



W H I T E P A P E R

Das Wettrüsten der Cyberkriminellen



Eugene Kaspersky
Gründer und CEO, Kaspersky Lab

Cyberkriminalität ist kein vorübergehendes Phänomen

In unserer modernen Gesellschaft verbringen inzwischen viele Menschen einen beträchtlichen Teil ihrer Zeit im Internet. Die virtuelle Welt ist in vielerlei Hinsicht ein Spiegelbild unserer realen Welt. Kriminelle - ein unschöner, aber fester Bestandteil unseres sozialen Lebens - sind ganz selbstverständlich auch in der virtuellen Welt aktiv.

Das System Cyberkriminalität ist dabei, mit etablierten Beziehungen und Geschäftsmodellen seine Reife zu erlangen.

Eugene Kaspersky

Cyberkriminalität breitet sich immer weiter aus, da der zunehmende Austausch von Geld und Daten im Internet ein verlockendes Ziel für Übeltäter darstellt. Nun ist das System Cyberkriminalität dabei, seine Reife zu erlangen – so existieren in diesem Bereich bereits etablierte Beziehungen und Geschäftsmodelle. Eine neue Klasse von Cyberkriminellen handelt ganz offen mit böartigem Code. Ganz gleich ob kleine Betrüger, die wiederholt versuchen, geringe Beträge zu stehlen, oder Personen, die große Summen auf einmal ergaunern: Cyberkriminalität ist eine Realität.

Cyberkriminalität als Geschäft

Moderne Cyberkriminalität funktioniert wie jedes andere Geschäft. Cyberkriminelle wenden dabei herkömmliche Geschäftsprinzipien wie Rentabilität, einfache Nutzung, Risikomanagement und Auswahl von Wachstumsmärkten an.

Cyberkriminalität ist lukrativ

Das wichtigste Kriterium für jegliche Art von Geschäft ist Rentabilität. Cyberkriminalität ist dabei keine Ausnahme. Ganz im Gegenteil: Cyberkriminalität ist äußerst lukrativ. Es werden einmalig große Summen gestohlen, genauso wie wiederholt kleinere Geldbeträge. Allein im Jahr 2007 wurde fast jeden Monat über größere Fälle von Cyberkriminalität berichtet.

Das wichtigste Kriterium für jegliche Art von Geschäft ist Rentabilität. Cyberkriminalität ist dabei keine Ausnahme.

Eugene Kaspersky

► **Januar 2007** – Russische Hacker stehlen mithilfe von Mittelsmännern aus Schweden 800.000 Euro von der schwedischen Bank Nordea.

Kriminelle Aktivitäten waren schon immer ein Spiegelbild legitimer Geschäfte – ein Beispiel wäre der Buchhalter der Mafia, der wie jeder andere Buchhalter die Geschäfte des „Unternehmens“ regelt. Dennoch ist der Bereich Cyberkriminalität zurzeit nicht in Form einer oder mehrerer weltweit agierender Mafia-Organisationen mit einer „Dr.-No“-Figur an der Spitze organisiert. Es handelt sich eher um miteinander verflochtene Gruppen, die verschiedene Funktionen übernehmen. Eine Person oder Gruppe, die ein Botnetz zum Ausführen von DDoS-Angriffen oder zum Verschicken von Spam-Nachrichten besitzt, benötigt zum Beispiel E-Mail-Adressen. Eine andere Person, die den Besitzer des Botnetzes nicht einmal kennen muss, füllt diese Lücke, indem sie die benötigten Adressen stiehlt und anschließend verkauft. Das läuft wie in der legalen Geschäftswelt ab. Genauso wie die Niederlassung eines großen Motorenherstellers in einer Region verwandte Unternehmen anzieht (zum Beispiel Hersteller von Vergasern, Muttern und Schrauben), müssen Cyberkriminelle nicht über eine feste Organisation miteinander verbunden sein. Sie können einfach zum gegenseitigen wirtschaftlichen Nutzen agieren.

► **Februar 2007** – Die brasilianische Polizei verhaftet 41 Hacker, die mithilfe eines Trojaners Daten von Bankkonten gestohlen und damit 4,74 Millionen Dollar ergaunert haben.

