Zeitschrift für Datenrecht und Informationssicherheit

digma

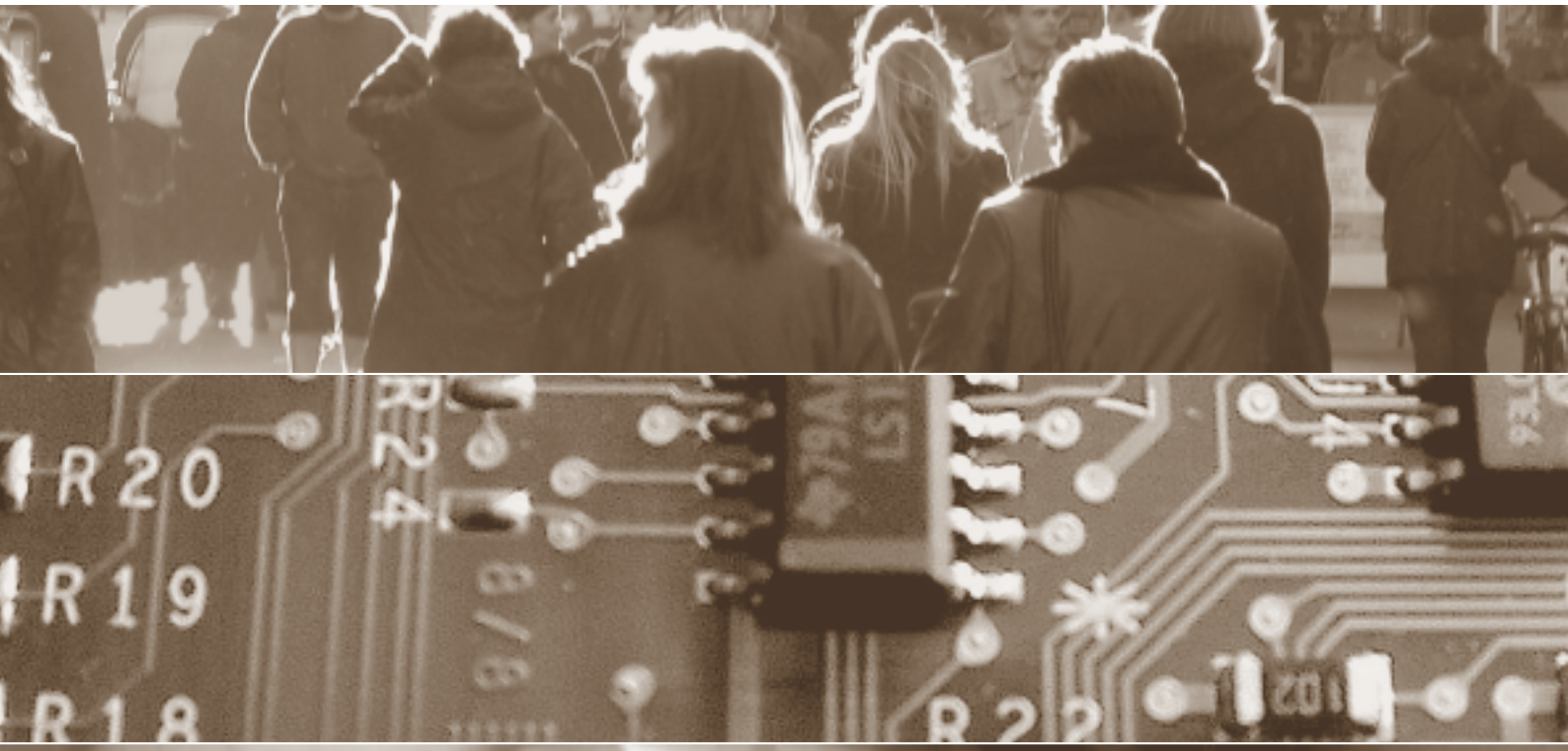
www.digma.info 8. Jahrgang, Heft 4, Dezember 2008

Schwerpunkt:

Cyber-Ermittlungen

fokus: Die Geschwätzigkeit des verlorenen Laptops
Cyber-Crime als Dienstleistung

report: Strategische Informationssicherheit



Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Günter Karjoth

Schulthess §

inhalt

fokus

Schwerpunkt:
Cyber-Ermittlungen

Die Geschwätzigkeit des verlorenen Laptops

Passwörter und Verschlüsselung sollen den unberechtigten Zugang zu Daten verhindern. Doch wie wirksam sind diese Massnahmen, wenn ein Computer abhanden kommt? Der Artikel zeigt, dass solche Laptops fast nichts für sich behalten können.

