 Diesen Artikel können Sie als Audiodatei beziehen; siehe www.spektrum.de/audio

COMPUTER
an der Angel

Um sensible Daten wie Passwörter und Bankverbindungen im Internet auszuspähen, setzen Kriminelle auf raffinierte Techniken – und auf einen naiven Umgang der Nutzer mit elektronischer Post.

Von Lorrie Faith Cranor

Wer würde da nicht erschrecken? Innerhalb weniger Wochen warnten mich E-Mails, dass meine Onlinebankdienste Gefahr liefen, deaktiviert zu werden, mein E-Bay-Passwort geändert werden müsse und Rechnungen für Musik-Downloads noch offenstünden. Zudem enthielt das elektronische Postfach noch die Information, die Zugangsdaten zu meinem Mailservice würden sich ändern, das Angebot einer Fluggesellschaft, gegen einen ansehnlichen Betrag an einer Onlineumfrage teilzunehmen sowie einen Spendenaufruf anlässlich drohender Hungersnöte in der Dritten Welt. Alle diese Nachrichten stammten dem Absender wie dem Erscheinungsbild der Mail nach von namhaften Unternehmen und Organisationen. Aber mit Ausnahme der Aufforderung von E-Bay stammten sie ausnahmslos von Kriminellen.

So genannte Phishing-E-Mails fischen nach Informationen, die sich zu Geld machen lassen: Zugangsdaten zu Bankkonten, Kreditkartennummern, Benutzernamen und Passwörter zu Onlineshops. Diese elektronischen Briefe sehen unverdächtig aus, stammen oft scheinbar von bekannten Firmen und fordern stets zu einer dringlichen Aktion auf, um entweder negative Konsequenzen zu vermeiden oder eine Belohnung zu erhalten. Der Empfänger soll typischerweise vertrauliche Informationen in ein Formular eintragen, einen Weblink anklicken oder einen Anhang öffnen. Nicht selten werden in den letzten beiden Fällen unbemerkt Trojaner genannte Schadprogramme auf dem Computer des Empfängers installiert, die einen Zugriff auf die erwünschten Daten verschaffen oder den Rechner bei künftigen Angriffen im Netz mit einspannen.

Die Anti-Phishing Working Group, ein internationales Konsortium aus Organisationen, die dem Internetbetrug den Kampf angesagt haben, behält solche Aktivitäten im Auge, einschließlich der Zahl der in jedem Monat entdeckten Phishing-Webadressen. Im April 2007 erreichten diese einen Spitzenwert von 55 643, im Juni 2009 wurde der zweithöchste Wert

COMPUTER: CHAD BAKER; ANGELHAKEN: GETTY IMAGES / RIKO PICTURES

von 49 084 gemessen. Wurden 2007 noch 92 bis 178 Firmennamen und -logos pro Monat missbraucht, um Opfer zu täuschen, waren es in der ersten Hälfte 2009 259 bis 310. Nach Angaben der Forschungs- und Beratungsfirma Gartner fielen 2007 geschätzte 3,6 Millionen Amerikaner Phishing-Attacken zum Opfer, ihr Verlust belief sich auf mehr als 3,2 Milliarden US-Dollar; im Jahr darauf war die Opferzahl auf mehr als fünf Millionen gestiegen, aktuelle Zahlen liegen noch nicht vor (Stand November 2009; zur Situation in Deutschland siehe Kasten S. 94).

Phish? Eine Rockband?

Spezielle E-Mail-Filter und Webbrowser warnen vor Phishing-Attacken, doch leider gelingt es kriminellen Softwareentwicklern immer wieder, kommerziellen Sicherheitsprogrammen einen Schritt voraus zu sein. Zudem ist ein Teil des Problems nicht technischer Natur: Phishing hat nur dann Erfolg, wenn der E-Mail-Empfänger sich täuschen lässt beziehungsweise entsprechende Schutzprogramme entweder nicht aktiviert oder ihre Warnungen missachtet. Deshalb untersucht meine Forschungsgruppe an der Carnegie Mellon University die Möglichkeiten, Internetnutzer zu schulen. Umgekehrt hilft diese Forschung, Anti-Phishing-Software zu entwickeln, die mit höherer Wahrscheinlichkeit korrekt benutzt wird.