► **Februar 2007** – In der Türkei werden 17 Mitglieder einer Bande verhaftet, die durch Betrug im Internet bis zu 500.000 Dollar gestohlen haben.

► **Februar 2007** – Li Jun wird wegen der Verbreitung des Panda-Wurms verhaftet, mit dem Kontonamen von Online-Spielen und Instant-Messaging-Anwendungen (IM) ausgespäht wurden. Durch den Verkauf der Malware soll Li Jun 13.000 Dollar verdient haben.

► **März 2007** – In Großbritannien werden fünf Osteuropäer wegen Kreditkartenbetrugs verhaftet. Der Schaden beträgt geschätzte 1,7 Millionen Pfund.

► **Juni 2007** – In Italien werden 150 Cyberkriminelle verhaftet. Sie sollen italienische Internetnutzer mit gefälschten E Mails bombardiert und damit 1,25 Millionen Euro ergaunert haben.

► **Juli 2007** – Russische Cyberdiebe sollen mithilfe eines Trojaners 500.000 Dollar von türkischen Banken gestohlen haben.

► **August 2007** – Der Ukrainer Maxim Yastremsky (alias „Maksik“) wird in der Türkei unter dem Vorwurf festgenommen, mit Identitätsdiebstahl zig Millionen Dollar verdient zu haben.

► **September 2007** – Gregory Kopiloff wird in den USA dafür angeklagt, mithilfe der P2P-Filesharing-Programme Limewire und Soulseek Daten gesammelt zu haben, die anschließend für Identitätsbetrug verwendet wurden. Kopiloff soll durch den Verkauf der gestohlenen Daten mehrere Zehntausend Dollar verdient haben.

► **Dezember 2007** – Cyberkriminelle brechen in die Computer des Oak Ridge National Laboratory (ORNL) ein, das zum Energieministerium der USA gehört. Angeblich gehören auch das Los Alamos National Laboratory sowie das Lawrence Livermore National Laboratory zu den Zielen. Bei diesem Angriff werden 12.000 Sozialversicherungsnummern und Geburtsdaten von ORNL Besuchern aus den Jahren 1999 bis 2004 gestohlen. Der Einbruch stellt eine Verletzung der nationalen Sicherheit dar und setzt die betroffenen Personen Identitätsdiebstahl und finanziellem Betrug aus.

Die meisten Fälle von Cyberkriminalität werden von den betroffenen Unternehmen intern oder von Ermittlungsbehörden verdeckt untersucht. Die Ergebnisse werden nur in den seltensten Fällen öffentlich gemacht.

