickt?

Wenn User eine Phishing-Mail öffnen, worauf klicken sie am häufigsten?

Mit einer Klickrate von 89 % wurde auf E-Mails reagiert, die die Verbesserung der E-Mail-Kommunikation behandelten, gefolgt von 86 %, die Sicherheitsupdates für Online-Shopping zum Inhalt hatten (Wombat Security). Weiterhin konnte ein Anstieg von geschäftsbezogenen, kommerziellen E-Mails registriert werden wie z. B. Versandbestätigungen und Überweisungsaufforderungen. Ein Klick in Kampagnen, die auf Windows 365, DocuSign und Dropbox basierten, wurden ebenfalls oft angenommen, genauso wie Kampagnen in Verbindung mit Universitäten.

Die folgenden Ergebnisse basieren auf simulierten Phishing-Kampagnen des US-Unternehmens Duo Security mit ca. 230.000 E-Mail-Empfängern. Immerhin 12% von ihnen gaben ihre Zugangsdaten in ein gefälschtes Website-Login-Formular ein.



Was wird meistens gestohlen?

Die Angreifer haben es meist auf persönliche oder Finanzinformationen wie diese abgesehen:

Benutzernamen und Passworte

Vertrauliche Unternehmensinformationen

Kontoverbindungen und Kreditkartennummern

Telefonnummern im Rahmen der Zwei-Faktor Authentifizierung

E-Mail-Adressen für weiteren SPAM-Versand

Persönliche Daten (Namen und Adressen für Betrugsversuche)

Mit einigen dieser Angaben können sie nun, nachdem sie Zugriff auf beispielsweise den E-Mail-Posteingang erhalten haben, einen Passwort-Reset in einem sozialen Medium durchführen. Denn mit Zugriff auf die E-Mails des Benutzers und geändertem Passwort kann die vollständige Kontrolle über Konten wie Twitter, Amazon etc. übernommen werden.

Wie können Sie sich nun vor Phishing-Angriffen schützen?

Ihre Administratoren haben einige Möglichkeiten:

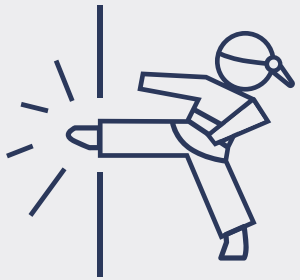
- Implementieren Sie, wenn möglich, eine Zwei-Faktor-Authentifizierung. So sind auch dann, wenn Passwörter „erbeutet“ wurden, die Konten durch den zweiten Faktor weiterhin geschützt. Denn ohne im Besitz z. B. Ihres Smartphones oder Sicherheitstokens zu sein, kann sich niemand einloggen.

- Zusätzlich sollten die Nutzer ermutigt werden, regelmäßige Sicherheitsupdates ihrer Geräte durchzuführen. Einige Phishing-Methoden prüfen über einen bösartigen Anhang die Softwareversion ab und kompromittieren erst dann, unter Ausnutzung der Schwachstellen, die Geräte.

- Verschaffen Sie sich einen genauen Überblick über die Geräte, die auf Ihr Netzwerk zugreifen. Oft nutzen User ihre persönlichen Smartphones und Notebooks, um die IT-Ressourcen des Unternehmens zu nutzen.

- Ein abgestimmter Endpunktschutz ist unumgänglich. Entwickeln Sie Sicherheitsrichtlinien und strenge Sicherheitskontrollen, um diesen Risiken vorzubeugen.

- Installieren Sie unternehmensweite Spamfilter und überdenken Sie weitere technischen Sicherheitsmaßnahmen.



Aber auch Ihre Mitarbeiter können Vorsichtsmaßnahmen treffen:

- Klicken Sie nicht auf E-Mail-Links, sondern geben Sie den Domainnamen selbst ein, bevor Sie sensible Daten in irgendein Web-Formular eingeben.
- Richten Sie, wenn möglich, für jedes Konto eine Zwei-Faktor-Authentifizierung ein.
- Seien Sie vorsichtig bei Nachrichten, die dringende Anfragen, Geldangebote oder Geschenke enthalten. Nachrichten mit dringenden Aufforderungen, sofortigen Zahlungen, Updates oder Passwortänderungen sind mit absoluter Vorsicht zu behandeln.
- Seien Sie vorsichtig bei vertrauensvollen Kontakten auf gemeinsamen Plattformen, ob beruflich oder privat.
- Überprüfen Sie die Absender der Nachrichten, wenn die Möglichkeit dazu besteht.
- Nutzen Sie Softwareupdates und konfigurieren Sie, wenn möglich, automatisierte Updates.

Steigern Sie die Security Awareness Ihrer Mitarbeiter

Der Schutz vor Bedrohungen durch Phishing erfordert einen neuen, auf den Menschen ausgerichteten Sicherheitsansatz. Wir empfehlen daher folgendes:

- Trainieren Sie Ihre Mitarbeiter, Angriffe zu erkennen, die auf sie abzielen.
- Dieses „Awareness-Training“ sollte Phishing-Simulationen beinhalten, die mit möglichst realen Taktiken arbeiten, um festzustellen, wo persönliche Unsicherheiten bestehen. Denn nur wer eine Gefahr erkennt, kann sich schützen.

Simulation eines Angriffs – Vorgehensweise

- Durch eine professionelle Phishing-Simulation können wir sämtliche Verteidigungsbarrieren Ihres Unternehmens überprüfen – vom Spam-Filter bis hin zum Mitarbeiter.
- Die Maßnahme wird in enger Abstimmung und im Rahmen der gemeinsam definierten Ausprägung datenschutzkonform durchgeführt. Im Projektierungsgespräch mit Ihnen, dem zuständigen Datenschutzbeauftragten und einem Beauftragten der Mitarbeitervertretung, wird das Vorgehen definiert.
- Am Ende der Kampagne erhalten Sie einen umfassenden Abschlussbericht, der ausschließlich anonymisierte Informationen enthält. Er vermittelt Ihnen einen detaillierten Überblick über die Ist-Situation Ihrer IT-Sicherheit, zu dem von uns durchgeführten Angriff.

datenschutz nord GmbH

Bremen – Hauptsitz
Konsul-Smidt-Straße 88
28217 Bremen
Tel.: +49 (0) 421 69 66 32-0

datenschutz süd GmbH

Würzburg – Hauptsitz
Wörthstraße 15
97082 Würzburg
Tel.: +49 (0) 931 30 49 76-0

Weitere Niederlassungen der **datenschutz nord Gruppe** siehe **www.datenschutz-nord-gruppe.de/standorte**

www.datenschutz-nord-gruppe.de
www.datenschutz-notizen.de