SECURITY
FACHARTIKEL

Phishing – eine rasant wachsende Problematik

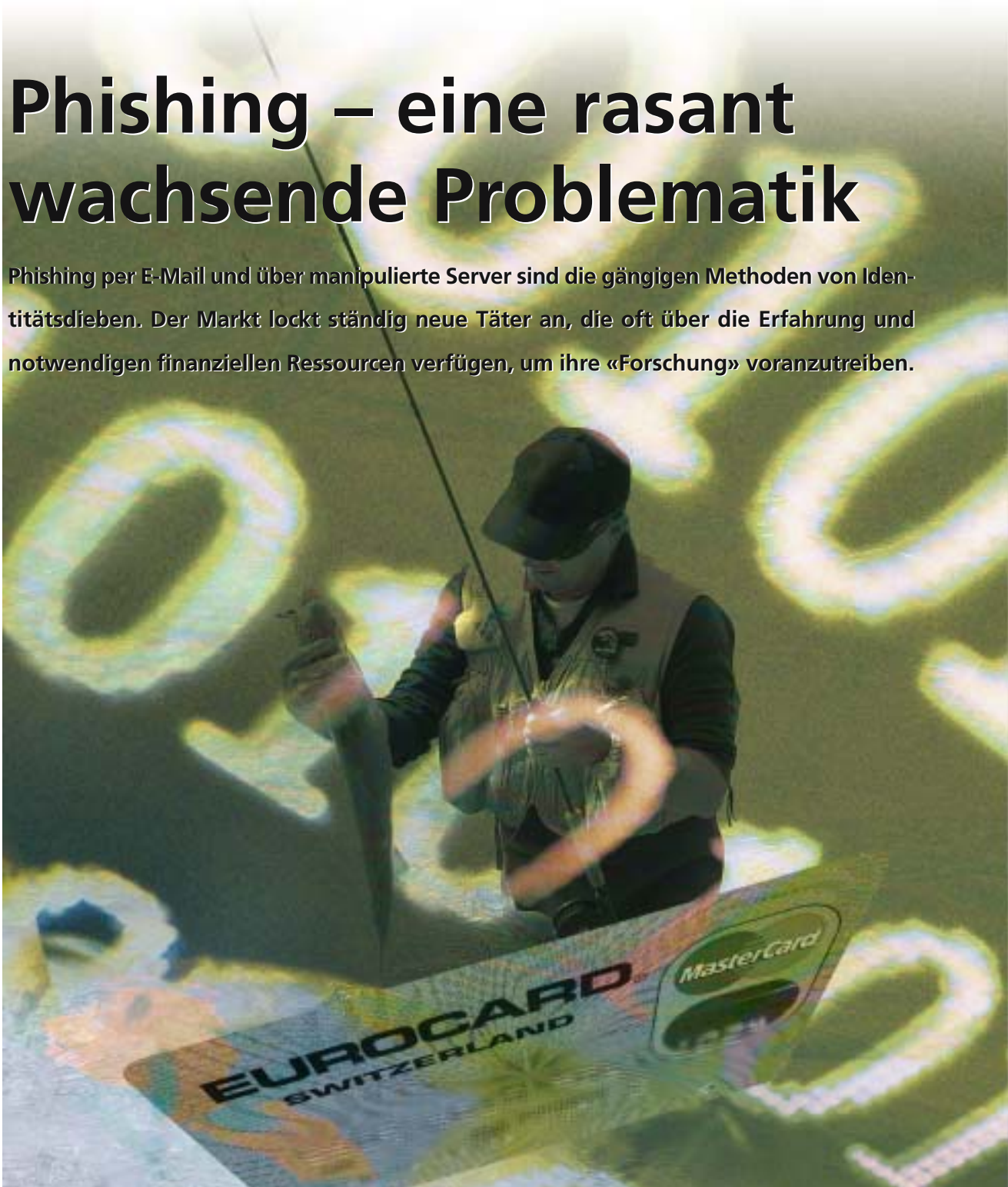
Phishing per E-Mail und über manipulierte Server sind die gängigen Methoden von Identitätsdieben. Der Markt lockt ständig neue Täter an, die oft über die Erfahrung und notwendigen finanziellen Ressourcen verfügen, um ihre «Forschung» voranzutreiben.

von Christoph Fischer

Phishing ist ein Begriff für das unerlaubte Aneignen von fremden Identifikationsmerkmalen. Die Schreibweise mit Ph statt F geht auf den Begriff phreaking zurück, eine in die Jahre gekommene Wortschöpfung der Hackerszene aus phone und freak, die Manipulationen von Telefonvermittlungen beschreibt. Das Phänomen Phishing selbst ist nicht neu, es zielte in der Anfangszeit der EDV-Welt allerdings nur auf den Diebstahl von Benutzerkonten auf Computersystemen oder den Zugang zu Online-Diensten.