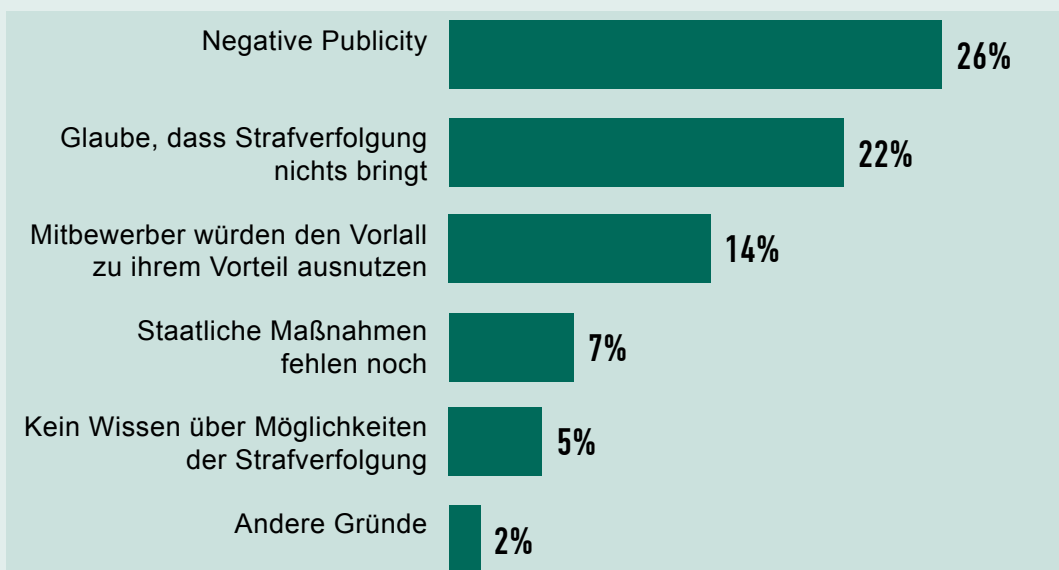
Eugene Kaspersky

► **Oktober 2007** – Greg King wird in den USA für seine Beteiligung an dem DDoS-Angriff auf Castle Cops im Februar 2007 verhaftet; ihm drohen 10 Jahre Gefängnis sowie eine Geldstrafe von 250.000 Dollar.

► **November 2007** – Das FBI verhaftet im Rahmen der zweiten Phase der Anti-Botnetz-Initiative „Operation Bot Roast“ acht Personen. Durch diese Initiative sollen bereits wirtschaftliche Schäden im Umfang von 20 Millionen Dollar sowie eine Million angegriffene Computer aufgedeckt worden sein.

Bei diesen Beispielen handelt es sich lediglich um die Spitze des Eisbergs. Die Opfer und/oder Ermittlungsbehörden haben diese Beispiele zur öffentlichen Diskussion freigegeben. Die meisten Fälle von Cyberkriminalität werden von den betroffenen Unternehmen allerdings intern beziehungsweise von den Ermittlungsbehörden verdeckt untersucht. Die Ergebnisse werden nur in den seltensten Fällen öffentlich gemacht. Die Grafik aus einem aktuellen Bericht des Computer Security Institute zeigt, warum Unternehmen Fälle von Cyberkriminalität fast nie öffentlich machen.

Gründe, warum Unternehmen digitale Einbrüche nicht melden



CSI 2007 Computer Crime and Security Survey
Quelle: Computer Security Institute

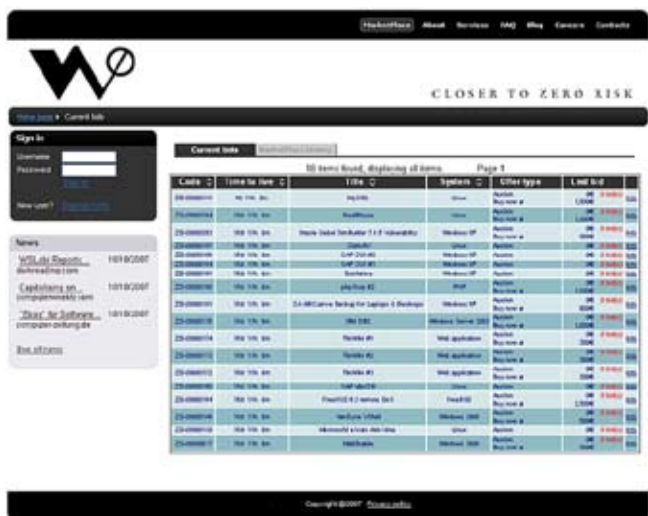
2007: 196 Befragte

Cyberkriminalität: einfach und risikoarm

Der zweite Schlüsselfaktor für die Zunahme von Cyberkriminalität als Geschäft ist das geringe Risiko. Der psychologische Aspekt, das Opfer zu sehen, dient in der realen Welt auch als Abschreckung. In der virtuellen Welt jedoch bekommen die Kriminellen ihre Opfer nie zu Gesicht. Reiche Unternehmen oder Personen, die man weder sehen noch anfassen kann, sind leichter zu bestehlen. Neben dem Deckmantel der Anonymität stehen verschiedenste Online-Ressourcen zur Verfügung, mit denen sich Schwachstellen verkaufen, Trojaner zum Aufbau von Botnetzen verwenden oder ganze Botnetze mieten lassen (siehe Abbildungen 2 und 3). Da immer mehr Menschen über ausreichende Internet-Kenntnisse verfügen, wird es zunehmend einfacher, Cyberkriminalität als Geschäft auszuüben.



