Janotta und Partner
Cybersecurity

Es ist leicht, Daten zu angeln.

Vor Phishing und Cybercrime richtig schützen

Janotta und Partner
Erfahren in IT Sicherheit seit 1999
Internet: www.janotta-partner.de
Email: info@janotta-partner.de

Kurse von Janotta und Partner

Inhalt

Phishing-Update: Die neuesten Methoden und ihre Auswirkungen auf Unternehmen

Einleitung

Seit Jahren ist das Pishing eine der größten Gefahren für Unternehmen und deren Kunden weltweit, doch das Ausmaß dieser Bedrohung nimmt noch immer zu. In der ersten Jahreshälfte 2012 fanden weltweit 19 Prozent mehr Phishing-Angriffe statt als in der zweiten Jahreshälfte 2011. Von Januar 2011 bis Juni 2012 erlitten Unternehmen durch Phishing und dessen Auswirkungen einen geschätzten Gesamtschaden in Höhe von 2,1 Milliarden USD.[1]

Dieser Anstieg beruht hauptsächlich auf zwei Faktoren: Phishing-Angriffe sind erstens relativ leicht umsetzbar und zweitens meist erfolgreich. Man muss kein versierter Hacker sein, um einen Phishing-Angriff zu starten. Ein bisschen Motivation und eine kleine Portion Bosheit und Habgier sind vollkommen ausreichend, denn eine florierende kriminelle Szene liefert gebrauchsfertige Phishing-Kits. Einige Internetkriminelle haben sogar ein als „Malware as a Service“ (MaaS) bekanntes Geschäftsmodell, das nicht nur die Malware selbst, sondern auch ergänzende „Dienstleistungen“ umfasst.[2]

Täglich werden rund 156 Millionen Phishing-E-Mails versandt, von denen ca. 16 Millionen die Sicherheitsfilter passieren. Etwa 50 Prozent dieser E-Mails, also um die acht Millionen, werden geöffnet und rund 800 000 Benutzer lassen sich dazu verleiten, auf einen schädlichen Link zu klicken. Wohlgemerkt: nicht 800 000 pro Jahr, sondern *800 000 pro Tag*.[3] Es ist daher wichtiger als je zuvor, stets über die neuesten Phishing-Maschen informiert zu sein, um dieser gewaltigen Flut schädlicher E-Mails standzuhalten. Nur so können Sie Ihr Unternehmen vorausschauend vor Betrügern schützen.

In diesem Dokument werden die neuesten Entwicklungen bei Phishing-Verfahren erläutert. Insbesondere wird dabei auf aktuelle Bedrohungen aus China eingegangen. Darüber hinaus enthält es Anregungen und Best Practices für den Einsatz technischer Vorkehrungen zum Schutz Ihres Unternehmens und Ihrer Kunden.

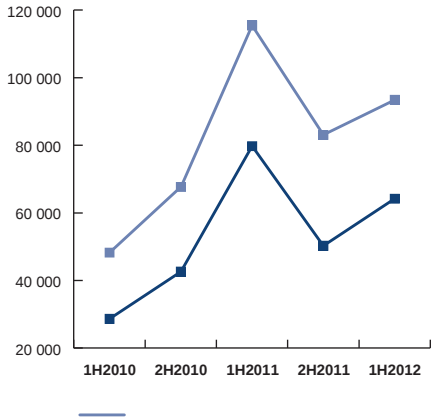
Phishing ist grenzenlos

Beim Phishing werden die Opfer durch anscheinend seriöse E-Mails und Websites dazu verleitet, vertrauliche Daten wie Benutzernamen, Kennwörter oder Kreditkartennummern preiszugeben. Diese altbekannte Betrugsform ist weltweit verbreitet und stellt eine massive und wachsende Bedrohung für Unternehmen und Verbraucher dar. Geografische Entfernung und Grenzen bieten so gut wie keinen Schutz vor Phishing.