Cyber-Crime als Dienstleistung

Die Möglichkeiten im Internet haben nicht nur legitime Geschäftsfelder transformiert: Auch professionelle, gut organisierte Cyber-Verbrecher profitieren davon.

Incident Reponse Capabilities

IT-Sicherheit darf nicht mehr nur den Schutz der eigenen IT-Infrastruktur zum Ziel haben, sondern muss auch dazu beitragen, Schäden an Systemen von Dritten zu verhindern. Der Autor betont auch die Wichtigkeit, auf Sicherheitsvorfälle reagieren zu können, wenn die präventiven Schutzvorkehrungen nicht ausreichen.

impressum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. Dr. iur. Rainer, J. Schweizer, Dr. Günter Karjoth

Redaktion: Dr. iur. Bruno Baeriswyl und Dr. iur. Beat Rudin

Rubrikenredaktor: Dr. iur. Amédéo Wermelinger

Zustelladresse: Redaktion digma, c/o Stiftung für Datenschutz und Informationssicherheit, Kirschgartenstrasse 7, CH-4010 Basel
Tel. +41 (0)61 270 17 70, redaktion@digma.info

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo Schweiz: CHF 158.00, Jahresabo Ausland: Euro 112.00 (inkl. Versandspesen), Einzelheft: CHF 42.00

Anzeigenmarketing: Publicitas Publimag AG, Mürtschenstrasse 39, Postfach, CH-8010 Zürich
Tel. +41 (0)44 250 31 31, Fax +41 (0)44 250 31 32, www.publimag.ch, service.zh@publimag.ch

Herstellung: Schulthess Druck AG, Arbenzstrasse 20, Postfach, CH-8034 Zürich

Verlag und Abonnementsverwaltung: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach, CH-8022 Zürich
Tel. +41 (0)44 200 29 99, Fax +41 (0)44 200 29 98, www.schulthess.com, zs.verlag@schulthess.com

Strategische Informations-sicherheit

Die Autorin hat in ihrer Dissertation Fallstudien zur Informationssicherheit in Grossunternehmen durchgeführt. Sie stellt fest, dass sich Informationssicherheit verschiebt von einem defensiv ausgerichteten hin zu einem Führungsinstrument, das einen Mehrwert für Unternehmen schafft.

ERP-Risiko-Management

In vielen Firmen werden wichtige Finanz- und Logistik-Prozesse, welche gesetzliche Compliance-Anforderungen erfüllen müssen, mit Hilfe von Enterprise-Resource-Planning-Managementsystemen abgedeckt. Eine ISSS-Tagung widmete sich verschiedenen Aspekten des Risikomanagements für ERP-Systeme.

Der «naked citizen» und sein Schwabbelbauch

Der Staatsschutz wird wieder aktiv, die Krankenkassen immer hungriger – aber der Bürger macht sich kaum Gedanken. Aber dann plötzlich … !

report

forum

Cyber Crime als Dienstleistung

Die Entwicklung der Sicherheit im Internet – vom schlauen Hacker zur organisierten Kriminalität

Stefan Frei, IT-Security-Forscher und Dozent für Netzwerksicherheit, Communication Systems Group, Institut für Technische Informatik und Kommunikationsnetze, ETH Zürich, Zürich
stefan.frei@tik.ee.ethz.ch

Prof. Dr. Bernhard Plattner, Leiter der Communication Systems Group, Institut für Technische Informatik und Kommunikationsnetze, ETH Zürich, Zürich
plattner@tik.ee.ethz.ch

Das Internet hat nicht nur legitime Geschäftsfelder transformiert: Auch professionelle, gut organisierte Cyberkriminelle profitieren davon.

Um die gegenwärtige Bedrohungslage zu verstehen und neue Entwicklungen bewerten zu können, ist es nützlich, einen Schritt zurück zu tun, um mit einem erweiterten Blickwinkel die wichtigsten Akteure erfassen und charakterisieren zu können. Dazu betrachten wir die Entwicklung der Sicherheit im Internet in den letzten drei Jahrzehnten. Es lassen sich verschiedene Phasen identifizieren, die sich primär durch die Population im Internet, den damaligen technischen Kontext und die Eigenschaften der Angreifer und deren Methoden unterscheiden.