Screenshot einer Website, über die Botnetze verkauft werden



Screenshot einer Website, über die neue Schwachstellen verkauft werden

Cyberkriminelle nutzen die Chancen des Web 2.0

Die ungeheure Menge an neuen Diensten, die über das Internet angeboten werden, sowie die Vielzahl der Menschen in der ganzen Welt, die diese Dienste gerne in Anspruch nehmen, tragen ebenfalls zum Erfolg von Cyberkriminalität bei. Zu den besonders angriffsgefährdeten Bereichen gehören folgende Bereiche:

Finanztransaktionen im Internet und Online-Banking – E Commerce-Unternehmen und Banken arbeiten unablässig daran, bei Online-Finanztransaktionen für Geschwindigkeit und Benutzerfreundlichkeit auf der einen und ausreichende Sicherheit auf der anderen Seite zu sorgen. Dennoch gibt es zahlreiche Möglichkeiten für Cyberkriminelle, zum Beispiel Kontodaten und Geld zu stehlen.

Anlagen zur Datenspeicherung und „Cloud Computing“ – Da Daten und Anwendungen zunehmend auf externen Remote Servern gespeichert werden, können Kriminelle den Datenverkehr abfangen, um Zugriff auf finanzielle, vertrauliche und andere sensible Daten zu erhalten.

Online Spiele – Zu den Cyberverbrechen gehört auch der Diebstahl von virtuellem Eigentum und Kennwörtern von Online-Spielen, die mit einem beträchtlichen Gewinn weiterverkauft werden.

Online Börsen – Diese einfache und schnelle Methode, auf Änderungen von Börsennotierungen reagieren zu können, ist ein verführerisches Ziel für Kriminelle – auch hier kann viel Geld verdient werden.

Web 2.0 – Soziale Netzwerke im Internet, Blogs, Foren, Wikis, MySpace, YouTube, Twitter – all diese Angebote basieren auf dem einfachen Herunterladen und Veröffentlichen sowie verschiedenen Methoden zur gemeinsamen Nutzung von Daten. Dabei geht jeder Teilnehmer das Risiko ein, zum Opfer von Malware zu werden.

Jede Generation von Kriminellen wählt ihre eigenen Werkzeuge. Moderne Cyberkriminelle nutzen bevorzugt Trojaner als Waffen, um Botnetze aufzubauen, Kennwörter und vertrauliche Daten zu stehlen, DoS Angriffe auszuführen oder Daten zu verschlüsseln, um Opfer erpressen zu können.

Ein besonders beunruhigendes Merkmal moderner Angriffe ist das Bestreben, die eigene Präsenz auf dem infizierten System aufrechtzuerhalten. Cyberkriminelle verwenden verschiedene Methoden, um dieses Ziel zu erreichen. Manche führen gezielte Angriffe aus, die sich an bestimmte Unternehmen richten. Das Verfassen von Malware für spezielle Ziele ist zwar schwierig und zeitaufwändig, doch sobald die gezielten Angriffe einmal lanciert worden sind, führen sie fast immer zum Erfolg. In der Regel sorgen diese Angriffe für eine ansehnliche Rendite, so dass gezielte Angriffe eine kleine, aber wichtige Form von Cyberkriminalität darstellen.

Moderne Botnetze

Moderne Botnetze bestehen aus einer teilweise recht großen Zahl infizierter Computer, die sich einfach steuern lassen und eine bequeme Verarbeitung der gesammelten Daten ermöglichen. Der erzielte Gewinn hängt sowohl von der Zahl der Opfer als auch der Häufigkeit ab, mit der neue Malware installiert werden muss. Je länger die Malware auf den Computern aktiv bleibt, desto mehr lässt sich damit verdienen. Andere verbreitete und effektive Methoden, mit denen moderne Cyberkriminelle ihre Gewinnmargen erhöhen, sind das Antreten gegen andere Botnetz-Besitzer sowie die Sabotage von Sicherheitslösungen.

Die Methoden der Cyberkriminellen

Ganz allgemein müssen moderne Cyberkriminelle zwei Verfahren berücksichtigen, um das gewünschte Endergebnis zu erzielen – Übermittlung und Einsatz.

