Das programmierte Verbrechen

Der Verein „Mimikama“ kämpft gegen Fakes und Fallen im Netz. Das Ziel: Aus Usern sollen aufgeklärte Nutzer werden.

TEXT CHRISTIAN SCHWEPPE
ILLUSTRATION FRIEDERIKE HANTEL

AN DIESEM MORGEN lehnt der Kämpfer Andre Wolf, 38, lässig in seinem Lederstuhl, noch herrscht Ruhe. Auf dem Schreibtisch stehen zwei Monitore und eine Facebook-Tasse. Neben Wolf sitzt Tom Wannenmacher, 46, der Mitkämpfer: verschränkte Arme, sanfter Blick. Ihr Büro liegt im 3. Wiener Gemeindebezirk und hat ein ganz besonderes Feature: Es ist ein kleiner, roter Knopf an der Wand. Drückt man ihn, wird es laut: „Warning, Warning, Bullshit-Alert!“

Andre Wolf und Tom Wannenmacher kämpfen gegen Betrug im Internet. „Mimikama“ heißt ihr Verein, was in der afrikanischen Sprache Kisuaheli „gefällt mir“ bedeutet. Vereinsziel ist, Betrug im Netz aufzudecken, Fakes zu identifizieren und aus Usern aufgeklärte Nutzer zu machen. Jeden Tag werden dem Verein verdächtige Websites, Links, Schadprogramme und zweifelhafte Berichte über plötzlich verstorbene Promis gemeldet. Weil Wolf und Wannenmacher diesen Hinweisen nachgehen und Fakes und Fallen identifizieren, haben die beiden ihren Spitznamen weg: Bullshitbuster. Das Wegräumen des Bullshits ist für die beiden eine Mission. Wolf hat seine Heimat Deutschland dafür verlassen, Wannenmacher seinen Job als Grafikdesigner hingeschmissen. Der Kampf läuft.

Der Bullshit ist zu alltäglich, um noch Schlagzeilen zu machen. Die sind reserviert für spektakuläre Cybercrimes: Attacken auf den Bundestag oder das NRW-Innenministerium, auf Krankenhäuser oder Wasserversorgungssysteme. Klar, der Schaden ist hier auch besonders groß. Nach Angaben der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) haben technische Ausfälle und Angriffe auf Informationssysteme bereits zu jährlichen Verlusten zwischen 260 und 340 Milliarden Euro geführt.

Doch dass nicht nur Unternehmen und Behörden Ziel von Internetkriminellen werden können, sondern jeder von uns, das ist den meisten Menschen bewusst. Laut einer im Februar 2015 veröffentlichten Eurobarometer-Umfrage machen EU-Bürger sich große Sorgen: 85 Prozent sind der Meinung, dass das Risiko steige, Opfer von Internetkriminalität zu werden. Und natürlich: Je mehr die Menschen ihr Leben ins Netz verlegen, desto größer das Risiko. Nach Angaben der Kommission sind Tag für Tag mehr als 150 000 Viren und andere Schadcodes im Umlauf – das programmierte Verbrechen.

Mimikama arbeitet auch mit deutschen Bundes- und Landesbehörden, IT-Firmen und Verbraucherzentralen zusammen, um den digitalen Abzockern und ihren neuesten Maschen auf die Spur zu kommen und die Menschen zu warnen. Doch die Halbwertszeit der Warnungen ist kurz: „Der neueste Betrugstrend ist meist drei Wochen später wieder vergessen“, sagt Wolf. Deswegen ist die Verteidigungsstrategie, zu der er rät, umso beständiger: sich mit Angreifern und ihren Tricks und Taktiken auseinanderzusetzen.

Trick 1

Vom Gewinner zum Verlierer – Fallen auf Facebook

Auf Facebook werden Gratis-iPhones angeboten oder Audis verlost. Doch wehe, ein User klickt darauf. Denn dann wird er auf eine andere Internetseite umgeleitet und dazu verführt, Namen, Anschrift oder E-Mail-Adresse einzugeben. Oder beim nächsten Klick hat er schon ein Abo abgeschlossen, für was auch immer. Beim Smartphone reicht manchmal schon ein einziger Klick, und die Falle schnappt zu.

Facebook ist eine besonders attraktive Plattform für solche Betrügereien, denn allein in Deutschland gibt es derzeit mehr als 27 Millionen Nutzer. Sie alle teilen Bilder, Videos und Statusmeldungen, sind neugierig und manchmal unvorsichtig.

Zum Klicken locken auch angeblich sensationelle Videos von Riesenschlangen oder Riesenbrüsten. Manchmal werden Nachrichtenseiten gefaket, auch gefälschte Artikel der SPIEGEL-Gruppe gab es bereits.