Phase 0: Pionierzeit (1980er-Jahre bis 1993)

In der Pionierzeit des Internets waren dessen Benutzer gleichzeitig dessen Designer und Entwickler, die in einer fast ausschliesslich akademischen Umgebung mit einer faszinierenden neuen Technologie experimentierten. Die damals getroffenen grundlegenden Entwurfsentscheide für viele der noch heute verwendeten Protokolle konzentrierten sich vor allem auf deren Funktionalität. Sicherheitsaspekte waren zu dieser Zeit höchstens eine Nebensache, weil sich kaum jemand einen bewussten Missbrauch dieser neuen Infrastruktur vorstellen konnte. Dieses Vertrauen wurde jedoch jäh erschüttert durch den sog. «Morris Worm», der 1988 erstmals die Gefahr aufzeigte, die durch eine automatische Verbreitung von ausführbaren Programmen entstehen kann. Zwar wollte der Autor dieses Wurms, ein Student namens Robert Morris, nur die damalige Grösse des Internets erforschen, aber aufgrund eines Fehlers im Programm legte der Wurm einen Grossteil des Internets lahm. Morris wurde später auf der Basis des 1986 erlassenen Computer Fraud and Abuse Act verurteilt, hat aber trotzdem Karriere gemacht: Er ist heute Professor am MIT.

Phase 1: Experimentieren (1993 bis 1999)

In dieser Zeit kam das Internet ins Blickfeld der Öffentlichkeit, angestossen durch die «Killer-Applikation» World Wide Web und die Verfügbarkeit des auch für Nicht-Techniker brauchbaren Web-Browsers «Mosaic». Die Benutzerpopulation bestand primär aus innovativen Nutzern und den Mitarbeitern grösserer Firmen; Letztere waren zunehmend im Web präsent. Die primären Anwendungen im Internet waren das Web und E-Mail.

Die Sicherheit im Internet war zu dieser Zeit vor allem durch die einsamen Hacker beeinträchtigt, die spätnachts ihre technischen Fähigkeiten erprobten, um Schwachstellen in Protokollen und Systemen zu finden und sie gezielt für Attacken auf einzelne Server zu nutzen. Das Konzept des Wurms – von Morris demonstriert – war natürlich gut bekannt und wurde in vereinzelten Experimenten, die ohne grosses Aufsehen verliefen, nachvollzogen.

Phase 2: Angeberei (1999 bis 2004)

Zu dieser Zeit waren ein signifikanter Teil der Bevölkerung der Industriestaaten und praktisch alle Firmen am Netz. Durch erste Web-Anwendungen für E-Commerce und den Übergang der Internet-Zugänge von Schmalband zu Breitband wurde das Internet für potenzielle Angreifer ein interessanteres Ziel. Zunehmend wurden Anleitungen für Angriffstechniken im Netz verbreitet, bis hin zu ausgefeilten Angriffsprogrammen, die von sogenannten «Script-Kiddies» ohne tiefe technische Kenntnisse zwischen Schulschluss und dem Abendessen ausgeführt werden konnten. In diese Phase fallen jedoch auch ernst zu nehmende Störungen durch Würmer mit einer massiven und schnellen Verbreitung, z. B. *Melissa*, *Code Red*, *SQL-Slammer* und *Mircrosoft Blaster*. Sie bedienten sich verschiedener Methoden der Ausbreitung (sowohl via E-Mail als auch direkt über die Netzwerk-Infrastruktur). Auch wenn diese Ereignisse teilweise grosse Publizität erhiel-

ten, waren die angerichteten Schäden eher kollateral als gezielt. Das Phänomen von unerwünschter E-Mail (Spam) hingegen begann die Nutzer zu ärgern.