Die „Anti-Phishing Working Group“ (APWG) berichtet von mindestens 93 462 verschiedenen Phishing-Angriffen, die in der ersten Hälfte des Jahres 2012 weltweit in 200 Top-Level-Domänen stattfanden. Das ist eine deutliche Steigerung gegenüber der zweiten Jahreshälfte 2011, in der die APWG 83 083 Phishing-Angriffe meldete. Vermutlich ist dieser Anstieg auf die weite Verbreitung von Angriffen auf gemeinsam genutzte virtuelle Server zurückzuführen. In der ersten Jahreshälfte 2012 wurden 64 204 verschiedene Domänennamen angegriffen, die 486 Unternehmen bzw. Organisationen gehören (siehe Abbildung 1).[4]

Allgemeine Statistik

	1H2012	2H2011	1H2011	2H2010	1H2010
Phishing-Domänen	64 204	50 298	79 753	42 624	28 646
Angriffe	93 462	83 083	115 472	67 677	48 244



Made in China: APT1 auf dem Vormarsch

Die meisten Phishing-Angriffe stammen vermutlich aus China. Dieser Trend erreichte in der ersten Jahreshälfte 2011 seinen Höhepunkt, als chinesische Phisher weltweit schätzungsweise 70 Prozent aller betrügerischen Domänen anmeldeten.[5]

Im Februar 2013 veröffentlichte das US-amerikanische Sicherheitsunternehmen Mandiant einen Bericht über eine besonders gefährliche Gruppe von Phishern, die angeblich in China ansässig ist. Diese von Mandiant als „APT1" bezeichnete Gruppe spioniert seit mindestens 2006 über das Internet eine Vielzahl von Opfern aus. Die Gruppe steht höchstwahrscheinlich im Dienst der chinesischen Volksbefreiungsarmee und wird von der chinesischen Regierung finanziell unterstützt. Den Untersuchungsergebnissen von Mandiant zufolge hat APT1 bei mindestens 141 Organisationen insgesamt Hunderte von Terabyte an Daten gestohlen und ist in der Lage, Dutzende von Organisationen gleichzeitig zu bespitzeln. Die extrem versierten Betrüger haben im Schnitt 356 Tage lang Zugriff auf das Netzwerk eines Opfers. In einem Fall verfügten sie sogar mehr als vier Jahre lang über ununterbrochenen Zugriff auf das Netzwerk einer Organisation.[6]

Die Analysten von Mandiant fanden einiges über die Taktiken, Verhaltensweisen und Standorte dieser Gruppe heraus. In über 97 Prozent der Fälle, in denen mutmaßliche Mitglieder von APT1 bei der Kontaktaufnahme mit der Infrastruktur der Gruppe beobachtet wurden, nutzten sie in Shanghai registrierte IP-Adressen. Die Spracheinstellung aller benutzten Systeme war vereinfachtes Chinesisch. In 767 verschiedenen Fällen nutzten vermutlich APT1 angehörende Angreifer das Hacker-Tool HTran (HUC Packet Transmit) zur Kommunikation zwischen ausnahmslos in China registrierten IP-Adressen und den Systemen ihrer Opfer.[7]

Das Ausmaß und die Raffinesse dieser Angriffe sind beispiellos. Mandiant vermutet daher, dass APT1 eine große Organisation mit möglicherweise Hunderten von Mitgliedern und einer Hardware-Infrastruktur von über 1000 Servern ist, die neben Phishing-Spezialisten auch Sprachwissenschaftler, Malwareprogrammierer und hoch qualifizierte Experten aus den bespitzelten Branchen beschäftigt.[8]

Zum Schutz Ihres Unternehmens und Ihrer Kunden vor einer Bedrohung dieser Größenordnung sind zuverlässige, vorausschauende Maßnahmen erforderlich. Um Organisationen bei der Verbesserung ihrer Sicherheitsmaßnahmen zu unterstützen, hat Mandiant über 3000 Indikatoren veröffentlicht, die auf einen APT1-Angriff hindeuten, darunter Domänennamen, IP-Adressen und MD5-Hashwerte. Diese Indikatoren können über Redline, das kostenlose hostbasierte Analysetool des Unternehmens, heruntergeladen werden. Wir empfehlen den umgehenden Einsatz dieses wertvollen Hilfsmittels.

