Internet-Kriminalität – ein gut organisierter Wirtschaftszweig

International operierende Banden profitieren von Sicherheitslücken im Internet, minimalen Sicherheitsstandards der Software und der Bequemlichkeit der Benutzer.

VON BERNHARD PLATTNER UND STEFAN FREI

In Kürze **Die zunehmende Bedeutung des Internets in Wirtschaft und Gesellschaft bietet Kriminellen Aussichten auf illegale Profite mit kleinem Risiko. Hinter Viren, Spam, und Phishing stehen nicht mehr einsame Hacker, sondern international operierende Banden. Diese arbeiten professionell: Arbeitsteilung, Automatisierung und Spezialisierung bringen raffinierte Attacken hervor. Entstanden ist eine service-basierte Ökonomie mit «Malware as a Service» als Angebot und einer weltweiten Nachfrage.**

PROF. DR. BERNHARD PLATTNER lehrt Technische Informatik an der ETH Zürich und ist Vorsteher des Instituts für Technische Informatik und Kommunikationsnetze. Er forscht und lehrt im Bereich Computernetze und IT-Sicherheit.
plattner@tik.ee.ethz.ch

DR. STEFAN FREI ist Research Analyst Director bei Secunia in Kopenhagen. Er ist für die Forschung im Bereich Cybersecurity verantwortlich und lehrt an der ETH Zürich. Secunia identifiziert und dokumentiert Sicherheitslücken in über 29 000 Softwareprodukten für Unternehmen und Regierungsbehörden rund um den Globus.
sfrei@secunia.com

Um die gegenwärtige Bedrohungslage zu verstehen und neue Entwicklungen bewerten zu können, ist es nützlich, einen Schritt zurück zu tun, um mit erweitertem Blickwinkel die wichtigsten Akteure zu erfassen und zu charakterisieren. Dazu soll die Entwicklung der Sicherheit im Internet in den vergangenen drei Jahrzehnten betrachtet werden. 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.

In der Pionierzeit des Internets waren die Benutzer gleichzeitig Designer und Entwickler, die in einer fast ausschliesslich akademischen Umgebung mit einer neuen Technologie experimentierten. 1994 gelangte das Internet ins Blickfeld der Öffentlichkeit, angestossen durch die «Killer-Applikation» World Wide Web und die Verfügbarkeit des auch für Nichttechniker brauchbaren Web-Browsers Mosaic. Die zunehmende Bedeutung des Internets blieb auch einsamen Hackern nicht verborgen, die Spass daran fanden, den Betrieb zu beeinträchtigen und berühmt zu werden. Ihre Aktivitäten führten zu ernst zu nehmenden Störungen: Würmer mit einer massiven und schnellen Verbreitung wie Melissa, Code Red, SQL-Slammer und Mircrosoft Blaster legten Teile des Internets lahm und erreichten weltweite Publizität.

Mit dem Aufkommen organisierter Krimineller, die das Internet als neues Spielfeld für profitable Geschäfte entdeckten, wurde klar, dass durch Würmer verursachte massive Störungen des Betriebs nicht das Mass aller Dinge sein konnten. Die Kriminellen begannen, schlecht geschützte, mit Schwachstellen versehene PCs von Privatpersonen anzugreifen und zu kontrollieren, ohne dass deren Besitzer sich dessen bewusst waren. Die übernommenen Rechner wurden in ein sogenanntes Botnetz, ein Netz von «Robotern», eingefügt und konnten nach Belieben für verschiedene Anwendungen eingesetzt werden, etwa für das Versenden von Spam oder für gezielte Angriffe auf einzelne Dienste im Netz.

