Neue Gefahren im Netz

Neue Schadsoftware bedroht Internetnutzer, Kriminelle spähen vertrauliche Daten aus, „Lovescammer“ nutzen das Vertrauen von Menschen für betrügerische Zwecke. Auch soziale Medien bergen Gefahren.

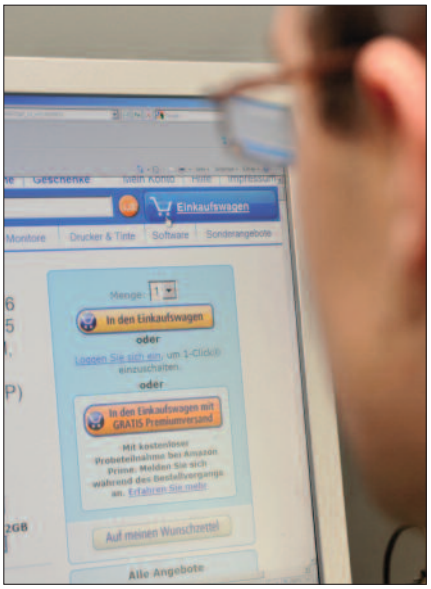
Benutzt keine *Microsoft*-E-Mails. Sie verkaufen die Daten an Regierungen.“ Dieser Satz sorgte auf der Kurznachrichtenplattform *Twitter* zum Jahreswechsel 2013/2014 für Aufregung. Denn die Meldung wurde nicht von einem privaten Nutzer in Umlauf gebracht, sondern von dem Account des Internet-Telefondienstanbieters *Skype*. Kurz darauf folgten ähnliche Nachrichten auf einem Blog und der *Facebook*-Seite des Unternehmens. *Skype* gehört zum Softwarekonzern *Microsoft*. Werbung gegen die eigene Sache?

Hinter den Warnungen steckte eine Hackergruppe, die sich als „Syrian Electronic Army“ bezeichnet. Sie hatte die Seiten von *Skype* kurzzeitig gekapert. Zweck der Aktion war es, die angebliche Kooperation zwischen *Microsoft* und der *NSA* anzuprangern, die dessen früherer Mitarbeiter Edward Snowden im Vorjahr publik gemacht hatte. Demnach habe der Dienst mithilfe des Programms „Prism“ Zugriff auf Kommunikationsinhalte der Nutzer von *Microsoft, Google, Facebook, Yahoo* und *Skype*. Zudem soll die *NSA* die Datenkabel zwischen den Rechenzentren von *Google* und *Yahoo* anzapfen – ohne deren Kenntnis.

Technologisches Know-how, Verträge, Prozessabläufe oder Preiskalkulationen sind nur einige Bereiche, auf die die „Späher“ zugreifen. Neben beruflichen Informationen gelangen auch private Fotografien, Nachrichten und Videos in ihre Hände – Informationen, die nur ungern mit anderen und gar nicht mit allen geteilt werden sollen.

Opfer von kriminellen Hackern kann jeder Internet-User werden. Passwörter, Bankdaten oder das Bestellverhalten werden ausgespäht. Die Folge: Bestellbetrug, Spam-E-Mails, personalisierte Werbung, ein leeres Konto oder Erpressung.

Daneben bieten gerade Websites von Privaten eine Möglichkeit, sich deren Infrastruktur zu eigen zu machen und Viren oder Schadsoftware über die gehackte Webseite in Umlauf zu bringen.



Bestellbetrug: Internetnutzer bezahlen für Waren, die sie nie erhalten.

Verrat durch Vertrauen. Neben diesen „klassischen“ Formen der Internetkriminalität floriert der Betrug mittels sozialer Netzwerke. Der häufig sorglose Umgang mit persönlichen Informationen ermöglicht es Betrügern, gezielt vorzugehen.

Postet ein User etwa auf *Facebook* oder der Fotoplattform *Instagram* häufig Bilder von Katzen, bekommt er E-Mails mit Werbung für Katzenfutter geschickt. Beim Öffnen der Nachricht oder des Anhangs wird dann eine Schadsoftware installiert.