Als wir 2004 mit unserem Projekt begannen, rekrutierten wir Personen auf den Straßen von Pittsburgh. Die meisten hatten keine Ahnung, wovon wir sprachen, und nahmen an, dass der Begriff Phishing etwas mit der US-amerikanischen Rockband Phish zu tun habe. Die wenigsten wussten eine Betrugsmail zu erkennen. Selbst die von einem Webbrowser angezeigten Sicherheitswarnungen wurden nur selten verstanden.

Das irritierte, denn Firmen, Behörden und Industrieverbände widmeten damals bereits Websites diesem Thema, um die Bevölkerung aufzuklären. Wir recherchierten und kamen zu dem Schluss: Viele waren in zu technischem Jargon verfasst und überforderten

In Kürze

- Als Phishing bezeichnet man das **Ausspähen sicherheitsrelevanter Informationen** wie Passwörter oder Bankverbindungen.
- Phisher verleiten ihre Opfer durch **fingierte Mails** dazu, sensible Daten in Abfragemasken einzugeben. Alternativ versuchen sie, deren Computer mit Spionagesoftware zu infizieren.
- Da Phishing **menschliche Schwächen** ausnutzt, verspricht eine Kombination von Schulung und anerkannter Sicherheitssoftware den besten Schutz.

SUSPEKTE SEITEN

Misstrauen Sie Webseiten mit folgenden Eigenheiten:

- **Alter der Domain**
  kleiner gleich zwölf Monate
- **bekannte Logos**
  Die Seite gehört zu keiner Domain des Logoeigners.
- **verdächtige Adresse**
  URL beinhaltet das @-Zeichen, einen Bindestrich, eine IP-Adresse oder mehr als fünf Punkte.
- **verdächtige Links**
  Der Link auf der Seite enthält ein @, einen Bindestrich oder einen Schreibfehler.
- **lexikalische Signatur**
  Die URL stimmt nicht mit der Adresse der durch Google hoch bewerteten gleichnamigen Webseite überein.

Computernutzer mit einem Überangebot an Informationen, andere lieferten zu wenig konkrete Ratschläge, wie man sich schützen könne.

Bei Untersuchungen unter Laborbedingungen zeigte sich auch bald, dass ein eher theoretisches Bewusstsein dieser Bedrohung nicht genügt, um auch ein adäquates Verhalten zu motivieren. Nicht selten werden Warnhinweise, wie sie Firmen an ihre Mitarbeiter und Kunden verschicken, schlicht ignoriert. Probanden ließen sich sogar leichter verleiten, fingierte Mails zu lesen als offenkundig sicherheitsrelevante Nachrichten.

