Checkliste: Spoofing- und Phishing Angriffe

Der Unterschied zwischen Spoofing und Phishing besteht darin, dass beim Spoofing eine andere Identität vorgetäuscht wird, während bei Phishing-Angriffen versucht wird, an sensible Informationen zu gelangen. Typisch bei Phishing-Angriffen ist, dass Opfer unter anderem mit Ködern wie gefälschten E-Mails „angelockt“ und dazu gebracht werden, vertrauliche personenbezogene Daten preiszugeben, die dann für Identitätsdiebstahl verwendet werden können.

Spoofing-Angriffe erwecken den Anschein, dass die Kommunikation vertrauenswürdig ist, da die Absender vertrauenswürdigen Absendern täuschend ähnlich sind. Viele Phisher verwenden Spoofing, um ihren Opfern vorzugaukeln, dass die E-Mail seriös ist. Mit dieser Art von manipulativem Social Engineering bringen Phishing-Betrüger Sie dazu, persönliche Informationen preiszugeben.

Wie bereits erwähnt, gibt es verschiedene Arten von Spoofing. Spoofing auf DNS- oder IP-Ebene unterscheidet sich vom Phishing, da technische Mittel verwendet werden, um einen Computer oder ein Netzwerk auszutricksen. Typosquatting zum Beispiel ist eine Art von Spoofing-Angriff, bei dem häufige Fehler bei der Eingabe von URLs ausgenutzt werden, um die Nutzer glauben zu machen, sie würden die gewünschte Website besuchen.

E-Mail-Spoofing und Phishing sind ähnlich und werden manchmal zusammen angewendet.

Arten von Spoofing

Spoofing bezieht sich auf jede Art von Cyberkriminalität, bei der sich Hacker als vertrauenswürdige Instanz ausgeben – und es gibt viele verschiedene Möglichkeiten, wie Hacker Spoofing für ihre Angriffe einsetzen können. Zwar zielen die verschiedenen Arten von Spoofing auf verschiedene Kanäle oder Opfer ab, aber allen Arten von Spoofing ist gemeint, dass sie **Schwachstellen ausnutzen und sich Ihr Vertrauen zunutze machen.**

E-Mail-Spoofing?

E-Mail-Spoofing ist, wenn Hacker E-Mails mit einer gefälschten E-Mail-Adresse erstellen und versenden, die das Opfer kennt, z. B. von seiner Bank. In der Geschäftswelt können sich Hacker als hochrangige Führungskräfte oder Geschäftspartner ausgeben und Interna von Mitarbeitern anfordern.

Aber wie funktioniert E-Mail-Spoofing, und wie kommen die Spoofer damit durch? E-Mails sind ein offenes und mäßig gesichertes System, mit dem Menschen unkompliziert Nachrichten austauschen können. Leider sind E-Mails dadurch auch anfällig für Missbrauch durch böswillige Akteure wie Spoofer.

Es gibt sogar Websites für E-Mail-Spoofing, die Hackern helfen, E-Mails schnell online zu fälschen. Anfang 2019 wurde der in Mumbai ansässige Farbenhersteller Asian Paints Opfer eines massiven E-Mail-Spoofing-Angriffs, bei dem die Hacker vorgaben, einer der Lieferanten des Unternehmens zu sein.

Die gute Nachricht ist, dass der E-Mail-Spamfilter darauf trainiert werden kann, Spam und andere verdächtige E-Mails zu erkennen. Und wenn das nicht funktioniert, können Sie Spoofing immer noch stoppen, wenn Sie wissen, wonach Sie suchen müssen.

Kostenlose E-Mail-Domain: Finanzinstitute und andere Unternehmen senden ihre E-Mails von ihren offiziellen Domains aus. Wenn Sie eine E-Mail erhalten haben, die echt aussieht, aber von einer Adresse eines kostenlosen E-Mail-Anbieters stammt, z. B. „IhreBank [de] yahoo.com“, handelt es sich möglicherweise um Spoofing.