Eine andere Möglichkeit sind Bestellbetrügereien: Wird festgestellt, dass ein Nutzer ein begeisterter Fischer ist, werden Nachrichten mit einer Kaufaufforderung, beispielsweise für eine Angelausrüstung, versandt. Das Opfer bezahlt, erhält die Waren jedoch nicht.

Besonderes „Glück“ hingegen wird bei Gewinnversprechen suggeriert: Dabei wird in E-Mails vorgegeben, der Empfänger hätte bei einer Lotterie oder bei einem anderem Gewinnspiel Geld oder einen wertvollen Preis gewonnen. Der Gewinn werde allerdings erst nach der Überweisung einer bestimmten Summe freigegeben.

Die Methode, mit der das Vertrauen der User am meisten ausgenützt werden, ist „Lovescam“. Dabei wird etwa via Partnervermittlungs-Portalen eine fiktive Liebesgeschichte aufgebaut, meist „Fernbeziehungen“: Um ein erstes Treffen zu ermöglichen, gibt der potenzielle Partner vor, Geld zu benötigen, um die Reise antreten zu können. Mit weiteren abenteuerlichen Behauptungen fordern die Täter bei den faszinierten Opfern weitere Geldsummen.

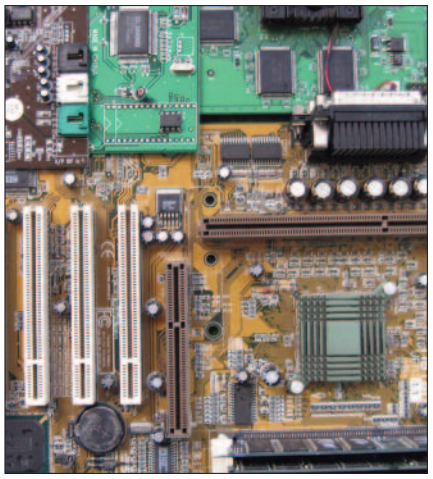
Soziale Netzwerke bieten auch (Cyber-)Stalkern ein Betätigungsfeld. Die E-Mails beinhalten Hass, Obszönitäten, Rufschädigungen und Bedrohungen. Wie drastisch dies ausfallen kann, zeigt der Fall einer Bloggerin. Ihr Fall wurde im Vorjahr bekannt. Die Frau, im Netz als serotonic aktiv, erhielt seit 2006 aggressive Nachrichten. Eine davon lautete: „Und dort lege dir den Mühlstein um den Hals, den ich so fleißig neben mir hergerollt habe. Leider passt nur dein Kopf rein (…). Und dann nur ein kleiner Sprung und alles ist vorbei.“

Derartiger Cyber-Hate verleitete bereits Jugendliche dazu, Selbstmord zu begehen. In England gab es innerhalb von zwei Jahren drei Verzweiflungstaten. In Österreich wurde bereits jeder fünfte 14- bis 19-Jährige Opfer von digitalem Mobbing.

Erpressung. „Sie haben sich einer strafbaren Handlung schuldig gemacht. Ihr Rechner wird gesperrt. Gegen ein Entgelt kann eine Entriegelung des Gerätes vorgenommen werden. Ihr Bundeskriminalamt.“ Poppt ein Fenster mit einer derartigen Nachricht beim Öffnen einer Seite auf, handelt es sich nicht um die Ahndung eines Deliktes, sondern um einen „Polizei-Virus“, auch Polizei-Trojaner“ genannt. Dabei wird mithilfe gefälschter Symbole, etwa eines Polizeilogos, Schadsoftware verschickt. Eine Betrugsform, die laut dem Cybercrime-Report des Bundeskriminalamts vor allem in Österreich beliebter wird. Im Jahr 2012 gingen bei der Staatsanwaltschaft über 3.000 Anzeigen bezüglich „Ransomware“ ein.

Finanzielle Motive sind es auch, die Passwort-Fischer („Phishing“) verfolgen. Dass die digitale Angelroute ausgeworfen wurde, merkt man, wenn ei-

FOTO: EGON WEISSHEIMER



Jeder PC mit Internetanschluss ist verwundbar, wenn die Anti-Viren-Software nicht auf dem neuesten Stand ist.

ne E-Mail einlangt, in der die Hausbank vorgibt, die Kundendaten abfragen zu wollen. Eine andere Variante stellen gefälschte Websites dar: Der Kunde glaubt, auf der Seite seines Geldinstituts gelandet zu sein und tätigt eine Überweisung. Das Geld erreicht aber nicht den gewünschten Empfänger, sondern geht an die Betrüger. Häufig sind „Finanzagenten" zwischengeschaltet, die ihr Konto für Überweisungen zur Verfügung stellen und die Gelder nach Abzug einer Provision weiterleiten.