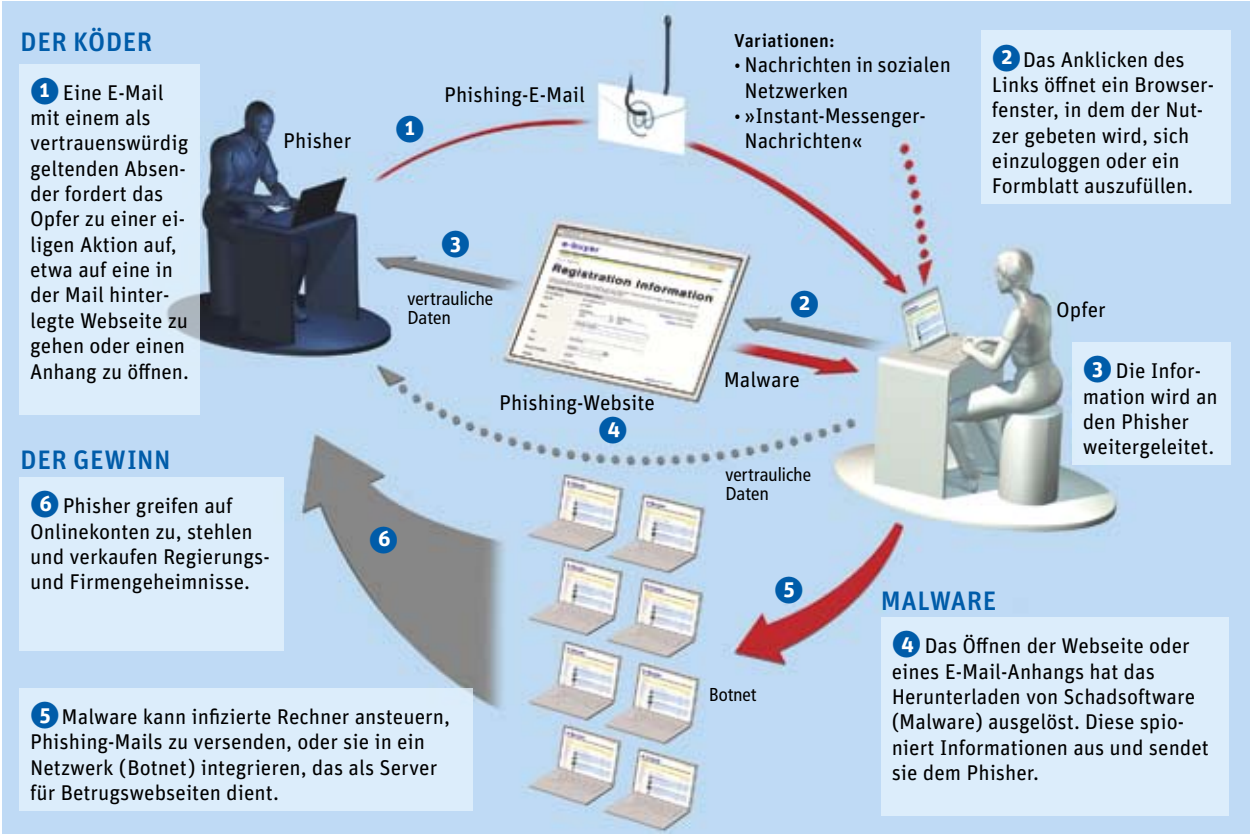
Mein Team entwickelte ein Trainingssystem, das Cartoons einsetzt. Die Figur Phish-Guru unterrichtet mögliche Opfer darin, wie sie sich selbst schützen können. Als besonders effektiv erwies es sich, unsere Probanden vor dem Training mit simulierten Phishing-Mails zu überrumpeln: Auch eine Woche nach der Unterweisung erinnerten sie sich an ihre Lektionen und ließen sich nicht täuschen.

Darauf aufbauend entwickelte mein Doktorand Steve Sheng ein Onlinetrainingsspiel namens Anti-Phishing Phil, das nicht nur das Rüstzeug dafür liefert, verdächtige Webadressen zu erkennen, sondern auch die Erfahrung vermittelt, wie es ist, einem Phisher ins Netz zu gehen (siehe Bild S. 95). In Labor- und Feldstudien konnten wir die Wirksamkeit dieser Software nachweisen. Die Zahl falsch-negativer Erkennung, also irrtümlich für seriös gehaltener Webseiten, nahm ebenso deutlich ab wie falsch-positive Identifizierungen, die irrtümliche Ablehnung harmloser Seiten. Wer Anti-Phishing Phil erlebt hatte, schnitt im Durchschnitt auch besser ab als Teilnehmer anderer Trainingsprogramme.

Da die Entwickler von Schadsoftware dazulernen und ihre Strategien ändern, genügt eine einmalige Fortbildung leider nicht. Selbst professionelle Computeranwender müssen sich immer wieder auf den aktuellen Stand bringen. Die Anti-Phishing Working Group (APWG) berichtet, dass beispielsweise die Infektion von Computern mit Trojaner genannten Schadprogrammen, die Passworte und andere persönliche Daten ausspähen, dramatisch zunimmt. Attacken, die auf ihre Opfer hin

WIE PHISHING FUNKTIONIERT

Um Zugangskodes zu erfahren, verschicken Verbrecher Mails, die anscheinend von einer vertrauenswürdigen Firma oder Person stammen. Wer der darin enthaltenen Aufforderung folgt, riskiert hohen finanziellen Schaden.



maßgeschneidert sind, sind ebenfalls ein Trend; man spricht anschaulich vom Speer-Phishing. Beispielsweise werden E-Mails an Firmenangehörige verschickt, als deren Absender ein Manager des Unternehmens firmiert. Wie leicht lässt man sich täuschen und öffnet den Anhang oder klickt auf den Weblink.