Phase 3: Technische Aufrüstung (2004 bis 2006)

Eine technische Aufrüstung konnte sowohl bei der Entwicklung des Internets als auch in neuen Angriffstechniken beobachtet werden. Die Nutzer konnten sich über schnellere und billigere Internet-Anschlüsse und über neue Web-basierte Applikationen freuen. Die potenziellen Angreifer hingegen erfreuten sich an immer komplexeren Anwendungen mit immer mehr nutzbaren Schwachstellen und dem Heer von gut erreichbaren, leistungsstarken PCs der Internet-Nutzer. Sie erkannten, dass durch Würmer verursachte massive Störungen des Betriebs kaum das Mass aller Dinge waren; vielmehr begannen sie, ohne grosses Aufsehen schlecht geschützte, mit Schwachstellen versehene PCs von Privatpersonen anzugreifen und zu kontrollieren, ohne dass deren Besitzer sich eines Angriffs bewusst wurden. Die übernommenen Rechner wurden in ein sog. Botnetz, ein Netz von «Robotern», eingefügt und konnten sodann nach Belieben für verschiedene Anwendungen eingesetzt werden, wahlweise für das Versenden von Spam oder für gezielte Angriffe auf einzelne Dienste im Netz. Es entwickelte sich ein eigentliches Wettrüsten zwischen den Angreifern, die stets neue Schwachstellen fanden und nutzten, und den Verteidigern, die den Schwachstellen und Angriffen mit Patches, Virenscannern und Firewalls zu Leibe rückten.

Phase 4: Professionalisierung und Kommerzialisierung (2006 bis heute)

In der Phase 3 wurden viele der heute bekannten Angriffstechniken entwickelt und zur Perfektion gebracht. Dies bedeutet nicht, dass heute keine neuen Techniken mehr entwickelt werden – vielmehr ist dies ein kontinuierlicher Prozess. Der wesentliche Unterschied zwischen den beiden Phasen ist, dass sich die Akteure geändert haben. Während in den vorangegangenen Phasen die Technik durch technische Fachleute im Untergrund entwickelt wurde, prägen heute professionell, kommerziell und organisiert handelnde Kriminelle das Bild.

Mit dem Aufkommen von Web 2.0 und der damit verbundenen rasanten Verbreitung komplexer Web-Dienste (z. B. «Software as a Service» mit Google Docs und Social Networks) wurden neue technische Angriffsszenarien denkbar, da sich das Web mehr und mehr zu einem Zweiweg-Medium entwickelte. Die Verbreitung neuer Plattformen wie Youtube, Facebook, Myspace usw. verschafft der organisierten Kriminalität direkten Zugang zu Millionen von Personen, die bereitwillig ihre persönlichen Daten offenlegen. «Social Engineering» als neue Angriffsmethode (bekannt von Phishing-Attacken, mit welchen Internet-Nutzer zur Preisgabe von Zugangsdaten z. B. ihrer Bankkonten gebracht werden) steht erst am Anfang. Rein technische Angriffe werden dadurch ersetzt oder wirksam ergänzt.

Cyber Crime heute

Die Angriffsmethoden heutiger Cyberkrimineller sind vielfältig und werden schnell an neue Gegebenheiten angepasst. Im Folgenden werden die wichtigsten Angriffsformen und deren Anwendungen beschrieben.

Plattformen wie Youtube und Facebook verschaffen der organisierten Kriminalität direkten Zugang zu Millionen von Personen, die bereitwillig ihre persönlichen Daten offenlegen.

Drive-by Download – ein Trend

Der breite Einsatz von Firewalls und immer besser geschützte Server-Systeme haben die Intensität von Angriffen aus dem Internet nicht vermindert; vielmehr haben sich diese auf das nächste Ziel verlagert – die Rechner der Nutzer. Der Web-Browser, die meistbenutzte Software im Internet, ist das Einfallstor.

Um einen PC über den Web-Browser erfolgreich angreifen zu können, müssen zwei Bedingungen erfüllt sein:

Kurz&bündig

Das anhaltende Wachstum des E-Commerce im Internet bietet Kriminellen gewaltige Aussichten für illegale Profite mit geringem Risiko. Hinter Viren, Spam, und Phishing stehen heute international operierende Banden. Diese arbeiten hochprofessionell: Durch Arbeitsteilung, Automatisierung und Spezialisierung sehen wir uns raffinierten Attacken ausgesetzt. Professionelle Programme zur Erstellung von Viren, Spam und Phishing-Seiten werden im Untergrund angeboten, mit Service-Abonnement für aktuellste Exploits und «Geld-zurück-Garantie» bei Entdeckung durch Anti-Viren-Programme. Wir durchleben den Wechsel von softwarebasierten Attacken zu einer servicebasierten Ökonomie – «Malware as a Service». Zum Verständnis dieser Entwicklung und geeigneter Gegenmassnahmen ist es wichtig, nicht nur die Technik, sondern vor allem die Anreizsysteme der Internet-Ökonomie zu verstehen. Der Angreifer muss nicht schlauer sein als die Schutzvorkehrung, es genügt, dass er schlauer ist als das Opfer.