Gemeinsam genutzte virtuelle Server bleiben eines der Hauptziele

Im vergangenen Jahr meldeten wir eine erhebliche Steigerung von Phishing-Angriffen auf gemeinsam genutzte virtuelle Server. Bei einem solchen Angriff verschafft sich ein Internetkrimineller Zugang zu einem Webserver, auf dem viele Domänen gehostet werden, und infiziert dann jede dieser Domänen mit Phishing-Inhalten. Infolgedessen zeigen alle auf diesem Server gehosteten Websites die Phishing-Seiten an, d. h. Tausende von Websites werden gleichzeitig infiziert.

Die Anzahl dieser Angriffe ging in der zweiten Jahreshälfte 2011 zurück, stieg 2012 aber erneut drastisch an: allein im Juni meldete die APWG 7000 Angriffe auf 44 verschiedene virtuelle Server, ein neuer Rekordwert.[9]

Feiertage und Ereignisse von weltweiter Bedeutung sind weiterhin beliebte Aufhänger

In der Vorweihnachtszeit 2012 fälschten Spammer erneut die Websites mehrerer seriöser Online-Händler, um mit „Weihnachtsangeboten", Gutscheinkarten und anderen Adventsködern auf Beutezug zu gehen. Mehrere Phishing-Angriffe nutzten die Hektik vieler US-Amerikaner am Ende des Steuerjahres aus, indem sie E-Mails verschickten, die angeblich von der Bundessteuerbehörde IRS (Internal Revenue Service) stammten.[10] Wie man es inzwischen kennt, wurden auch Ereignisse von weltweiter Bedeutung wieder zum Anlass für regelrechte Wellen von Betrugsversuchen genommen. Im vergangenen Jahr waren dies insbesondere die Olympischen Sommerspiele in London.

Der von Phishing-Fachleuten vorhergesagte deutliche Anstieg der Anzahl von Phishing-E-Mails im Vorfeld der Olympischen Spiele[11] blieb nicht aus. Im Verlauf des Sommers machte Zscaler auf eine steigende Anzahl von Websites aufmerksam, die angeblich Eintrittskarten für die olympischen Wettbewerbe verkauften,[12] und Omniquad entlarvte eine als Olympia-Sonderaktion von British Airways getarnte Scheinlotterie[13]. Ähnliche Betrugsversuche sind im Vorfeld zukünftiger Sportereignisse von weltweiter Bedeutung zu erwarten. Der FIFA Konföderationen-Pokal 2013 und die Fußball-Weltmeisterschaft 2014 in Brasilien sowie die Olympischen Winterspiele 2014 im russischen Sotschi sind nur einige Beispiele.

Phishing auf dem Nährboden der Krisenangst

In wirtschaftlich turbulenten Zeiten fällt es Betrügern besonders leicht, die Ängste ihrer Opfer auszunutzen. In den USA versenden Kriminelle beispielsweise bevorzugt E-Mails, die anscheinend von einem Geldinstitut stammen, das vor Kurzem die Bank oder Bausparkasse des Opfers übernommen hat.[14] Verbraucher sind oft nur unzureichend über die Art und den derzeitigen Stand dieser Übernahmen oder Fusionen informiert und Betrüger nutzen diese Ungewissheit nur zu gern aus.

Der beste Schutz vor derartigen Betrugsversuchen ist die klare, verständliche und widerspruchsfreie Benachrichtigung der Kunden über alle Stadien einer solchen Transaktion. Je besser Kunden informiert sind, desto unwahrscheinlicher ist es, dass sie einem Betrüger zum Opfer fallen.

Kombination aus Phishing und Malware

Bei einigen Angriffsvarianten wird versucht, die Erfolgsrate mit einer Kombination aus Phishing und Malware zu steigern.[15] Ein Beispiel: Jemand erhält eine echt wirkende E-Card-Mitteilung, die in Wirklichkeit aber die erste Stufe eines raffinierten Angriffs ist. Der Empfänger klickt auf den Link in der E-Mail, um die Karte abzurufen, gelangt jedoch zu einer gefälschten Website, von der ein Trojaner auf den Computer des Opfers geladen wird. Oder das Opfer erhält die Mitteilung, dass erst ein Softwareupdate geladen werden muss, bevor die Karte angezeigt werden kann. Das Opfer lädt die Software herunter, bei der es sich tatsächlich um einen Keylogger handelt.