Gute Seiten, schlechte Seiten

In vielen Browsern sind bereits Sicherheitsfilter eingebaut, andere entdecken verdächtige Websites mit Hilfe von Add-ons, also kleinen Zusatzprogrammen. Doch alle Raffinesse der Entwickler ist vergebens, wenn deren Warnungen nicht verstanden werden. Solche Probleme melden Gruppen wie die unsere an die Hersteller. Schon deshalb empfiehlt es sich, Internetsoftware immer auf dem neuesten Stand zu halten.

Zusätzlich zur Erkennbarkeit beeinflusst auch die Verlässlichkeit das Nutzerverhalten. Eine hohe Rate falsch-positiver Entscheidungen erschüttert die Glaubwürdigkeit eines Filters, und seine Warnungen werden leicht ignoriert. Die von uns getesteten Werkzeuge kombinieren verschiedene Methoden, um Betrugsnachrichten und kriminelle Websites zu identifizieren. So gibt es Listen erkannter Webadressen (Blacklists), die ständig aktualisiert werden, beziehungsweise Tabellen seriöser Seiten (Whitelists).

Einige Filter analysieren besuchte Internetseiten anhand von Heuristiken (siehe auch die Randspalte links). So sind Webadressen verdächtig, die denen wohl bekannter Marken ähneln wie etwa »www.annazon.com« (ein Kriterium, das wir auch in unseren Schulungen lehren). Da Betrugsseiten typischerweise nur Stunden bis Wochen aktiv sind, überprüfen die Programme auch das Alter einer Seite. Dieses Kriterium kann die Erkennungsrate drastisch verbessern. So testeten wir 2008 acht Anti-Phishing-Programme mit neuen Betrugsseiten. Programme, die sich ausschließlich auf Blacklists stützten, erkannten zunächst nur 20 Prozent davon, und erst nach fünf Stunden erreichten die meisten eine Quote von immerhin 60 Prozent. Solche aber, die zudem Heuristiken nutzten, identifi-

Erkennen phishiger E-Mails

Ein Markenname, einer Institution oder gar der Name eines Mitarbeiters suggerieren Vertrauenswürdigkeit. Anhand diverser Merkmale können Computernutzer und spezielle Programme fingierte Nachrichten aber dennoch als solche erkennen.

Typische Merkmale

professionelles Layout, bekanntes Firmenlogo

eilige Angelegenheit, die eine Aktion fordert

Warnung, falls Aktion nicht erfolgt

Hinweis auf Phishing-Mails
Wird der Cursor über den Link geführt, entspricht die in einer Browserzeile erscheinende Adresse nicht der im Text angezeigten.

Betreff: Musterbank Eilige E-Mail-Verifikation
Von: »Musterbank« Kreditkarten@Musterbank.de
Datum: Mon, 06. Juli 2009, 15.12.43
An: Mustermann@provider.de
Priorität: Normal
Optionen: View Full Header | View Printable Version

MusterBank

Sehr geehrte(r) Musterbankkunde,

Diese E-Mail wurde Ihnen vom Musterbank-Server gesandt, um Ihre E-Mail-Adresse zu verifizieren. Sie müssen diesen Vorgang abschließen, indem Sie hier oder auf den Link weiter unten klicken und sich mit Ihrem Musterbank-Nutzernamen und Passwort anmelden. Dies dient Ihrem eigenen Schutz – weil einige unserer Kunden keinen Zugang mehr zu ihren E-Mail-Adressen haben und wir dies verifizieren müssen. Aus Gründen der Sicherheit sind wir gezwungen, Ihren Kontozugang einzuschränken, falls Ihre Zugangsdaten nicht innerhalb der nächsten 72 Stunden verifiziert werden.

Um Ihre E-Mail-Adresse zu bestätigen und Zugang zu Ihrem Bankkonto zu erhalten, klicken Sie auf den Link weiter unten. Falls nach Anklicken des Links nichts geschieht, kopieren Sie den Link und fügen Sie ihn in die Adressleiste Ihres Webbrowsers ein.

http://www.MusterBank.de/EMailVerifikation

Vielen Dank

Ihr Kontomanagement

http://musterbank-OnlineKonto.de/KontoZusammenfassung.htm?verify=email

Kriterien für Softwarefilter

HTML- oder JavaScript-Kode – der auch in seriösen E-Mails vorkommt – ermöglicht es, verlinkte Internetadressen zu verbergen.