- der Browser ist durch eine Schwachstelle verwundbar, und
- der Browser lädt eine Seite, welche die Schwachstelle auszunutzen weiss.

Die erste Bedingung ist leider allzu oft erfüllt. In einer vor Kurzem an der ETH Zürich in Zusammenarbeit mit Google und IBM durchgeführten Studie wurde nachgewiesen, dass über 40% der Internet-Benutzer mit einem nicht vollständig gepatchten, d. h. einem unsicheren Browser surfen und damit ein einfaches Opfer für sogenannte Drive-by-Download-Attacken werden. Drive-by-Download bezeichnet das unbewusste Herunterladen von schädlicher Software (*Malware*) auf den PC des Benutzers. Dafür werden von Angreifern gezielt häufig besuchte Webseiten ohne Wissen ihrer Betreiber manipuliert. Da der Besucher die Website kennt und ihr vertraut, hegt er kaum Verdacht, beim Besuch eine Software zu laden und auszuführen. Diese Form eines Angriffs nimmt seit 2007 ständig zu und hat mittlerweile E-Mail als primäre Methode für die Verbreitung von Malware verdrängt.

Derzeit wird ein ungeschützt ans Internet angeschlossener Computer innert weniger Minuten infiziert.

Automatisierte Angriffe

Seit Längerem ist eine zunehmende Automatisierung von Internet-Attacken zu beobachten. Das Internet wird fortwährend nach verwundbaren Computern abgesucht, welche sodann vollautomatisch infiziert werden. Derzeit wird ein ungeschützt ans Internet angeschlossener Computer innert weniger Minuten infiziert.

Dem Cyber-Verbrecher stehen dazu verschiedene Angriffswerkzeuge zur Verfügung, welche die Planung und Durchführung von Angriffskampagnen automatisieren. Die Möglichkeiten und die Entwicklung dieser Hilfsmittel zeigen die fortlaufende Professionalisierung und Organisation krimineller Angreifer. Aktuelle Angriffswerkzeuge sind sehr ausgereift, sowohl was ihre technische Funktionalität als auch was die eingebauten Verwaltungsfunktionen und die Art ihres Betriebs betrifft. Moderne Angriffswerkzeuge sind durchgängig modular aufgebaut, um eine schnelle Integration neuer Angriffstechniken zu gewährleisten. Zur Verhinderung der Detektion, Rückverfolgbarkeit und Analyse kommen hoch entwickelte technische Verfahren zum Einsatz.

Heutige Angriffswerkzeuge lassen sich an die Bedürfnisse des jeweiligen «Kunden» anpassen und verfügen über ausgereifte Funktionen für die Steuerung der Angriffe und die Erfolgskontrolle. So lässt sich eine Kampagne nur gegen ein bestimmtes Land, ein Betriebssystem oder eine bestimmte Sprachregion durchführen. Mit umfangreichen Berichten wird der Erfolg genaustens gemessen, was wertvolle Informationen für die Optimierung einer Kampagne und die kontinuierliche Weiterentwicklung der Malware liefert.

Bekannte Angriffswerkzeuge sind IcePack, Mpack, und Neosploit. IcePack erschien erstmals im Juli 2007 und wird als IcePack Light Edition für USD 30 oder IcePack Platinum Edition für USD 400 angeboten. Hersteller ist die «IDT Group» aus Russland, und das Produkt wurde zwischenzeitlich ins Englische und Französische übersetzt. Das aus dem russischen Untergrund stammende Mpack Toolkit (Malware Pack) wird für USD 500 bis 1000 weltweit angeboten. Mpack wie auch IcePack ermöglichen automatisierte Attacken gegen Web-Browser, angeblich mit einer Erfolgsrate von 40 bis 50%.