Allgemeine Grußformel: Die meisten Unternehmen werden Sie mit Ihrem Namen ansprechen. Seien Sie skeptisch gegenüber E-Mails, die mit „Sehr geehrte Kundin, sehr geehrter Kunde“ beginnen oder in denen Sie mit Ihrem E-Mail-Benutzernamen angesprochen werden.

Anforderung persönlicher Informationen: Unternehmen und Arbeitgeber sollten bereits über alle Informationen verfügen, die sie benötigen. Sie sollten Ihnen keine E-Mails senden, um Dinge wie Ihre Benutzeranmeldeinformationen oder Kreditkarteninformationen anzufordern. Solche E-Mails könnten ein Phishing-Scam mit Spoofing-Techniken sein.

Gefälschte E-Mails enthalten oft unechte E-Mail-Adressen, allgemeine Grußformeln, Aufforderungen zur Angabe persönlicher Daten und erzeugen den Eindruck von Dringlichkeit.

Merkwürdige Anhänge: Einige Spoofer versuchen mit Phishing-Angriffen Spam-Filter zu umgehen, indem sie den schädlichen Inhalt ihrer E-Mail in einen Anhang einfügen. Achten Sie besonders auf .HTML- oder .EXE-Anhänge, da diese möglicherweise Malware auf Ihrem Gerät installieren. Klicken Sie niemals auf unbekannte Anhänge oder Links, wenn Sie verdächtige E-Mails erhalten.

Fehler und Uneinheitlichkeit: Entspricht der Name des Absenders der von ihm verwendeten E-Mail-Adresse? Gibt es offensichtliche Rechtschreib- oder Grammatikfehler? Ist Ihr Name richtig geschrieben? Seriöse Unternehmen machen diese Art von nachlässigen Tippfehlern (hoffentlich!) nicht in den E-Mails, die sie an ihre Kunden versenden.

Künstlich erzeugte Dringlichkeit: Spoofer möchten, dass Sie schnelle Entscheidungen treffen und sich keine Zeit zum Nachdenken nehmen. Ihr Konto wird gelöscht! Ihnen wird ein Bußgeld auferlegt! Die Regierung wird Sie verklagen! Je mehr Angst die Hacker auslösen können, desto höher ist die Wahrscheinlichkeit, dass ihre Opfer auf den Betrug hereinfallen.

Kleine Schreibabweichungen: Viele Spoofer versuchen sogar, Opfer dazu zu bringen, komplette gefälschte Websites zu besuchen. Sie lassen ihre Website wie die echte aussehen, indem sie einige „clevere“ Rechtschreibtricks anwenden, z. B. ein kleines L durch ein großes I ersetzen oder eine andere Domain-Endung verwenden.

Typosquatting: Typosquatting, auch bekannt als URL-Hijacking oder Brandjacking, macht sich häufige Tippfehler zunutze, die Menschen bei der Eingabe von Webadressen in ihren Browsern machen. Wenn Sie die Website mit der falsch geschriebenen Adresse aufrufen, landen Sie wohl möglich auf einer Hacker-Website.

Website-Spoofing

Beim Website-Spoofing erstellt ein Hacker eine gefälschte Website, die wie eine seriöse aussieht. Wenn Sie sich anmelden, erhalten die Hacker Ihre Anmeldedaten. Damit könnten sie dann auf Ihr Konto zugreifen.

Böswillige Spoofer verwenden manchmal eine getarnte URL, die Sie über ihr eigenes System umleitet und dabei Ihre persönlichen Daten sammelt. Sie können sogar das wahre Ziel der URL verschleiern, indem sie spezielle Steuerzeichen einfügen, die eine andere Bedeutung haben als die Zeichen, die Sie sehen. Wie beim Typosquatting ist die URL der tatsächlich gemeinten Adresse so ähnlich, dass Sie den Unterschied wahrscheinlich nicht bemerken.

Gefälschte Websites sind häufig in gefälschten E-Mails und Phishing-Kampagnen verlinkt, beachten Sie daher die oben genannten Warnzeichen für gefälschte E-Mails, um sich zu schützen.