Über Phishing geladene Keylogger nutzen Aufzeichnungsfunktionen, die bestimmte Aktionen und bestimmte Arten von Websites, beispielsweise von Geldinstituten oder Online-Händlern, überwachen. Auf diese Weise können vertrauliche Daten wie Kontonummern, Benutzernamen und Kennwörter ausgespäht werden.

Phishing mit SMS und Mobiltelefonen

Neuerdings geben Betrüger sich nicht nur per E-Mail, sondern auch in SMS-Nachrichten als tatsächlich existierende Geldinstitute aus, um ihre Opfer auf Malware-Seiten zu locken. Die Anzahl dieser sogenannten „SMiShing“-Angriffe stieg in der ersten Jahreshälfte 2012 auf das Fünffache.[16] Im November wiesen Wissenschaftler an der North Carolina State University darauf hin, dass mehrere Android-Plattformen besonders anfällig für SMiShing-Angriffe waren.[17] Daraufhin beseitigte Google die identifizierten Schwachstellen innerhalb einiger Wochen.

Ein typischer SMiShing-Angriff beginnt mit einer SMS, in der vorgegeben wird, dass die Kredit- bzw. Bankkarte des Handybesitzers gesperrt worden sei. Der Empfänger wird aufgefordert, eine bestimmte Telefonnummer anzurufen oder eine gefälschte Website zu besuchen, um die Karte zu reaktivieren. Auf dieser Website bzw. durch ein telefonisches Sprachdialogsystem wird das Opfer aufgefordert, Karten- und Kontonummer sowie die PIN anzugeben.

Phishing als Gefahr für Ihr Unternehmen

Von Phishing-Angriffen ist nach wie vor hauptsächlich, aber bei Weitem nicht ausschließlich, die Finanzbranche betroffen. Auktionsplattformen, Bezahldienste, Online-Shops, soziale Netzwerke, Mobilfunkanbieter und Industrieunternehmen sind ebenfalls häufige Ziele. Kurz gefasst heißt das, dass sich kein Unternehmen und keine Branche vor Angriffen sicher wähnen darf.

Der gute Ruf Ihrer Marke im Internet wird geschädigt, wenn Kriminelle die offizielle Website Ihres Unternehmens nachahmen und für einen Phishing-Angriff missbrauchen. Die Befürchtung, diesen Betrügern zum Opfer zu fallen, wird Verbraucher wahrscheinlich auch vom Besuch Ihrer echten Website abhalten. Zusätzlich zu diesen direkt durch den Angriff verursachten Verlusten ist Ihr Unternehmen auch indirekt gefährdet:

- Der Vertrauensverlust kann sich negativ auf die Besucherzahlen bzw. Online-Umsätze auswirken.
- Möglicherweise müssen Sie ein Bußgeld zahlen, wenn Kundendaten gestohlen oder manipuliert werden.

Selbst Angriffe gegen andere Marken können Ihrem Unternehmen schaden, denn wenn die Kunden erst einmal durch Phishing verunsichert sind, vermeiden sie mitunter sämtliche Online-Geschäfte – auch mit Ihnen.

Schutz für Ihr Unternehmen

Es gibt zwar keine Wunderwaffe, dafür aber eine Reihe brauchbarer technischer Ansätze zum Schutz Ihres Unternehmens und Ihrer Kunden. Die meisten gängigen Phishing-Methoden setzen darauf, die Internetbenutzer auf betrügerische Websites zu locken. Hier setzen Schutzmechanismen wie Secure Sockets Layer (SSL) und Extended Validation SSL (EV SSL) an: Sie verschlüsseln vertrauliche Informationen und belegen die Legitimität Ihrer Website.

Cyberkriminelle verstehen:

Sie wollen Ihre Daten und Ihr Geld.

Adrian Janotta sagt:

Phishing ist ein Kunstwort, das sich vom englischen „fishing“ableitet. Gemeint ist damit das „Angeln“ nach Passwörtern undanderen persönlichen Daten. Phishing gibt es in vielenunterschiedlichen Erscheinungsformen. Die Kriminellen versuchen,Internetnutzer über E-Mails, Messenger, Webseiten oder sozialeNetzwerke zur Preisgabe von Daten oder zum Download vonSchad-Software zu verleiten.