Eine Malware, welche das Zielsystem infizieren soll, durchläuft eine rigorose Qualitätsprüfung und wird vor der «Auslieferung» solange modifiziert, bis sie von Anti-Viren-Programmen nicht mehr erkannt wird. Mit ihrer aktiven Verbreitung steigt jedoch zwangsweise die Wahrscheinlichkeit der Entdeckung. Diesem Umstand begegnen die kriminellen Hersteller auf zwei Arten:

- Es werden vor der Auslieferung bereits viele Varianten einer Malware auf Vorrat produziert, und
- eine Variante wird nur für eine begrenzte Anzahl Infektionen verwendet.

Damit wird einerseits die Wahrscheinlichkeit, von Anti-Viren-Programmen erkannt zu werden, stark reduziert; andererseits werden die Anti-Viren-Hersteller mit einer grossen Anzahl neuer Varianten konfrontiert, was enorme Ressourcen

Literatur und Links

- Understanding the Web browser threat, 2008, <http:// www.techzoom.net/insecurity-iceberg>.
- Symantec Corporation, Threat Report 2007, published April 2008, <http://www.symantec.com>.
- McAfee Avert Labs Blog – You have to pay for quality, 7. Mai 2008.
- MPack Analysis, <http://isc.sans.org/diary.html?storyid=3015>.
- Who's Stealing Your Passwords?, <http://www.cio.com/article/print/135500>.
- Organized Crime and Cybercrime: Synergies, Trends, and Responses, Phil Williams, <http://www.crime-research.org/library/Cybercrime.htm>.
- Das Internet als Kampfzone, NZZ vom 15. August 2008.

bindet und die Fähigkeit, zeitgerecht neue Signaturen zu produzieren, beeinträchtigt. Die infizierten Systeme werden sodann üblicherweise in ein «Botnetz» integriert.

Botnetze

Die Durchführung krimineller Aktivitäten, wie der Massenversand von Spam, das Hosting von Phishing-Webseiten oder das Ausführen von DoS-Attacken, setzt eine entsprechende Infrastruktur voraus. Dazu werden sogenannte Botnetze mit Tausenden oder Millionen von vernetzten Computern aufgebaut. Ein Botnetz dient der Bereitstellung der benötigten Bandbreite und Rechenkapazität. Weiter gewährt ein massiv verteiltes System Ausfallsicherheit und Schutz vor Rückverfolgung. Die Akteure verwenden dafür nicht eigene Computer, sondern beschaffen sich die Infrastruktur, indem sie im grossen Stil mittels automatisierter Angriffe am Internet angeschlossene Computer in Besitz nehmen. Vornehmlich schlecht geschützte Maschinen von Endbenutzern werden im Versteckten zu «Bots» umfunktioniert, ohne dass der Benutzer davon etwas bemerkt.

Die Bot-Software ist hochentwickelt: Eventuell vorhandene Anti-Viren-Software und Auto-Update-Mechanismen werden im Hintergrund deaktiviert, die Firewall wird umkonfiguriert und die Bot-Prozesse werden versteckt ausgeführt, um einen möglichst zuverlässigen und langen Betrieb des Bots sicherzustellen.

Hat sich der Bot erfolgreich eingenistet, stellt er dem Betreiber des Botnetzes, dem «Botmaster», verschiedene Dienste zur Verfügung.

Zur zentralen Steuerung werden hoch entwickelte, kryptografisch geschützte Netze (Command and Control Networks) verwendet, welche die Rückverfolgung weitgehend verunmöglichen. Dies erklärt, warum es äusserst schwierig ist, solche Aktivitäten zu unterbinden oder die Drahtzieher dahinter zu identifizieren. Derzeit mehren sich multifunktional einsetzbare Botnetze, in welchen neue Funktionen bei Bedarf nachgeladen werden können. Der Botmaster nutzt sein Botnetz selbst oder er bietet es Dritten als kostenpflichtigen Dienst an. Die Preise liegen bei USD 350 pro Woche für 5000 bis 6000 Bots.

Bots hinter einer Firewall versenden nur Spam, wohingegen Bots, die ohne Firewall betrieben werden und gut erreichbar sind, für das Hosten von Malware, Spam- und Phishingseiten genutzt werden.

Wird ein Bot identifiziert und vom Netz genommen, so übernimmt ein anderer automatisch seine Funktion. Die Rückverfolgung führt in der Regel zu einem unwissenden und überraschten Besitzer. Hinzu kommt, dass Botnetze international aufgestellt sind und keine geografischen oder rechtlichen Grenzen kennen. Immerhin wurde in diesem Frühjahr ein 18jähriger Neuseeländer verurteilt, welcher ein Botnetz mit über 1,3 Millionen Bots betrieben hatte.