Webadressen von Firmen vermitteln Authentizität, der Link aber leitet zu einer anderen Seite.

Phishing-Domains sind meist kurzlebig; ein Filter kann entsprechende Listen befragen, ob die in der Mail verlinkte Webseite schon länger existiert.

zierten von Anfang an fast 90 Prozent der Phishing-Attacken.

Erfolg versprechen auch Analysetechniken des Maschinenlernens. Mein Mitarbeiter Norman Sadeh versucht mit diesen Verfahren Merkmale auszumachen, die bezeichnend für Phishing sein können. Zum Beispiel gibt es in solchen Mails oft Weblinks, die im lesbaren Text wie die Adresse einer bekannten und seriösen Website aussehen – tatsächlich aber durch den hinterlegten Computerkode auf die Seite des Angreifers führen. Andere Adressen enthalten oft fünf und mehr Punkte und verweisen auf Domainnamen, die erst kürzlich den internationalen Domainservern gemeldet wurden. Doch diese beiden Kriterien sind nicht hundertprozentig scharf, denn es gibt Betrugs-E-Mails ohne diese Merkmale, und mitunter treffen sie auch auf seriöse E-Mails zu. Deshalb trainieren meine Mitarbeiter unser Programm PhishPatrol anhand einer großen Sammlung seriöser und betrügerischer E-Mails. Es analysiert sie und lernt selbstständig, welche Merkmalkombination höchstwahrscheinlich korrekt auf Phishing hinweist. Inzwischen erkennt PhishPatrol mehr als 95 Prozent der kriminellen E-Mails und liefert nur bei etwa 0,1 Prozent der seriösen Nachrichten fälschlicherweise Warnungen.

Wir haben auch einige der dort genutzten Strategien mit anderen Ansätzen kombiniert. Jason Hong leitete in unserer Gruppe die Entwicklung der Software Cantina, die den Inhalt einer Internetseite und verschiedene andere Merkmale bewertet. Cantina nutzt zunächst einen gängigen Algorithmus, um auf dieser Seite fünf Begriffe zu identifizieren, die offenbar wichtig, im Internet insgesamt aber vergleichsweise ungebräuchlich sind. Eine solche lexikalische Signatur der Login-Seite von E-Bay ergäbe vielleicht »E-Bay, Mitgliedsname, einloggen, Hilfe, vergessen«. Würde man umgekehrt diese fünf Ausdrücke in die Google-Suchmaschine eintragen, sollte die Login-Seite von E-Bay unter den obersten Suchergebnissen erscheinen. Phishing-Websites, die sich den Anschein dieser Seite geben, dürften eher nicht auftauchen. Denn eines der Kriterien, das Googles proprietärer Algorithmus zum Ranking von Seiten nutzt, ist die Anzahl der von anderen Adressen dorthin führenden Links. Allerdings ist das keine unfehlbare Methode, besonders dann, wenn eine seriöse Website erst kürzlich kreiert wurde; folglich ist es nur eines von mehreren Merkmalen, das Cantina berücksichtigt.

Täuschend echt – simulierte Internetportale

Im Kampf gegen diese Form der Onlinekriminalität entdeckt auch die Gegenseite immer neue Angriffsmöglichkeiten: Phishing-Nachrichten werden via Instant Messenger und Handy-SMS versandt; Teilnehmer des beliebten Onlinespiels »World of Warcraft« erhielten fingierte E-Mails des Betreibers. Über die Kurznachrichtendienste sozialer Netzwerke wie Facebook wurden »klassische« Pornolockangebote verbreitet – etwa mit Betreffzeilen wie »Wurden diese Fotos wirklich ins Netz

