Das „Phishing"-Phänomen: Ursprung, Erfolg und Prävention

Seit den ersten Erwähnungen im Jahr 1996 wendet das Phishing-Phänomen zunehmend raffiniertere „Social Engineering"-Techniken an, um sich Zugang zu vertraulichen Informationen zu verschaffen, indem die Gutgläubigkeit der Opfer, die diese empfindlichen Personen- oder Firmendaten aus nicht autorisierten Quellen - in der Regel als Antwort auf elektronische Nachrichten - versenden, ausgenutzt wird. Der Erfolg dieses Phänomens entsteht in der Tat aus der Schwierigkeit heraus, die sich für den durchschnittlichen Nutzer ergibt, eine vom Spammer gesendete, betrügerische E-Mail von einer offiziellen Mail aus vertraulichen Quellen zu unterscheiden, da diese Nachrichten Internetseiten oder Mitteilungen von für den Empfänger bekannten Institutionen durch Graphik und Inhalt nachahmen. Es ist zudem wissenschaftlich erwiesen worden, dass viele Personen gerade auf Spam und Phishing antworten. Die schlechte Nachricht: Ihre Zahl nimmt stetig zu (von 5% im Jahr 2005 auf 10% im Jahr 2007).

GEOGRAPHISCHE HERKUNFT und VERBREITUNG

37 % aller Phishing-Attacken stammen aus den USA, gefolgt von Korea (20%), China, Polen, Japan und Russland. Neben der elektronischen Post stellt nicht nur das Instant Messaging (IM) den wohl gebräuchlichsten Weg für Phishing dar. Des Weiteren gibt es immer mehr Phishing-Webseiten, auf die Benutzer durch sorgfältige Manipulation von Suchmotoren gelockt werden. Phone-Phishing ist, insbesondere mit VoIP-Fähigkeiten, ebenfalls gängig. VoIP-Programme, wie Skype, werden zunehmend zum Versenden von Spam- und Phishing E-Mails genutzt. Doch dabei bleibt es nicht. Selbst im Mobiltelefonbereich fasst Phishing Fuß, indem Applets an das Mobiltelefon des Unglücklichen gesendet werden und dieser, ohne etwas zu ahnen, prompt seine eigenen personenbezogenen Daten eingibt. Letztendlich verbreiten sich Phishing-Nachrichten auch über RSS-Feeds, die normalerweise mit Blogs und öffentlichen Foren verbunden sind, bzw. auch über MP3-Files.

Fakten und statistische Zahlen

- der heutige Email-Verkehr besteht mittlerweile zu über 70% (mit Spitzen von 90% je nach Uhrzeit) aus Spam.
- Phishing macht nur **1% aller Spams** aus.
- Phishing ist ein gezielter Angriff, der zumeist Geldinstituten gilt (92.4% aller Phishing-Nachrichten).
- In der Zeit vom 1. September 2006 bis 31. August 2007 entwendeten Cyber-Kriminelle **allein in den USA** gut 3,2 Milliarden Dollar bei ca. 3,6 Millionen Kontoinhabern, die sich durch falsche E-Mails täuschen ließen, welche dem Anschein nach von der eigenen Bank, dem kreditkartenverwaltenden Geldinstitut oder von Online- Käufen und –Auktionen kamen.

TENDENZEN, ZIELE und ZUKUNFT des PHISHINGS

Die Verbreitung von telematischen Betrügereien und insbesondere von Phishing wird, gerade in Anbetracht des hohen Rentabilitätsindexes, bis zum Jahr 2009 hin zunehmen. Es steht außer Zweifel, dass dieses Phänomen stetig an Zuwachs gewinnt und durch einen progressiven Wechsel von E-Mail-

Phishing zu Phishing im Web 2.0, sowie durch Ausnutzung "alternativer Methoden" (VoIP, Mobiltelefonie, MP3) gefördert wird.

Zur Zeit kommt schon eine Menge an Spam aus „sozialen Netzen", die wie Face-Book, Linkedin, Twitter etc. auf Web 2.0 basieren, oder von Blogs, wo bereits schwer zu erkennen, ob die betreffende Post von akkreditierten Nutzern oder Spammern eingebracht worden ist. Die betrügerische Ausnutzung von Web 2.0-freigegebenen Plattformen wird der gegenwärtigen Nutzung des E-Mailkanals weit überlegen sein: Phisher werden alsbald in der Lage sein, den E-Mailversand durch Übergehen der Anti-Phishing-Instrumente und durch teilweises Umleiten zuverlässiger Webseiten zu umgehen.

In dieser Übergangsphase hat die Anwendung des E-Mailinstrumentes eine weitere Entwicklung auf sich nehmen müssen - das Spear Phishing – ein gezielter Angriff auf ausgesuchte Personen oder Firmen, basierend auf stark spezifischen und höchst personalisierten Social Engineering- Techniken, die Schutz und Warnungen noch schwieriger gestalten lassen. Die Angriffsmethode besteht darin, sich für einen Kollegen auszugeben, der Grund und Recht auf das Einholen vertraulicher Informationen über Informationssysteme oder Personalverwaltungen hat..