Heute wird Phishing professionell im globalen Rahmen und grossen Stil von gut organisierten Gruppen betrieben. Primäre Ziele dieser Banden sind Zugänge zu Bankkonten, Internet-Payment-Systemen und Versteigerungsplattformen.

Die Aktivitäten der Täter haben sich zunächst auf Länder konzentriert, die keine starke Authentifikation, wie Smartcards, Token-Generatoren oder Einmalpasswörter wie TANs verwenden. Speziell sind die USA, England, Australien und Neuseeland betroffen. Hier gehen die Schadenssummen in Millionenbeträge pro Monat. Genaue Zahlen sind sehr schwer zu ermitteln, da es keine verpflichtende zentrale Meldesysteme und entsprechende Dunkelziffern gibt. Vorsichtige Schätzungen gehen allerdings von weltweiten Schäden in dreistelliger Millionenhöhe (Euro) für das Jahr 2005 aus. Die Zuwachsraten sind ebenfalls beängstigend, so lag das monatliche



Wachstum in England für das letzten Quartal zwischen 15% und 32%. Dies bedeutet, die Tätergruppen verfügen über entsprechende finanzielle Ressourcen, um ihre Technik ständig weiter zu entwickeln und die Komplexität des Logistiksystems für die gestohlenen Werte zu perfektionieren.

Wie funktioniert Phishing?

Klassisches Phishing besteht aus einer gefälschten Webseite und einer Massen-E-Mail zur Bewerbung dieser Seite. Die Mehrzahl dieser Werbemails ist in extrem schlechten Englisch oder Deutsch verfasst – und trotzdem ist die Opferzahl erstaunlich hoch. Im Lauf der Zeit wurden die Methoden variiert und verfeinert. Zum einen mussten die Täter den Spam-Filtern ausweichen und durch immer neue Tricks diese Mechanismen austricksen, zum anderen haben die Täter die Gegenwehr der Banken und den von ihnen angeheuerten Dienstleistern zu spüren bekommen.

Heute werden gefälschte Websites in Ländern untergebracht, die für die betroffenen Institute Sprach-, Zeitzonen- und Rechtssystem-Probleme darstellen. Typischerweise werden die Attacken an Wochenenden und Feiertagen gestartet, um die «Überlebenszeit» der Attacke zu maximieren.

Der Zielserver ist meist ein System mit schlechter Wartung, dem die gefälschten Seiten und ein Skript zum Abtransport der «Beute» untergeschoben werden. Der Transport erfolgt in vielen Fällen per E-Mail zu einem Freemail-Provider. Neuere Entwicklungen zeigen einen Trend zur Redundanz. Es werden Spam-Mails mit verschiedenen Adressen ausgesendet, was den Aufwand bei der Bekämpfung vervielfacht, allerdings auch die Chancen für einen Fehler der Täter erhöht. So wurde erst kürzlich ein junger Este verhaftet, der bei seinen vielen Verbindungen eine einzige ohne Tarnung aufbaute.

Die zweite, weitaus erfolgreichere Methode des Phishings basiert auf trojanischen Pferden. Hier erfolgt die initiale Verbreitung ebenfalls via Spam, die auf speziell präparierten Websites lockt. Es wurde bislang ein Spektrum von Pornografieangeboten und gefälschten Rechnungen via E-Mail, bis hin zu einer sehr amateurhaft gestalteten Nachrichtenmeldung über ein Attentat gegen George W. Bush als Verteilmechanismus gesichtet.

Jene Besucher dieser so beworbenen Sites, die ihre Browser nicht besonders abgesichert und nicht in einem absolut aktuellen Pflegezustand gehalten haben, infizieren ihren Rechner mit einem trojanischen Pferd. Ab dem Infektionszeitpunkt werden dann alle für die Täter interessanten Transaktionen abgehört und meist in verschlüsselter Form an einen oder mehrere «tote Briefkästen» im Internet übermittelt.

Das Schlupfloch im Browser, durch das die trojanischen Pferde Zugang zu den Daten erhalten – auch wenn sie in einer sichereren Https-Verbindung übertragen werden –, nennt sich BHO (browser help object). Dies ist kein Ausnutzen eines Bugs, sondern eine kreativ genutzte Eigenschaft des Microsoft Internet Explorer. Die Erfahrung zeigt, dass die Schad-Software zum Zeitpunkt ihrer Entdeckung der Antivirus-Industrie meist unbekannt ist. Dies bedeutet, dass jegliche Präventivwirkung der Antivirus-Software versagt, es sei denn die Kette von Entdeckung, Isolierung, Weiterleitung an die Antivirus-Industrie und das Einspielen der Patches wird perfektioniert. Die Reaktionszeit der Hersteller liegt heute im Mittel zwischen vier Stunden und zwei Tagen.