Adressen werden über angebliche Gewinnspiele gesammelt, die auf Facebook beworben werden. Für die Betrüger ist das ein einträgliches Geschäft. Der Nutzer hat anschließend noch mehr Werbe-Mails im Postfach.

Besonders perfide sind Fake-Meldungen wie falsche Todesmeldungen von Schauspielern oder Sportstars, die so sensationell sind, dass der Verstand ausgeschaltet wird und der User schnell klickt. Zuletzt kursierten beispielsweise Meldungen über einen Selbstmord von Stefan Raab und einen Autounfall von Oliver Kahn. „Auch Schumi ist gestern erst wieder gestorben“, sagt Andre Wolf.

Die Masche mit falschen Todesmeldungen sei besonders beliebt, sagt er. Sie setzt auf das Überraschungsmoment in einer immer schnelleren Digitalwelt. Wolf sagt: „Genau für solche Fälle brauchen User mehr Medienkompetenz. Denn der Trick ist schnell durchschaubar.“

HOAX: Eine Falschmeldung oder ein Gerücht. Früher oft per E-Mail versandt, heute eines der größten Probleme von Facebook.

VIREN: Das sind kleine Programme, die beispielsweise als Anhang auf einen Computer eingeschleust werden. Sie können zum kompletten Datenverlust führen. Die Übergänge zu anderen Formen von Schadprogrammen sind fließend. Der klassische Virus ist darauf angelegt, einen Computer zu zerstören oder zu beschädigen.

Trick 2

Eine neue Generation der Betrugsmail – Phishing 2.0

Die wohl bekannteste Form des Internetbetrugs ist Phishing, also das Kombinieren fingierter E-Mails mit gefälschten Websites. Das Ziel der Kriminellen: sensible Daten wie Kreditkartennummern, PINs und TANs oder Passwörter abzufischen. Die E-Mails sehen täuschend echt aus, sind aber doch nur Täuschung.

„Es ist schon lange nicht mehr so, dass Phishingmails billig in gebrochenem Deutsch daherkommen“, sagt Wolf. In Wahrheit würden sie sogar in Deutschland geschrieben und teils über sichere Verbindungen geschickt. „Das ist eine ganz neue Generation von Phishingmails, verfeinert und professionalisiert.“

Meist müssen PayPal oder Amazon als Absender herhalten. Betrüger bauen die Original-Website bis ins Detail nach – inklusive Quelltext. Die Fälschung ist kaum zu erkennen, umso wichtiger ist der Blick in die URL-Zeile. Ein Beispiel: Die Adresse von PayPal lautet tatsächlich www.paypal.com. Gefälschte Versionen sind leicht abgewandelt, etwa paypal-bund.org, oder sie enthalten am Ende sogar nicht einmal mehr den Markennamen PayPal („privatkunden.de-web221.pw“). Experten nennen das Vortäuschen einer seriösen URL-Identität „URL-Spoofing“.

Andre Wolf rät: „Die URL liest man immer von hinten. Von einem Markennamen am Anfang der Zeile sollte man sich nicht blenden lassen.“ In neuesten Phishingmails werden sogar die tatsächlichen Postadressen von Usern genutzt. Der dynamische Einbau solcher Daten sorgt für Scheinauthentizität, die den Betrug noch raffinierter macht.

Der Betrug reicht bis zum Diebstahl ganzer Identitäten. Für Nutzer kann das mit dem kompletten Kontrollverlust enden. Meist hat Identitätsdiebstahl zwei Motive: finanzielle und persönliche, zum Beispiel Rache. In Deutschland ist Identitätsdiebstahl nicht per se als Straftat im Strafgesetzbuch verankert, dagegen Delikte wie Nachstellung oder Urkundenfälschung sehr wohl.

FRIEDERIKE HANTEL / SPIEGEL WISSEN

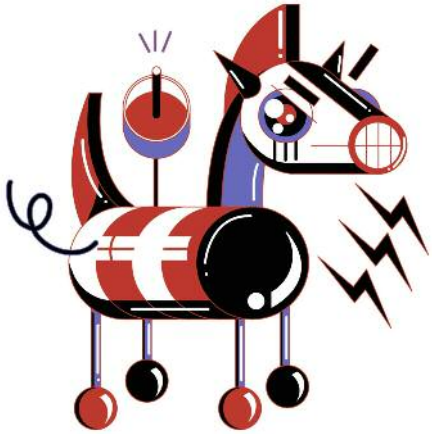
BOTNETS: Ein Netzwerk von infizierten Computern, das Angreifer aus der Ferne kontrollieren können. Es nutzt oft Domains mit kurzer Lebensdauer zur Verschleierung.