Nach ersten „Klon"-Versuchen von Mobilfunkgeräten durch Aufforderung, eine bestimmte Nummer anzurufen, ist in den ersten vier Monaten des Jahres 2008 eine enorme Phishing- Angriffswelle per SMS verzeichnet worden. Die Nachrichten fordern den Nutzer dazu auf, den neuesten Klingelton, das neueste Spiel gratis herunterzuladen oder eine Nummer zur Aktivierung eines neuen „Sondertarifs" anzuwählen.

Sowohl die Ausnutzung der mobilen Carrier- Netze durch Phisher, als auch die an VoIP- Systeme (SPIT - Spam over Internet Telephony) gerichteten Angriffe werden in dem Zweijahreskurs 2008/2009 einen beachtlichen Zuwachs erfahren.

Ob Aufforderungen zum Herunterladen von MP3- Dateien, die Trojanische Pferde tarnen, von betrügerischen E-Mails, die sich kaum noch von "Zulässigen" unterscheiden lassen, von Blogpost, die unter dem Tarnmantel falscher Informationen auf Phishing- Seiten verweist oder von Usefull Tools für die eigene Informatik-Infrastruktur... Alle haben nur ein Ziel: Backdoor-Installationen auf kompromittierten Computern, die für einen Computer- oder Netzwerkzugang sorgen, um an vertrauliche Daten und Informationen zu gelangen. Zuweilen gelingen sogar„Keylogger- Installationen", die den Cybernet-Kriminellen mit Tastenfolgen versorgen, die zur Eingabe von Benutzernamen oder Passwörtern gedrückt worden. Gleichfalls können vom Angreifer Viren installiert werden, die alle Dateien eines besonderen Typs, zu denen der Computer des ahnungslosen Opfers Zugang hat, versenden .

FOLGEN des PHISHINGS

Der durch Spammer/Phisher erzeugte, enorme Verkehr stellt für Provider und Carrier einen riesigen Resourcenverlust dar: zur Bandbreiten-Ausnutzung für betrügerische Zwecke kommt die missbräuchliche Verwendung von E-Mailspeicherplätzen hinzu, deren Archivierungsfähigkeiten nunmehr der Monopolisierung von Spam unterliegen. Neben den wirtschaftlichen Schäden sind auch die rechtlichen Auswirkungen auf den Provider zu bedenken, wenn der Kunde eines Internetproviders oder Telefon-Carriers die Resourcen für Phishing oder Spam nutzt. In Anbetracht des o.g. prozentuellen Spam-Anteils in der elektronischen Post lässt sich auf Firmenebene hingegen der dem einzelnen Angestellten

zugefügte Produktivitätsschaden leicht erkennen, ohne dass hier die wirtschaftliche/das Ansehen beeinträchtigende Belastung berücksichtigt wird, wenn der Angestellte den Phishern ins Netz geht.

METHODEN der ERKENNUNG und PRÄVENTION

Obwohl bereits im Jahr 2006 eine Untersuchung der„Universität von Pittsburg (USA) ausführlich zeigte, dass Reputationsfilter, die auf IP-Adressen von "betrügerischen" Seiten basieren, korrupt sind und aufgrund ihrer raschen Obsoleszenz und mangelnden Qualitätskontrolle gleichermaßen eine beträchtliche Zahl an falschen Positiven (Blockierung vertrauenswürdiger Seiten) und falschen Negativen (gewährleisteter Zugang zu Phishing-Seiten) hervorbringen, wenden viele Hersteller diese Filter zur Spam-Bekämpfung an.

Angesichts der zahlreichen Verbreitungsweisen von Spam gilt der gleichzeitige Einsatz verschiedener Techniken generell als beste Methode zur Phishing- oder Spambekämpfung , wie beispielsweise die Identifizierung von „Early Talkern" (von Spammern ad hoc geschaffene Roboter, um an SMTP- Server möglichst viele Mails in kürzester Zeit zu übermitteln), die Kontrolle unbekannter Empfänger, die Ermittlung eines Domainnamen über die IP-Adresse (Inverse Lookup-Abfrage), die Simulation von Protokoll- und Regelverletzungen, etc., wie auch die gesamtheitliche Anwendung ad hoc entwickelter heuristischer Regeln.

Darüber hinaus stellt das zusätzliche Blockieren eingehender E-Mailverbindungen, noch bevor die elektronischen Nachrichten den Mailserver über das Internet erreicht haben, eine der idealsten Methoden dar, die WAN/LAN- Infrastruktur der Provider /Carrier und Firmen vor unrechtmäßigen Ausnutzungen zu bewahren: je besser die angewandte heuristische Antispam-Engine, desto besser der Schutz gegen Phishing.

HEURISTISCHE REGELN

Heuristische Regeln sind empirische, nicht prognostizierbare Regeln, abgeleitet von fortgeschrittenen Analysen aller Nachrichtenabschnitte: Header-Fields, Betreff-Text, Text und/oder HTML-Code, Name und Inhalt der Anhänge.