Die so abgehörten Daten können weitaus brisanter sein als nur die Zugangsdaten für Bankkonten. Viele Unternehmen haben webbasierte Extranet-Anwendungen, die tief in ein Unternehmen greifen können. Eine bessere Absicherung sollte von allen Betreibern von «secure» Webpages im Rahmen einer Risikobewertung in Betracht gezogen werden.

Was kann man gegen diese digitale Wegelagerei tun?

Die erste Gegenmassnahme gegen Phishing heisst Aufklärung. Die meisten interviewten Opfer solcher Attacken konnten sich nicht vorstellen, dass so ein Angriff möglich sein kann und vor allem, dass sie je Ziel einer solchen Attacke sein könnten. Der Zustand der betroffenen Rechner war in fast allen Fällen mangelhaft. Entweder war keine Antivirus-Software installiert oder sie war in sehr schlechtem Wartungszustand. Personal Firewalls wurden keine gefunden, auch waren Betriebssystem-Patches nicht eingespielt worden.

Es wird immer einen gewissen Anteil von Benutzern geben, die nicht durch Awareness-Kampagnen erreicht werden, dennoch ist Aufklärung extrem wichtig, um die Flut der Attacken zumindest teilweise ins Leere laufen zu lassen. Ziele dieser Aufklärungskampagnen sollten neben den Themen «Wie halte ich mein System sauber» auch sein, «Was ist Phishing?» oder «Wie erkenne ich Nebeneffekte eines Angriffs?». Die frühe Meldung eines Angriffs ermöglicht das Stoppen von Zahlungsläufen und das Einleiten von zusätzlichen Massnahmen, die auch andere Opfer schützen.

Neben der Awareness der breiten Masse ist eine Schulung der Hotlines, Kundenberater und des Sicherheitspersonals der Banken dringend notwendig, um eine konsistente und optimale Reaktion auf Phishingattacken zu ermöglichen.

Als Unterstützung der Awarenesskampagnen sollten auch gewisse Verhaltensmuster bei Marketingaktivitäten vermieden werden. Für einen technisch nicht versierten Anwender ist jede E-Mail mit einem vertrauen Absender und dem Logo seiner Bank ein Original. Grundsätzliche Überlegungen beim Aufstellen von Policies zur Verwendung von E-Mail können hier eine falsche Konditionierung der Anwender verhindern.

Bei dem technischen Aufbau von Websites ergeben sich viele Möglichkeiten, präventive Schritte gegen den Missbrauch und das all zu leichte Nachstellen der Webpräsenz einzuleiten. Neben klassischen Angriffspunkten mit Cross-site-scripting und Frame hijacking sind Pop-up-Fenster eine typische Falle.

Das Einrichten einer zentralen Ansprechstelle für derartige Angriffe oder zumindest deutlich erkennbare Informationen auf den einzelnen Websites der Banken würden die Meldewege verbessern und somit kritische Verzögerungen vermeiden.

Schliesslich ist auch der Staat gefordert, mit entsprechender Entschlossenheit zu reagieren. Strafrechtliche Verfolgung ist eine Komponente, die ohne grössere Probleme angewendet werden kann, aber die zeitnahe Reaktion, um Schäden zu minimieren und eine Rückverfolgung zu ermöglichen, ist nur selten zu finden. Die Mechanismen der internationalen Zusammenarbeit sind auf die Herausforderungen dieser digitalen Katz- und Maus-Spiele nicht vorbereitet.

Ausblick

Die enormen Gewinne der Angreifer haben einen Markt geschaffen, der mehr Täter anlocken wird. Die etablierten Gruppierungen haben sowohl die Erfahrung, als auch die notwendigen finanziellen Ressourcen, um ihre «Forschung» voranzutreiben und sich breit aufzustellen. Phishing wird, wie die Viren-Thematik, ein Dauerbrenner werden. Es ist dringend notwendig, über neue Sicherheitsmechanismen bei webbasiertem Banking und anderen Transaktionen nachzudenken. In der Zwischenzeit kann nur eine Mischung aus Vorsorge- und Notfallmassnahmen das Schadenpotenzial in Grenzen halten. ■

Der Artikel basiert auf einem Referat, das der deutsche IT-Security-Experte Christoph Fischer anlässlich des bwsecurity day 2005 im Hotel Mövenpick Zürich-Regensdorf hielt.