Trick 3

Die Portalfrage – Onlineflirts, Shopping und Jobsuche

Früher waren es die Heiratsschwindler, die einsamen Frauen das Konto abräumten, heute sind es „Fembots“, die Männern das Geld entlocken. Männer, die sich beim falschen Portal anmelden, erhalten eine Mail, dass sich eine (tolle!, wunderschöne!) Frau für sie interessiere. Kontakt zu ihr aufzunehmen kostet einiges, aber ist das Liebesglück nicht alles Geld der Welt wert? Andere zahlen für die Aussicht auf eine „geile Affäre ohne Schwierigkeiten“. Die Traumfrau fürs Heim oder fürs Bett ist jedoch die Erfindung eines Computerprogramms; das verlorene Geld hingegen sehr real. Gerade im Netz gilt der Spruch: Augen auf bei der Partnerwahl!

Hinter einer solchen Abzocke steckt ein gut organisiertes System. Da sei auch die Polizei machtlos, sagt Wolf. Er rät zu Misstrauen, wenn schnell Geld überwiesen werden soll, zum Beispiel über Western Union. „Das ist eine einfache Sicherheitsregel, aber offenbar befolgen sie viel zu wenige“, so Mimikama-Mann Wolf.



TROJANER: Ein Schadprogramm, das als nützliche Anwendung getarnt ist. Ins System gelangen Trojaner häufig über E-Mails und Downloads. Hier geht es um das Ausspähen von Daten.

Zum Basisprogramm der Selbstverteidigung gehört, nur geschützte WLAN-Netzwerke zu nutzen und Filehoster und Firewalls korrekt zu installieren. Gegen manche Attacken gibt es spezielle Abwehrmethoden: Der sogenannte E-Blocker zum Beispiel soll dafür sorgen, dass das Onlinetracking von Suchmaschinen-Abfragen unterbunden wird – etwa wenn User online nach Krankheitssymptomen gesucht haben und niemand davon erfahren soll.

Verschlüsselungstechnik für digitale Kommunikation hilft im besten Fall gegen die NSA, aber nicht gegen Viren. „Das wissen viele nicht. Aber es ist so, als würde man ein Schloss an der Haustür anbringen, sie nachts aber offen stehen lassen“, sagt der Anti-Betrugs-Experte Wolf. Für ihn ist es schwer verständlich, dass Menschen ihre Wohnungstür mit Querriegeln sichern und Drückerkolonnen nicht die Tür öffnen, aber auf Phishingmails reinfallen.

Und was ist die beste Strategie gegen Betrüger im Netz? „Zu wissen, wie sie arbeiten – das ist der beste Schutz“, sagt Wolf. Die EU-Kommission kann zukünftig einiges Wissen beitragen, denn sie will 450 Millionen Euro für die Grundlagenforschung gegen Internetkriminalität bereitstellen. Und es ist nie ein Fehler, vor dem Klicken innezuhalten und nachzudenken.

Trick 4

Natürliche Schwäche – Social Engineering

Viele der Betrugsmaschen missbrauchen digitale Strukturen. Doch eine genauso große Gefahr wie das Netz ist der User selbst. Beim Social Engineering profitieren Betrüger von der Leichtfertigkeit, mit der wir Daten herausgeben. Es geht um erschlichenes Vertrauen und falsche Hoffnungen.

Zu beobachten ist das derzeit bei Kontaktversuchen angeblicher IT-Techniker von Microsoft. „Sie melden sich mit einem Problem in der Technik des Opfers und bitten darum, sich mit einem bestimmten Tool Zugriff auf den Rechner verschaffen zu dürfen.“

Viele der späteren Betrugsopfer würden in ihrer Panik Vertrauen in den angeblich namhaften Anbieter fassen – mit fatalen Folgen. Denn aus der Ferne übernimmt der Techniker die Kontrolle über den fremden Rechner. Auf die digitale Geiselnahme, folgt meist eine Lösegeldforderung. Auch mit speziellen Trojanern wird diese Form der Erpressung angewandt, Experten sprechen von „Ransomware“. Ein Beispiel hierfür ist der BKA-Trojaner, der Usern vortäuschte, eine Behörde habe sie bei Gesetzesverstößen enttarnt und fordere nun eine Strafzahlung.

IT-Experten raten Privatpersonen: niemals zahlen. Die Landesanstalt für Medien Nordrhein-Westfalen empfiehlt, sich auch bei Mahnungen und Inkassoschreiben nicht unter Druck setzen zu lassen. Kunden müssten erst handeln, wenn sie einen gerichtlichen Mahnbescheid erhalten.

WÜRMER: Diese Art Schadprogramm kann sich selbst vervielfältigen und über Wechselmedien wie USB-Sticks verbreiten. Etwa jedes fünfte Schadprogramm ist ein Wurm – er verbraucht enorme Netzwerkressourcen und kann erheblichen finanziellen Schaden anrichten.

Christian Schweppe war überrascht über die neue Perfektion von Phishingmails und warf gleich einen Blick in den eigenen Spamordner. Er stieß auf ominöse Amazon-Gutscheine und hatte ein Auto gewonnen.