Phishing in der Bundesrepublik

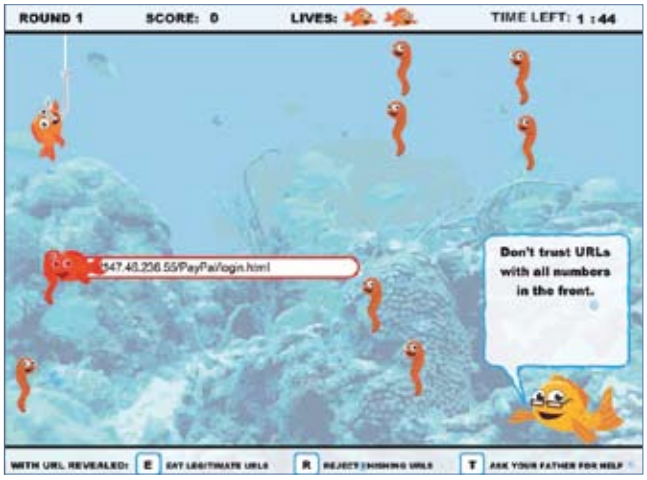
Nach Angaben des Bundeskriminalamts stieg die Zahl der registrierten Fälle in den Jahren 2005 bis 2007 von 2500 auf 4200, sank aber 2008 zunächst auf 1778, vermutlich auf Grund der flächendeckenden Einführung des iTAN-Systems beim Onlinebanking. Entwarnung gibt die Behörde aber nicht: Seit Ende 2008 klettern die Zahlen wieder nach oben, und vermehrt wurde das iTAN-System überwunden.

Auch die Schadenssummen wachsen, sie erreichten 2008 häufig Beträge von 10 000 Euro. Neben Bankdaten hätten es Kriminelle laut BKA zunehmend auf die digitale Identität der Bürger abgesehen. Der Diebstahl von Kreditkartennummern, Zugangsdaten bei Auktionshäusern oder Passwörtern für soziale Netzwerke und Aktiendepots nahm 2008 um rund zehn Prozent auf mehr als 37 000 Fälle zu.

Laut BKA kommen in Europa inzwischen hauptsächlich Trojaner zum Einsatz, die unbemerkt die Eingaben des Nutzers protokollieren. Sie gelangen als Anhang einer Mail auf den Computer, via Download oder als Drive-by-Infection, einer unbemerkten »Ansteckung« beim Besuch einer infizierten Webseite. Insgesamt sollen 25 bis 30 Prozent der in Deutschland mit dem Internet verbundenen Rechner bereits von Schadsoftware befallen sein, schätzen Hersteller von Anti-Virus-Programmen und Sicherheitsdienstleister.

Das BKA empfiehlt deshalb:

- nie ohne Firewall und Virenschutz ins Internet
- Virenschutz-, Browser- und E-Mail-Software aktuell halten
- Vorsicht beim Öffnen von Mail-Anhängen
- keinen Links folgen, die per Mail einer angeblichen Bank kommen
- keine TANs eingeben, wenn keine Überweisung vorgenommen wird
- ungewöhnliche Fehlermeldungen beim Onlinebanking sofort der Bank melden und den eigenen Zugang sperren lassen
- regelmäßig Kontoauszüge prüfen
- für alle sicherheitsrelevanten Internetaktivitäten wie das Onlinebanking einen extra Rechner verwenden
- Vorsicht bei Jobangeboten im Internet: Wer sich als *mule* anwerben lässt, macht sich mindestens der Geldwäsche schuldig.



CMU USABLE PRIVACY AND SECURITY LABORATORY & WOMBAT SECURITY TECHNOLOGIES INC.

gestellt?« –, die einen Link enthielten, der zu einer simulierten Facebook-Login-Seite führte. Raffinierterweise leiteten die Phishing-Seiten nach Eingabe der Zugangsdaten tatsächlich an die richtige Adresse weiter. In eine ähnliche Falle kann die Einwahl in ein öffentliches WLAN führen.

Eine Variante des Phishing erlebt derzeit ein exponentielles Wachstum: betrügerische Schutzsoftware. So wurden Besucher der Webseite der »New York Times« im vergangenen September nach dem Anklicken eines Werbebanners vor einer möglichen Infektion ihres Rechners gewarnt und der Erwerb eines Anti-Virus-Programms empfohlen. Wer dem nachgab, war sein Geld los, denn was sich dann installierte, gab nur vor, ein Schutzprogramm zu sein. Tatsächlich richtete die Malware eher Schaden an, da sie die Sicherheitsstufe des Internet Explorers und Windows-Systemeinstellungen veränderte. Nach Auskunft der APWG hatte sich die Zahl solcher Fälle betrügerischer *(rogue)* Anti-Malware-Programme international von etwa 22 000 im Januar auf mehr als 152 000 im Juni 2009 erhöht. Der besondere Reiz für die Phisher: Solche Software ist für echte Schutzprogramme schwer zu erkennen, solange sie nicht zusätzlich Trojaner und dergleichen installiert. Denn letztlich gibt sie nur vor, etwas anderes zu sein, als sie ist. Gut 200 Gangs weltweit folgen diesem »Geschäftsmodell«.