Manchmal ist die Betrugsabsicht soeinfach zu erkennen, dass wohl niemand darauf hereinfällt. Oftarbeiten die Täter jedoch mit Tricks des Social Engineering. Siespielen mit Neugier oder Angst, und dann lassen die potenziellenOpfer alle Vorsicht vergessen. Wenn dann auch noch die E-Mails oderdie Webseiten professionell und fehlerfrei gestaltet sind, könnendie Kriminellen ihre Kampagne wahrscheinlich mit hohenErfolgsaussichten durchführen. Wer jedoch die Techniken der Täterkennt, kann sich erfolgreicher vor solchen Betrügereien schützen.

Für eine wirkungsvolle Betrugsprävention und den Aufbau von Markenvertrauen fordern Best Practices für die Sicherheit strengste Verschlüsselungs- und Authentifizierungsmechanismen. SSL ist der weltweite Standard für Online-Sicherheit und wird zur Verschlüsselung und zum Schutz von Daten eingesetzt, die mit dem überall verfügbaren HTTPS-Protokoll per Internet übertragen werden. SSL schützt Daten, die bei unverschlüsselter Übertragung abgefangen und manipuliert werden könnten. Alle gängigen Betriebssysteme, Browser, Internetanwendungen und Serverhardware-Komponenten unterstützen SSL.

Zum Schutz vor Phishing und als vertrauensbildende Maßnahme müssen Sie Ihren Kunden beweisen, dass Ihr Unternehmen seriös ist. Die Lösung hierfür ist ein SSL-Zertifikat mit Extended Validation (EV). Es basiert auf den derzeit strengsten Vergabekriterien und signalisiert Besuchern, dass die Website tatsächlich dem angegebenen Unternehmen gehört.

EV SSL macht es Besuchern ganz einfach, die Vertrauenswürdigkeit einer Website zuverlässig zu erkennen: Aktuelle Browser zeigen eine grün hinterlegte Adressleiste, in der der Name des Inhabers des SSL-Zertifikats und der Name der ausstellenden Zertifizierungsstelle angegeben werden. Die grün hinterlegte Adressleiste signalisiert dem Website-Besucher, dass der Datenverkehr verschlüsselt wird und die Legitimität Ihres Unternehmens nach den derzeit strengsten Kriterien überprüft wurde. Internetkriminelle können nicht beeinflussen, welche Informationen in der Adressleiste erscheinen. Sie können also nicht ihren eigenen Namen dort anzeigen lassen und sind aufgrund des strengen Authentifizierungsverfahrens auch nicht in der Lage, sich ein echtes EV SSL-Zertifikat zu verschaffen. Damit ist Extended Validation vor der Ausnutzung durch Internetkriminelle sicher.

Abbildung 2: Adressleiste einer Website mit EV SSL-Zertifikat im Internet Explorer

Aufklärung von Kunden und Mitarbeitern

Auch wenn Sie EV SSL einsetzen, sollten Sie Ihre Kunden und Mitarbeiter weiterhin über sicheres Verhalten im Internet und Maßnahmen zur Betrugsprävention aufklären. Dazu gehört das Erkennen von Anhaltspunkten für einen Phishing-Versuch:

- falsche Schreibweisen, Rechtschreibfehler (werden seltener, da Phisher sorgfältiger arbeiten)
- allgemeine Grußformeln statt einer persönlichen Anrede, dringliche Handlungsaufforderungen
- Drohungen mit einem negativen Kontostatus
- Aufforderungen zum Angeben persönlicher Daten
- falsche Domänennamen bzw. Links

Erklären Sie Ihren Kunden und Mitarbeitern außerdem, woran sie eine echte, sichere Website erkennen, bevor sie persönliche oder vertrauliche Informationen eingeben:

- Die Adressleiste sollte grün hinterlegt sein.
- Die URL muss mit https beginnen.
- Mit einem Klick auf das Vorhängeschloss kann überprüft werden, ob die Zertifikatsdaten der erwarteten Website entsprechen.

Beim Aufbau von Vertrauen spielt die Aufklärung eine wichtige Rolle. Durch die Befähigung Ihrer Kunden zur fundierten Beurteilung der Sicherheit Ihrer Website können Sie Ihren Umsatz steigern, sich von Ihren Mitbewerbern abheben und – durch die Verlagerung von Einkäufen auf die Website – sogar Ihre Betriebskosten senken.