Mit dem Aufkommen von Web 2.0 und der damit verbundenen rasanten Verbreitung komplexer Web-Dienste (zum Beispiel Software as a Service mit Google Docs und Social Networks) wurden neue technische Angriffsszenarien machbar, da sich das Web vermehrt zu einem Zweiweg-Medium entwickelte. Die Verbreitung neuer Plattformen wie Youtube, Facebook und Myspace verschafft potenziellen Angreifern 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, beispielsweise zu ihren Bankverbindungen, gebracht werden) steht erst am Anfang. Rein technische

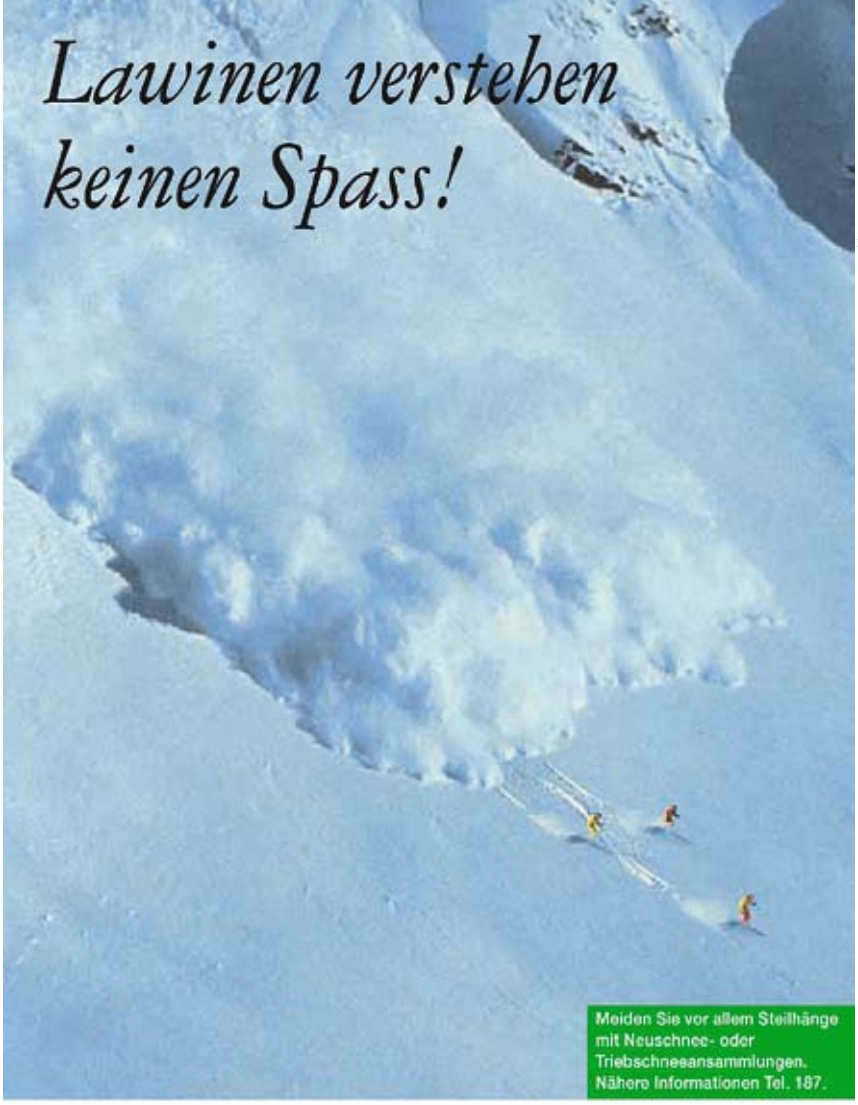

Bild: suva

Sicherheit in der Freizeit: Trotz Spass ist im Wintersport Vorsicht angebracht.

Angriffe werden dadurch ersetzt oder wirksam ergänzt.

Während in der Vergangenheit die Technik der Angriffsmethoden durch Fachleute im Untergrund entwickelt wurde, prägen heute gut organisierte, professionell und kommerziell handelnde kriminelle Organisationen das Bild. Die Angriffsmethoden heutiger Cyberkrimineller sind vielfältig und werden schnell an neue Gegebenheiten angepasst.

Die heute im Büro und im privaten Umfeld eingesetzten IT-Systeme haben zwei grundlegende Arten von Schwachstellen: Erstens sind dies Software- oder Hardware-Schwachstellen, die von Angreifern mit sogenannten Exploits genutzt werden können. Ein Exploit ist ein speziell gestaltetes Programm oder ein Inhalt, dessen Ausführung zur Folge haben kann, dass der Angreifer die Kontrolle über den PC des Opfers übernehmen kann. Zweitens stellen die Eigentümer und Benutzer von PCs selbst Schwachstellen dar, indem sie unbedarft Anhänge von E-Mails öffnen oder Programme aus dubiosen Quellen installieren und damit einem Angreifer die Übernahme ihres Rechners ermöglichen.