Längst sind keine Kleinkriminellen mehr am Werk, sondern Profis. Organisierte Phisher-Banden wie die vermutlich von Osteuropa aus agierende »Rock Phish Gang« setzen Tausende von mit Trojanern infizierte Computern ahnungsloser Nutzer für ihre Attacken ein. Dass es sich nicht um ein marginales Problem handelt, verdeutlicht die Statistik. Laut der jüngsten Erhebung von Panda Labs, einem Forschungsnetzwerk und Anbieter von Schutzsoftware, waren von mehr als 20 Millionen Rechnern weltweit Mitte 2009 54 Prozent mit Schadsoftware aller Art infiziert, während es Ende 2008 noch 35 Prozent gewesen waren.

Befallene Computer versenden Betrugsmails und maskieren so die Internetadresse der eigentlichen Phishing-Website. Eine andere von diesen Banden genutzte Taktik, um den Ausgangspunkt eines netzweiten Angriffs zu verschleiern, ist die von Sicherheitsexperten Fast-Flux genannte Methode: Den Kriminellen gelingt es, die Domainname-Server zu manipulieren, also die Knotenrechner, die eine Adresse wie »www.spektrum.de« in eine aus Zahlen bestehende Adresse umsetzen. Die Banden sorgen durch ihren Eingriff dafür, dass die Server ständig die zum Domainnamen der Betrugsseite korrespondierende numerische Adresse ändern.

Überraschenderweise werden Phishing-E-Mails nicht unbedingt von dubiosen Servern schwer kontrollierbarer Inselstaaten verschickt. Nach Auskunft von Avira, einem deutschen Hersteller von Sicherheitssoftware, stammen mehr als 14 Prozent der deutschen Phishing-E-Mails auch von deutschen Servern. Im internationalen Vergleich allerdings kommen sie nur auf zwei bis drei Prozent, den Spitzenplatz infizierter Webseiten belegt inzwischen China mit 36 Prozent im Juni 2009 vor den USA mit »nur« 29 Prozent.

Bei aller technischen Raffinesse sind Phisher mitunter doch auf menschliche Hilfe angewiesen, und hier kommen wieder arglose Gutgläubigkeit oder Gier ins Spiel. Um ihre Identität beim Zugriff auf ein fremdes Konto zu verdecken, rekrutieren sie *mules* (Maulesel) für angebliche Heimarbeitsplätze oder scheinbare Gefälligkeiten. Deren Tätigkeit besteht im Transferieren von Geld. Kommen Ermittler diesen oft ahnungslosen Personen auf die Spur, gilt der Grundsatz: Unwissenheit schützt nicht vor Strafe. ◁

Onlinetraining gegen Onlinekriminalität: Bei »Anti-Phishing Phil« schlüpfen Spieler in die Rolle des Fisches Phil, der sich entscheiden muss, ob er einen mit einer URL verbundenen Wurm frisst oder ihn zurückweist (links). Während und nach jeder Runde wird das Verhalten kommentiert, und es werden Tipps gegeben (rechts). In Laborstudien erkannten derart geschulte Probanden infizierte Webseiten sehr viel besser als solche, die mit Standardmaterial trainiert wurden.

Lorrie Faith Cranor lehrt Informatik an der Carnegie Mellon University in Pittsburgh (Pennsylvania) und leitet dort ein Labor zum Themenbereich »Schutz persönlicher und sicherheitsrelevanter Daten«. Mit Wombat Security Technologies Inc. will sie die entwickelten Anti-Phishing-Verfahren vermarkten.

Weblinks zu diesem Thema finden Sie unter www.spektrum.de/artikel/1014874.