Spoofer versuchen, Ihr Vertrauen zu gewinnen, sei es durch eine dringend wirkende E-Mail, eine nachgebaute Website oder eine gefälschte IP-Adresse. Einige Arten von Spoofing sind leicht zu erkennen, wie z. B. gefälschte Anrufe von ungültigen Nummern. Falsche Websites und andere Angriffe sind schwerer zu erkennen.

Prüfung einer Website auf Seriosität

Sie können die Authentizität einer Website prüfen, indem Sie sich ihr digitales Zertifikat ansehen. Suchen Sie das Vorhängeschloss-Symbol in der Adressleiste. Klicken Sie darauf – jetzt sollten Sie sehen können, ob das Zertifikat gültig ist oder nicht.

IP-Spoofing

IP-Spoofing findet auf einer tieferen Ebene des Internets als das E-Mail-Spoofing statt. Beim IP-Spoofing manipulieren die Hacker eines der grundlegenden Protokolle des Internets. Jedes Gerät stellt über eine IP-Adresse eine Verbindung zum Internet her. Dabei handelt es sich um eine Zahlenfolge, die anderen Geräten mitteilt, wo es sich befindet. Wenn Ihr Gerät Informationen sendet und empfängt, verwendet es Datenpakete, die die IP-Adresse Ihres Geräts finden können.

Viele geschlossene Netzwerke sind so konfiguriert, dass sie nur Pakete von bestimmten, vorab genehmigten IP-Adressen akzeptieren. Dies ist eine Sicherheitsmaßnahme, um zu verhindern, dass unbekannte Geräte auf das Netzwerk zugreifen. Ein Hacker kann einen IP-Spoofing-Angriff verwenden, um die IP-Adresse seines Geräts zu ändern und ein ansonsten abgesichertes Netzwerk dazu zu bringen, ihm Zugriff zu gewähren. Sie können Ihre IP-Adresse verbergen, damit Hacker sich nicht als Sie ausgeben können.

IP-Spoofing ist besonders beliebt bei DDoS-Angriffen, bei denen ein Hacker ein Netzwerk überlastet, indem er es mit eingehendem Datenverkehr überflutet. Es ist einfach, Datenverkehr von einer einzelnen IP-Adresse zu blockieren. Aber mit IP-Spoofing können Hacker den Datenverkehr so erscheinen lassen, als stamme er aus mehreren Quellen. Dies macht die Abwehr viel schwieriger.

Einige Botnets verfolgen den gegenteiligen Ansatz: Sie nutzen IP-Spoofing, um den Eindruck zu erwecken, dass der Datenverkehr von vielen Geräten eigentlich nur von einem stammt. Dazu verbinden sich die Geräte im Botnet mit vielen Servern und verwenden dann IP-Spoofing, um die Antworten nur an ein Gerät zu leiten. Der eingehende Datenverkehr überfordert die Zielserver rasch.

ARP-Spoofing: Beim Address Resolution Protocol (ARP)-Spoofing kann ein Hacker ein lokales Netzwerk (LAN) infiltrieren, indem er seinen Computer als Netzwerkmitglied maskiert. Hacker verwenden ARP-Spoofing, um Informationen mit Man-In-the-Middle-Angriffen zu stehlen. Dabei fangen Hacker heimlich eine Unterhaltung ab, geben sich als beide Teilnehmer aus und können so die besprochenen Informationen abgreifen

DNS-Spoofing: Diese Technik wird auch als DNS-Cache-Poisoning bezeichnet und leitet die Opfer von einer Website zu einer anderen um. Der Hacker „vergiftet“ die Auflistung der Zielwebsite auf einem DNS-Server, indem er die zugehörige IP-Adresse in eine seiner Wahl ändert, wodurch die Opfer auf betrügerische Websites umgeleitet werden, auf denen persönliche Daten gesammelt oder Malware auf ihren Computer heruntergeladen wird. DNS-Spoofing ist eine gängige Technik bei Pharming-Angriffen.

Call-ID-Spoofing: Da sie den Anschein erwecken lassen können, dass ihre Anrufe von einer vertrauenswürdigen Nummer oder bestimmten geografischen Regionen stammen, ist ID-Spoofing bei Robocallern sehr beliebt. Sobald das Opfer den Anruf entgegennimmt, versucht der Angreifer, an vertrauliche Informationen zu gelangen. Call-ID-Spoofing kann auch zum Senden von gefälschten oder Spam-Textnachrichten verwendet werden.