Auf einem Botnetz werden typischerweise folgende Aktionen ausgeführt:

Gegen Dritte gerichtete Aktionen

- Versand von Spam-, Phishing-Mails;
- Hosting und Betrieb von Phishing- oder Malware-Sites;
- Speichermedium zur Verbreitung illegaler Inhalte;
- Ausführen von DDoS Attacken;
- Weiterleiten von Kommunikation zur Verschleierung des Ursprungs (sog. Proxies);

Cyber-Verbrecher wenden heute bekannte Geschäftsmethoden wie Arbeitsteilung und Spezialisierung zur Effizienzsteigerung und zur Realisierung von Skalenerträgen an.

- Systematische Suche nach Passwörtern für den Zugang zu Benutzerkonten, z. B. Webmail, Social Networks, usw.

Gegen den Eigentümer gerichtete Aktionen

- Ausspähen lokaler Daten (Zuganspasswörter, Mail-Adressen, persönliche Daten für Identitätsdiebstahl);
- Ausspähen lokaler Verbindungen (Mail, Webforms, E-Banking, …);
- Angriffe auf das lokale/interne Netzwerk.

Der Aufbau von Botnetzen erfolgt über verschiedene Kanäle, wie z. B. mittels Infektion durch Viren, über E-Mails, Schwachstellen im Browser, mit Applikationen, die der Benutzer herunterlädt und für legitim hält (interessante Programme, Spiele, …), oder mit Würmern, von Dritten erhaltenen USB-Sticks usw.

Organisierte Kriminalität

Die Qualität der Angriffswerkzeuge und die Art des Vertriebs zeigen, dass kriminelle Angreifer heute bekannte betriebliche Ansätze wie Arbeitsteilung und Spezialisierung zur Effizienzsteigerung und zur Realisierung von Skalenerträgen anwenden. Die technische Expertise für Cyber-Attacken muss daher nicht selbst aufgebaut werden; vielmehr wird das benötigte Spezialwissen eingekauft.

Einige Werkzeuge bieten aktuellste Angriffsvarianten per Abonnement an. Malware wird auch schon mal mit einer «Geld-zurück-Garantie» beworben, für den Fall, dass ein Anti-Viren-

Programm innert 30 Tagen ab Kauf die Malware entdecken sollte.

Wir erleben derzeit den Wandel von unkoordinierten Einzelangriffen zu einer auf Dienstleistung ausgerichteten Ökonomie – «Malware as a Service»:

- Verkauf oder Leasing von schädlicher Software und von Angriffsplattformen;
- Pay-per-visit oder Pay-per-infection-Angebote.

Die den Opfern gestohlene Information wird direkt in Untergrundmärkten und Auktionen zum Verkauf angeboten. Die folgende Auflistung zeigt typische Angebote und deren Preise:

Auf der anderen Seite stehen Millionen Internetbenutzer und eine Softwareindustrie ohne Produktehaftung oder minimale Sicherheitsstandards.

- Personenidentität: 1–15 USD;
- Login für Online-Auktionen: 1–8 USD;
- Login für E-Mail: 4–30 USD;
- E-Mail-Adressen: 0.83–10 USD/Million;
- Kreditkarten: 0.40–20.0 USD;
- Bankkonten: etwa 1/10 des Saldos.

Der Preis für die Zugangsdaten zu Bankkonten hängt vom verfügbaren Saldo, der Bank und dem Land ab. Er widerspiegelt das Risiko für einen erfolgreichen Geldtransfer. Operiert wird zudem nach dem Prinzip «Distribute Pain/Concentrate Gain». Die enorme Grösse des Internet-Marktes aus Sicht der Cyberkriminellen erlaubt die Verteilung der Verluste auf Tausende oder Hunderttausende. Eine Belastung von USD 10 auf 10 000 Kreditkarten von fünf unterschiedlichen Banken ergibt einen Gewinn von 100 000 USD. Dagegen fällt eine einzelne Belastung in der Höhe von USD 10 dem Opfer entweder nicht auf oder die Weiterverfolgung wird als nicht lohnenswert erachtet. Ein Verlust von USD 20 000 ist für eine Bank zu gering, um den Aufwand für die Verfolgung einiger tausend Transaktionen zu leisten. Die Strafverfolgungsbehörden können und werden nichts tun, ausser es gehen so viele Klagen ein, dass das Problem als genügend gross zur Rechtfertigung der benötigten Ressourcen erkannt wird.