Aufgestellt werden heuristische Regeln von Fachleuten, auf der Suche nach unvermuteten, allgemeinen Merkmalen diverser Nachrichten (insbesondere wenn teilweise oder gänzlich automatisch generiert), welche gezwungenermaßen, und ganz gleich welchen Themas, auch durch künftige Spam- und Phishing-Nachrichten verteilt werden. Dieser Prozess wird als "heuristische Voraussage" bezeichnet und ist ein in seiner Art einmaliges System, das von NETASQ für die Antispam-Engine von NETASQ MFILTRO angewandt wird.

WIE FUNKTIONIERT ein PROAKTIVER SCHUTZ

Die heuristische Voraussage stellt ein wesentliches Instrument zur Behebung evtl. Antispam- und Anti-Phishing- Sicherheitslecks in der Zeitspanne dar, die dem Hersteller bleibt, um Analysen vorzunehmen und gegen unbekannte Bedrohungen einzuschreiten.

Mit der heuristischen Voraussage wird das Filtern von unbekannten Phishing-, Virus- und Spam-Attacken ermöglicht, ohne dass Interventionen oder Aktualisierungen der Vorrichtung erforderlich sind, bzw. es einer „Lernkurve" bedarf. Auf diese Weise sind die Nutzer auch geschützt, wenn keine Updates von Antivirus-Lösungen oder Signature-based IPS verfügbar sind. Die Erstellung eines Systems der heuristischen Voraussage besteht darin, nur die Filter-Regeln zu schaffen und beizubehalten, die auf „illegale" E-Mails, die eine hohe Wahrscheinlichkeit haben, nochmals aufzutauchen, basiert sind. Dies erfolgt, ähnlich der Bayes'schen Filterung, nach Identifizierungskriterien, denen folgendes Prinzip zugrunde liegt: viele Ereignisse stehen in gegenseitiger Abhängigkeit und ihre künftige Wiederkehr hängt unmittelbar davon ab, wie oft jenes Ereignis im Vorfeld auftrat.

Eine heuristische Regel kann besonders als „Voraussage" betrachtet werden, wenn sie so entwickelt worden ist, dass sie auf einen spezifischen Angriff anspricht, aber auch weiterhin die Nachfolgenden wirksam blockiert.

DIE NETASQ-LÖSUNG

NETASQ MFILTRO verwendet eine heuristische Anti-Spam Engine mit einer 99.5 % Catch-Rate und nahezu keinen falschen Positiven.

NETASQ MFILTRO stoppt bereits 80% der Spams auf der Ebene der Pop3-Connection durch den gleichzeitigen Einsatz verschiedener Techniken (siehe „Erkennung und Prävention") und die verbleibenden 20% dank der eigenen, fortschrittlichen Engine zur heuristischen Prognose, die sich zahlreicher Module, wie Anti-Phishing, Anti-Spam, BildAnalysen, etc. bedient.

Die NETASQ MFILTRO-Engine zur heuristischen Prognose zeichnet sich im Besonderen in der Erkennung neuer Spam-Techniken, wie Verbreitungen über MP3 und durch fortschrittlichere Social Engineering Techniken aus.

NETASQ MFILTRO- Lösungen bieten mit ihrer einzigartigen Kombination aus verschiedenen heuristischen Antispam-, Antispyware und Antiphishing-Technologien mehrere Vorteile, wie eine Verbesserung des Sicherheitsniveaus für E-Mailbenutzer und deren Produktivitätssteigerung. Mit NETASQ MFILTRO wird die elektronische Post wieder zu dem, was sie einst war: ein effizientes Kommunikationsinstrument.

> *"**Innerhalb weniger Minuten** habe ich NETASQ MFILTRO installiert. Am nächsten Morgen erhielt ich verschiedene Anrufe und alle sagten mir: 'Keine Ahnung, wie Du es angestellt hast, **aber verändere nichts mehr** daran.' Selbstverständlich habe ich ihren Rat befolgt ."*
>
> **Nicolas T.**
> Systemadministrator

Mit der Entscheidung von NETASQ, den Kaspersky Antivirus zusätzlich zu dem vorinstallierten Antivirus-System CLAM-AV zu integrieren, wird dem Benutzer ein bestmöglicher und europaweit vielfach ausgezeichneter Antivirenschutz geboten.

Eine solide Berichtsplattform lässt gleichfalls eine Messung des Return on Investment (ROI) in Echtzeit zu. NETASQ MFILTRO schiebt nicht nur dem Spam einen Riegel vor und schützt vor Phishing, sondern misst auch, wieviel der generell verloren gegangenen Zeit der Benutzer sparen konnte.

NETASQ MFILTRO

mfiltro.netasq.com

NETASQ FRANKREICH
Paris . +33 1 46 21 82 30 . france@netasq.com

NETASQ INTERNATIONAL
BENELUX & NORDICS . Antwerpen . +32 3 242 88 10 . benelux@netasq.com
SPANIEN . Madrid . +34 91 761 0290 . iberia@netasq.com
ITALIEN . Mailand . +39 02 3809 3751 . italia@netasq.com
UK . London . +44 1912574802 . uk@netasq.com
GERMANY . deutschland@netasq.com

NETASQ we secure IT