Trotz Firewalls: Rechner haben technische Schwachstellen

An technischen Schwachstellen besteht kein Mangel: Im Bericht über das erste Halbjahr 2010 weist der dänische Sicherheitsspezialist Secunia darauf hin, dass jährlich durchschnittlich 4500 Schwachstellen identifiziert und beschrieben werden. Schwachstellen finden sich in Betriebssystemen (Windows, Mac-OS, Linux), in Web-Browsern (Internet Explorer, Firefox, Safari), in Web-Servern (Apache, IIS), aber auch in populären Zusatzprogrammen wie dem Adobe Reader oder Adobe Flash Player.

Der breite Einsatz von Firewalls und immer besser geschützten Server-Systemen hat die Intensität der Angriffe 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 anzugreifen, müssen zwei Bedingungen erfüllt sein:

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

Die erste Bedingung ist leider allzu oft erfüllt. In einer 2008 an der ETH Zürich in Zusammenarbeit mit Google und IBM durchgeführten Studie wurde nachgewiesen, dass über 40 Prozent der weltweiten Internet-Nutzer mit einem nicht vollständig gepatchten, das heisst 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 durch den Besuch einer unverdächtigen Webseite. Dafür werden von Angreifern gezielt häufig besuchte Webseiten ohne Wissen ihrer Betreiber manipuliert. Die Web-Browser der Besucher werden danach auf einen von den Angreifern betriebenen Webserver umgeleitet, der verwundbare Rechner als solcher identifiziert und infiziert. Dieser Vorgang bleibt den Nutzern verborgen und ist insofern tückisch, als diese die besuchte Website als vertrauenswürdig einstufen. Diese Form eines Angriffs nimmt ständig zu und hat mittlerweile E-Mail als primäre

Methode für die Verbreitung von Malware verdrängt.

Die Infizierung geschieht oft innert weniger Minuten

Seit Längerem nimmt die Automatisierung von Internet-Attacken zu. Das Internet wird fortwährend nach verwundbaren Computern abgesucht, die dann automatisch angegriffen werden. Ein ungeschützt ans Internet angeschlossener Computer wird oft innert weniger Minuten infiziert.

Den Cyber-Verbrechern stehen dazu verschiedene Angriffswerkzeuge zur Verfügung, welche die Planung und Durchführung von Angriffskampagnen automatisieren. Die Angriffswerkzeuge sind ausgereift, sowohl was ihre technische Funktionalität als auch die eingebauten Verwaltungsfunktionen und die Art ihres Betriebs betrifft. Sie sind durchgängig modular aufgebaut, um eine schnelle Integration neuer Angriffstechniken zu gewährleisten. Zur Verhinderung ihrer Entdeckung, Rückverfolgbarkeit und Analyse kommen raffinierte technische Verfahren zum Einsatz.

Heutige Angriffswerkzeuge lassen sich an die Bedürfnisse des jeweiligen «Kunden» anpassen und verfügen über 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. Der Erfolg wird genauestens gemessen, was wertvolle Informationen für die Optimierung einer Kampagne und die kontinuierliche Weiterentwicklung der Malware liefert.

Bekannte Angriffswerkzeuge sind IcePack, Mpack, Neosploit und Zeus. IcePack erschien erstmals im Juli 2007 und wird als IcePack Light Edition für 30 US-Dollar oder IcePack Platinum Edition für 400 US-Dollar 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 500 bis 1000 US-Dollar weltweit angeboten. Mpack wie auch IcePack ermöglichen automatisierte Attacken gegen Web-Browser, angeblich mit einer Erfolgsrate von 40 bis 50 Prozent.

Eine Malware, die das Zielsystem infizieren soll, durchläuft eine rigorose Qualitätsprüfung und wird vor der Auslieferung so lange 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
- eine Variante wird nur für eine begrenzte Anzahl Infektionen verwendet.