Arbeitsteilung und Spezialisierung ermöglichen Angriffe von einer Qualität und Grösse, wie sie ein Einzelner nie durchführen könnte. Dies wird direkt sichtbar im vermehrten Auftreten von lokalisierten Phishing-Attacken, welche in korrekter Sprache (z. B. Deutsch) formuliert sind, auf lokale Gegebenheiten Bezug nehmen (z. B. lokale Ereignisse wie Unwetter, Erdbeben, Wahlen) und vermehrt auch Nischenanbieter betreffen (z. B. lokale und kleinere Finanzinstitute).

Dies sind eindeutige Indizien dafür, dass hinter den Angriffen mafiöse, kriminelle Organisationen stehen.

Ausblick und Massnahmen

Wir mussten in den letzten Jahren erkennen, dass Sicherheit im Internet nicht nur mit technischen Massnahmen erreicht werden kann. Folglich genügt zum Verständnis von Cyberkriminalität und der Entwicklung von geeigneten Gegenmassnahmen eine rein technische Betrachtungsweise nicht. Wichtig ist es, die ökonomischen Anreizsysteme zu verstehen. Kriminelle Organisationen haben entdeckt, dass ihnen das Internet neue Möglichkeiten und Skalenerträge erlaubt. Das anhaltende Wachstum des E-Commerce im Internet bietet gewaltige Aussichten für illegale Profite mit geringem Risiko. Auf der anderen Seite stehen Millionen Nutzer und eine Softwareindustrie mit minimalen Sicherheitsstandards und ohne Produktehaftung.

Weiter zeigt der Erfolg von Phishing und Social Engineering, dass kriminelle Organisationen immer weniger auf technische Schwachstellen angewiesen sind.

Der Angreifer muss nur schlauer sein als das Opfer

Gut organisierte und professionell agierende Kriminelle sind unsere ständigen Begleiter, bisher in der realen und nun auch in der virtuellen Welt. Wir müssen dies verstehen und lernen, damit umzugehen, also die Risiken zu erkennen, sie zu akzeptieren und sie zu möglichst klein zu halten. Die Betreiber von Warenhäusern haben längst erkannt, dass sich Ladendiebstähle nicht vollständig vermeiden lassen und somit einkalkuliert und auf ein erträgliches Mass reduziert werden müssen.

Effektive Massnahmen gegen die Cyberkriminalität fordern die Gesellschaft, die Technik und das Individuum heraus. Sensibilisierung und Ausbildung, grenzüberschreitende Koordination der Behörden und die Einführung minimaler Qualitätsstandards für Software und einer verbindlichen Produktehaftung müssen auf der Stufe der Gesellschaft angegangen werden.

Die Technik ist gefordert, Produkte mit verbesserter Sicherheit (aktiver und auch passiver) zu liefern und eine herstellerübergreifende Integration voran zu treiben. Hinzu kommt die Forderung nach verbesserter Bedienbarkeit für Endbenutzer: Sicherheit, die nicht verstanden wird, ist schlichtweg inexistent.

Nicht zuletzt jedoch liegt die Verantwortung bei uns allen: Wir sind angehalten, sorgfältig mit unseren persönlichen Daten umzugehen und Online-Angebote kritisch zu hinterfragen. ■

Zeitschrift für Datenrecht und Informationssicherheit
digma
www.digma.info
erscheint vierteljährlich

Meine Bestellung

❑ 1 Jahresabonnement digma (4 Hefte des laufenden Jahrgangs)
à **CHF 158.00** bzw. bei Zustellung ins Ausland **EUR 123.00** (inkl. Versandkosten)

Name Vorname

Firma

Strasse

PLZ Ort Land

Datum Unterschrift

Bitte senden Sie Ihre Bestellung an:
Schulthess Juristische Medien AG, Zwingliplatz 2, CH-8022 Zürich
Telefon +41 44 200 29 19
Telefax +41 44 200 29 18
E-Mail: zs.verlag@schulthess.com
Homepage: www.schulthess.com

Schulthess §