Dabei dürfen Sie jedoch nicht vergessen, dass auf Phishing spezialisierte Internetkriminelle ernst zu nehmende und wandlungsfähige Gegner sind. Ihre Angriffe kommen in immer neuem Gewand daher, zielen jedoch stets darauf ab, menschliche Züge wie Mitgefühl, Vertrauen oder Neugier auszunutzen. Der Schutz Ihrer Marke und Ihres Unternehmens vor diesen Betrugsversuchen erfordert stetige Wachsamkeit, ist jedoch nicht unmöglich. Wenn Sie modernste SSL-Technik einsetzen, sich regelmäßig über die neuesten Phishing-Maschen informieren und eine Zertifizierungsstelle wählen, die in puncto Online-Sicherheit die höchstmöglichen Standards einhält, können Sie diesen Betrügern einen Schritt voraus bleiben und Ihr Unternehmen voranbringen.

Glossar

Zertifizierungsstelle: Eine Zertifizierungsstelle ist eine vertrauenswürdige Instanz, die zunächst die Richtigkeit der vom Antragsteller gelieferten Angaben überprüft und dann ein digitales Zertifikat, etwa ein SSL-Zertifikat, ausstellt.

Verschlüsselung: Bei der Verschlüsselung wird eine Nachricht auf eine Weise unlesbar gemacht, dass nur der rechtmäßige Empfänger sie wieder lesbar machen kann. SSL (Secure Sockets Layer) richtet einen privaten Kommunikationskanal ein, in dem Daten während der Online-Übertragung verschlüsselt werden, so dass vertrauliche Daten vor elektronischen Lauschangriffen geschützt sind.

SSL-Zertifikat mit Extended Validation (EV): Für diese Zertifikate hat das CA/Browser Forum als zuständige Instanz höhere Standards für die Überprüfung festgelegt als für gewöhnliche SSL-Zertifikate. Aktuelle gängige Browser wie etwa der Microsoft® Internet Explorer zeigen die URL in der Adressleiste des Browsers auf grünem Hintergrund an, wenn die betreffende Website durch ein SSL-Zertifikat mit EV geschützt ist.

HTTPS: Webseiten, deren Adresse mit „https“ statt mit „http“ beginnt, ermöglichen die sichere Übertragung von Daten durch Verwendung der gesicherten Variante des http-Protokolls. Die Adresskomponente „https“ ist eines der Sicherheitsmerkmale, auf die alle Internetbenutzer beim Senden vertraulicher Angaben – etwa Kreditkartennummern, persönliche Daten oder Daten von Geschäftspartnern – achten sollten.

Secure Sockets Layer (SSL): Das SSL-Verfahren und sein Nachfolger TLS (Transport Layer Security) gewährleisten die Sicherheit von Online-Transaktionen durch Verschlüsselung. SSL verwendet zur Ver- und Entschlüsselung der Daten zwei Schlüssel: einen öffentlichen, allgemein bekannten Schlüssel, und einen privaten Schlüssel, den nur der Empfänger der Nachricht kennt.

SSL-Zertifikat: Ein SSL-Zertifikat enthält eine digitale Signatur, die einen öffentlichen Schlüssel mit einer Identität verknüpft. Mit SSL-Zertifikaten lassen sich vertrauliche Daten zur Übertragung über das Internet verschlüsseln. Bei extern überprüften Zertifikaten dienen sie außerdem als Bestätigung der Identität des Zertifikatsinhabers.

Falls Sie weitere Fragen haben, schreiben Sie uns oder rufen Sie uns an.:

- **Telefonisch**

  –

  Telefon: +49 9721 / 370 38 1

  Ansprechpartner:
  Marc Dornieden

- **Per E-Mail an info@janotta-partner.de**
- **Besuchen Sie unsere Website:**
  https://www.janotta-partner.de

Janotta & Partner Schulungen bieten Ihnen neuestes Know how der IT Sicherheit sowie der Cybersecuirty Forschung. Wir freuen uns auf Ihren Kontakt.

Mehr zum Kurs

https://janotta-partner.de/kurs-phishing.html

Janotta und Partner
Cybersecurity