Damit wird einerseits die Wahrscheinlichkeit, dass die Malware von Anti-Viren-Programmen erkannt wird, stark reduziert; andererseits werden die Hersteller von Anti-Viren-Programmen mit einer grossen Anzahl neuer Varianten konfrontiert, was enorme Ressourcen bindet und die Fähigkeit, zeitgerecht neue Signaturen zu produzieren, beeinträchtigt. Die infizierten Systeme werden sodann üblicherweise in ein Botnetz integriert.

Botnetze stellen genügend Rechenkapazität bereit

Kriminelle Aktivitäten, wie der Massenversand von Spam oder das «Hosten» (Betreiben) von Phishing-Webseiten, setzen eine entsprechende Infrastruktur voraus. Dazu werden 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, beispielsweise durch Infektion mit Viren, über E-Mails, Schwachstellen im Browser, mit Applikationen, die der Benutzer herunterlädt und für legitim hält, oder sogar mit von Dritten erhaltenen USB-Sticks.

Die Bot-Software schützt sich selbst: Eventuell vorhandene Anti-Viren-Software und Auto-Update-Mechanismen werden deaktiviert, die Firewall wird umkonfiguriert und die Bot-Prozesse werden versteckt ausgeführt, um einen möglichst zuverlässigen und langen Betrieb des Bots sicherzustellen. Anschliessend wird der Rechner in ein Botnetz integriert und zuerst Aktionen ausgeführt, die sich gegen den Eigentümer des Rechners richten: Ausspähen lokaler Daten und lokaler Verbindungen (Zugangsschlüssel, Mail-Adressen, persönliche Daten) mit dem Ziel, die Identität des Eigentümers zu missbrauchen. Danach folgen Angriffe auf das lokale oder firmeninterne Netz. Erst zu einem späteren Zeitpunkt wird der Bot vollständig aktiv und hilft beim Versand von Spam- oder Phishing-Mails mit oder wird für das Hosten von Phishing oder Malware-Sites eingesetzt. Weitere Einsatzgebiete sind die Verbreitung illegaler Inhalte (harte Pornografie, urheberrechtlich geschützte Inhalte), das Ausführen von Denial-of-Service (Überlastung von Infrastruktur-

systemen)-Angriffen sowie die systematische Suche nach Passwörtern für den Zugang zu Benutzerkonten von Webmail-Diensten und sozialen Netzen. Der Botmaster nutzt sein Botnetz selbst oder er bietet es Dritten als kostenpflichtigen Dienst an. Die Preise liegen bei 350 US-Dollar pro Woche für 5000 bis 6000 Bots. Aktuelle Entwicklungen sind multifunktional einsetzbare Botnetze, in die neue Funktionen bei Bedarf nachgeladen werden können.

Zur zentralen Steuerung werden kryptografisch geschützte Netze (Command and Control Networks) verwendet, welche die Rückverfolgung erschweren. Wird trotzdem ein Bot identifiziert und vom Netz genommen, so übernimmt ein anderer automatisch dessen Funktion. Die Rückverfolgung durch die Behörden führt in der Regel zu einem unwissenden und überraschten Endbenutzer. Hinzu kommt, dass Botnetze international sind und keine nationalen oder rechtlichen Grenzen kennen. Unter diesen Umständen ist es äusserst schwierig, diese Aktivitäten zu unterbinden oder die Drahtzieher dahinter zu identifizieren. Immerhin gelang es dem FBI in den Jahren 2007 und 2008, in koordinierten Aktionen einige Betreiber von Botnetzen aufzuspüren. Sie wurden teilweise zu langjährigen Gefängnisstrafen verurteilt.

Bisher waren es vor allem Schwachstellen in Betriebssystemen und Web-Browsern, die als Wegbereiter für Angreifer dienten. Nun rücken jedoch Schwachstellen in Anwendungen von Drittherstellern, wie zum Beispiel Adobe, Oracle oder HP in den Vordergrund. Berichte von Microsoft, Secunia und ScanSafe argumentieren, dass für mehr als 80 Prozent aller Sicherheitsvorkommnisse Schwachstellen in Programmen von Drittherstellern verantwortlich sind. Auch die Firma Adobe (Acrobat Reader, Flash Player) ist kürzlich in die Kritik geraten und hat in der Folge Besserung gelobt.