Tendenz steigend. Der ungewollte Abfluss von sensiblen Informationen ist eine häufig unterschätzte Bedrohung. Im ersten Halbjahr 2013 wurden in Österreich 6.413 Anzeigen wegen Internetdelikte registriert. Das ergibt einen Anstieg von 63 Prozent im Vergleich zum ersten Halbjahr 2012. Die Aufklärungsquote betrug 40,4 Prozent.

Die Dunkelziffer ist hoch, da viele Unternehmen aus Angst um ihr Image keine Anzeigen machen. Das belegt eine Studie des Bundesamts für Verfassungsschutz und Terrorismusbekämpfung (BVT) aus dem Jahr 2010. Damals gaben 31 Prozent der Firmen an, bereits Opfer von Wirtschafts- und Industriespionage geworden zu sein. Nur 13 Prozent wandten sich an die Sicherheitsbehörden. Zur Angst, ein schlechtes Image zu bekommen, kommt ein fehlendes Bewusstsein um die Problematik. Denn laut der Studie schätzt die Hälfte der Unternehmen das Risiko, Opfer ungewollten Informationsabflusses zu werden, als gering ein. Zehn Prozent glauben, gar nicht gefährdet zu sein.

Schutz vor Schadsoftware. Da sich Trojaner und Viren mit enormer Geschwindigkeit verändern – alle 15 Sekunden entsteht ein neues Schadprogramm –, sind Schutzmaßnahmen unerlässlich.

Eine Anti-Viren-Software sollte stets auf dem neuesten Stand sein, Sicherheits-Updates für die Schutzsoftware sollten regelmäßig erfolgen; Gleiches gilt für Betriebssysteme und Browser.

Eine Prüfung von fremden CDs, DVDs oder USB-Sticks vor der Benutzung verringert das Risiko, Opfer von Cyber-Kriminellen zu werden. Langen E-Mails ein, deren Absender unbekannt sind bzw. nicht vertrauenswürdig wirken, ist ein Löschen – ohne das Mail geöffnet zu haben – der sicherste Weg, um Trojaner abzuwehren. Daneben können Hyperlinks, die per E-Mail versandt werden, beim Anklicken zu Webseiten führen können, die Schadsoftware enthalten.

Hacker knacken Passwörter, um an Bankdaten, Fotografien und andere heikle Unterlagen zu gelangen. Zur Vorbeugung ist es ratsam, nicht dasselbe Passwort für mehrere Dienste zu verwenden. Auch eine Kombination aus Zahlen, Buchstaben und Sonderzeichen sollte gewählt werden, die mindestens acht Zeichen umfasst. Um nicht Phishing-Opfer zu werden, sollte die offizielle Adresse der Bank in die Suchleiste eingegeben werden.

Für Überweisungen und andere Kundenaufträge sind Transaktionsnummern (TANs) nötig. Sollten mehrere TANs zugleich abgefragt oder zusätzlich Kreditkarten- und Adressdaten verlangt werden, sollte der Auftrag abgebrochen und das Geldinstitut informiert werden. Sollten „Banken" per E-Mail nach Kundendaten fragen, handelt es sich ebenfalls um Betrug.

Vorsicht walten sollte man auch bei der Installation von Software oder Zusatzprogrammen („Plug-ins"). Eine Gefahr sind Schadprogramme, die in Gratis-Downloads oder Raubkopien von dubiosen Anbietern versteckt sind. In sozialen Netzwerken sollte darauf geachtet werden, welche Informationen mit welchen Nutzern geteilt werden. Je sorgfältiger die eigene Kontaktliste beäugt wird, desto weniger Angriffsfläche wird potenziellen Betrügern und Stalkern geboten. *Hellin Sapinski*

FOTO: EGON WEISSHEIMER