GPS-Spoofing: Einige Menschen versuchen, ihren physischen Standort falsch darzustellen, indem sie ihre GPS-Koordinaten fälschen. Jede mobile App, die Smartphone-Standortdaten verwendet, ist ein potenzielles Ziel für GPS-Spoofing-Angriffe.

SMS-Spoofing: Hacker können manipulierte SMS-Nachrichten senden, die scheinbar von einer anderen Nummer stammen. SMS-Spoofing-Angriffe enthalten oft schadhafte Links zu gefälschten Websites. Andere fordern das Opfer auf, etwas herunterzuladen, das sich als Malware herausstellt.

So kann Spoofing verhindert werden

Oben haben wir beschrieben, was Spoofing bedeutet und wie es funktioniert. Lesen Sie jetzt unsere Tipps zur Spoofing-Prävention und erfahren Sie, wie Sie sich vor Spoofing-Angriffen schützen können:

Wichtig: Bleiben Sie wachsam gegenüber den bekanntesten Arten von Spoofing. Achten Sie immer auf mögliche Anzeichen eines Spoofing-Angriffs. So ist die Gefahr für Sie geringer, ausgetrickst zu werden.

Machen Sie einen Bestätigungsanruf: Wenn Sie aufgefordert werden, persönliche Informationen, wie etwa Passwort oder Kreditkartennummer, preiszugeben, rufen Sie

den Absender auf der Telefonnummer an, die auf der offiziellen Webseite aufgeführt ist. Geben Sie die URL manuell in Ihren Webbrowser ein, überprüfen Sie die Website auf Anzeichen von Website-Spoofing und klicken Sie in der verdächtigen E-Mail, die Sie erhalten haben, nicht auf Links.

Hüten Sie sich vor merkwürdigen Anhängen: Öffnen Sie niemals Anhänge, deren Empfang Sie nicht erwartet haben, insbesondere wenn sie ungewöhnliche Dateierweiterungen haben.

Ihre IP-Adresse wird verborgen: Gewöhnen Sie sich an, Ihre IP-Adresse beim Surfen im Internet zu verbergen, um IP-Spoofing zu verhindern.

Ändern Sie Ihre Passwörter regelmäßig: Wenn es einem Spoofer gelingt, an Ihre Zugangsdaten zu kommen, kann er keinen großen Schaden anrichten, wenn Sie bereits ein neues Passwort haben. Erstellen Sie sichere Passwörter, die schwer zu erraten sind, und verwenden Sie einen Passwort-Manager, um sie sicher zu speichern.

Erst prüfen, dann klicken: Bewegen Sie den Mauszeiger über Links, um die URL zu prüfen. Wenn Sie auf den Link geklickt haben, prüfen Sie noch einmal die URL, um sicherzugehen, dass Sie nicht weitergeleitet wurden. Bevorzugen Sie Websites mit HTTPS-Verschlüsselung.

Melden Sie Spoofing-Versuche: Wenn Sie eine gefälschte E-Mail oder andere Mitteilung erhalten haben, teilen Sie dem vermeintlichen Absender mit, dass er oder sie Opfer eines Angriffs geworden ist. Dies kann dazu beitragen, zukünftige Spoofing-Angriffe zu verhindern. Die meisten Unternehmen haben auf ihrer Website einen Bereich, wo Sie Spoofing und andere Sicherheitsprobleme melden können.

Verwenden Sie einen sicheren Browser: Steigen Sie auf einen Browser um, bei dem Sicherheit und Datenschutz Priorität haben und der weniger anfällig für Hijacking-Versuche ist als herkömmliche Browser.

Verwenden Sie eine starke Antivirensoftware: Viele der besten kostenlosen Antivirenprogramme enthalten Funktionen, die Bedrohungen in Echtzeit erkennen. Installieren Sie einen vertrauenswürdigen Antivirenschutz, um Ihr Gerät noch besser vor Spoofing zu schützen.