Populäre Software in PCs ist das wichtigste Ziel von Attacken. Doch ein kürzlicher Angriff auf eine in industriellen Steuerungen und Automationssystemen eingesetzte Software der Firma Siemens (SIMATIC WinCC) hat aufhorchen lassen. Zwar verwendeten die Angreifer eine Sicherheitslücke im Windows-Betriebssystem, aber die bisher festgestellten Angriffe konzentrierten sich primär auf die sogenannten SCADA-Systeme (Supervisory Control and Data Access System).

Software-Schwachstellen sind die primären Wegbereiter für Angriffe aus dem Internet. Die Angreifer spekulieren darauf, dass viele schlecht gewartete Rechner im Netz sind. Deshalb ist darauf zu achten, dass die Programme jeweils auf dem neusten Stand sind, indem alle Sicherheitsupdates installiert werden, sobald sie verfügbar sind. Ebenfalls ist die Aktivierung einer Firewall und die Installation eines Anti-Viren-Programmes essentiell, denn häufig werden für Angriffe längst bekannte Schwachstellen genutzt.

Doch wie bringt man den eigenen Rechner auf den aktuellen Stand der Technik? Selbstverständlich müssen die automatischen Updates für das Betriebssystem eingeschaltet sein. Der erwähnte Bericht von Secunia zeigt jedoch, dass die Hälfte der Nutzer mehr als 66 Programme von mehr als 22 verschiedenen Herstellern installiert hat. Das bedeutet, dass die Nutzer jährlich mehr als 75 sicherheitsrelevante Ratschläge befolgen müssten, indem sie Updates herunterladen und installieren, von verschiedenen Webseiten mit jeweils herstellerspezifischer Darstellung und mit Mechanismen, die von Hersteller zu Hersteller variieren. Es liegt auf der Hand, dass die Komplexität dieses Prozesses viele davon abhält, ihre Rechner zu pflegen. Ein (noch nicht vorhandener) herstellerunabhängiger, standardisierter Update-Mechanismus würde

Daten-transparenz?

die Komplexität vermindern und zu besserem Schutz führen.

Etwas weniger komfortabel als das automatische Nachführen aller installierten Programme ist der von der Firma Secunia kostenlos bereitgestellte Personal Software Inspector (PSI). Das Programm stellt die Versionsnummern der auf einem System installierten Programme fest und vergleicht sie mit den Daten einer aktuell gehaltenen Programm- und Patch-Datenbank.

Nur wenige Nutzer kümmern sich um Sicherheits-Updates

Stellt der PSI ein veraltetes oder unsicheres Programm fest, wird der Nutzer informiert und direkt zur Webseite des Herstellers geführt, wo die aktuelle Version oft einfach heruntergeladen werden kann. Secunia PSI wird gegenwärtig von über 2,6 Millionen Nutzern verwendet. Dies ist jedoch eine kleine Zahl, gemessen an den weltweit 1,6 Milliarden Nutzern des Internets.

Zum Verständnis von Cyberkriminalität und der Entwicklung von geeigneten Gegenmassnahmen genügt die technische Betrachtungsweise nicht. Wichtig ist auch, die ökonomischen Anreizsysteme zu verstehen. Das Internet erlaubt kriminellen Organisationen neue Möglichkeiten und Skalenerträge. 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.

Die Bedienbarkeit muss besser werden: Sicherheit, die nicht verstanden wird, ist inexistent.

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

Effektive Massnahmen gegen die Cyberkriminalität fordern die Technik, die Gesellschaft und das Individuum heraus. Sensibilisierung und Ausbildung, Rechtsetzung, welche die internationale Dimension des Problems berücksichtigt, grenzüberschreitende Koordination der Behörden und die Einführung minimaler Qualitätsstandards für Software und einer verbindlichen Produktehaftung müssen von der Gesellschaft angegangen werden.

Die Technik ist gefordert, Produkte mit verbesserter Sicherheit (aktiver und passiver) zu liefern und eine herstellerübergreifende Integration voranzutreiben. Hinzu kommt die Forderung nach verbesserter Bedienbarkeit für Endbenutzer: Sicherheit, die nicht verstanden wird, ist inexistent. Nicht zuletzt liegt die Verantwortung bei allen: Wir sind angehalten, sorgfältig mit unseren persönlichen Daten umzugehen und Online-Angebote kritisch zu hinterfragen. ■