Andere verbreitete und effektive Methoden, mit denen moderne Cyberkriminelle ihre Gewinnmargen erhöhen, sind das Antreten gegen andere Botnetzbesitzer sowie die Sabotage von Sicherheitslösungen.

Eugene Kaspersky

Übermittlung

Der erste Schritt aller Cyberverbrechen besteht aus der Übermittlung und Installation der Malware. Cyberkriminelle verwenden verschiedene Methoden, um dieses Ziel zu erreichen. Zu den am weitesten verbreiteten Übermittlungstechniken (auch „Infektionsvektoren“ genannt) gehören Spam-E Mails und infizierte Websites.

Eine ideale Voraussetzung für Kriminelle sind schwach geschützte Computer, auf denen die Malware umgehend installiert werden kann – egal ob sie per Spam oder in einem so genannten Drive-by-Download übertragen wird. Bei so einem Drive-by-Download wird die Malware von einer Website heruntergeladen, die das Opfer beim Surfen aufgerufen hat, ohne zu ahnen, dass diese mit Malware infiziert ist.

Einsatz

Nachdem die Malware installiert worden ist, soll diese so lange wie möglich unerkannt bleiben. Die Autoren von Malware verwenden unterschiedliche Strategien, um die Lebensdauer der einzelnen Bestandteile zu erhöhen. Tarnung ist die wichtigste Strategie – sowohl für die Übermittlung als auch das Überleben der Malware auf dem infizierten Computer. Je weniger sichtbar Malware für Frühwarnsysteme von Antiviren-Programmen und Ermittlungsbehörden ist, desto länger kann die Malware dazu verwendet werden, auf infizierte Computer zuzugreifen und geheime Daten zu sammeln.

Zu den am meisten verbreiteten Tarnmethoden gehören Rootkit-Technologien, die Unterdrückung von Fehlermeldungen im System, die verdeckte Zunahmen der Dateigröße, verschiedene Packprogramme sowie die Unterdrückung der Warnmeldungen von Antiviren-Programmen. Autoren von Malware verwenden häufig auch unterschiedliche Verschleiervorgänge, damit Malware nicht erkannt wird. Polymorphie zum Beispiel ist eine Möglichkeit, die in den 90er Jahren weit verbreitet war, dann jedoch fast verschwunden ist.

Heute greifen Malware-Autoren wieder auf Polymorphie zurück. Dabei wird jedoch nur selten versucht, den Code auf den angegriffenen Computern zu verändern. Stattdessen gibt es einen auffälligen Trend hin zu serverseitiger Polymorphie – also die Rekompilierung von Code auf Webservern mit Leerbefehlen vom Typ „Nichts ausführen“, der sich im Laufe der Zeit ändert. So wird es deutlich schwieriger, neue Malware auf dem Server zu erkennen. Heutzutage gibt es Websites, bei denen Bots Malware alle fünf Minuten neu kompilieren.

Angriffe auf Sicherheits-Lösungen

Ein anderes verbreitetes Verfahren im Bereich Malware ist die Sabotage von Sicherheits-Programmen, damit die Malware nicht erkannt und deren Lebensdauer erhöht wird. Dabei werden Programm-Prozesse beendet, Dateien von Windows-Hosts geändert oder kompletter Code wird gelöscht, um eine Aktualisierung der Antiviren-Programme zu verhindern.

Außerdem entfernen viele Schadprogramme bereits installierten bössartigen Code anderer Autoren – allerdings nicht zum Vorteil des Benutzers, sondern um den

angegriffenen Computer selbst übernehmen und kontrollieren zu können. Der Wettbewerb zwischen bösartigen Programmen macht die vielfältigen Möglichkeiten deutlich, die Autoren von Malware sowie die für Malware zahlenden Kriminellen haben.

Häufig sorgt Malware für die Entfernung anderer zuvor installierter Schadprogramme, um den angegriffenen Computer selbst zu übernehmen und zu kontrollieren.

Eugene Kaspersky

Der menschliche Faktor

Letztendlich ist jedes Sicherheits-System nur so wirksam wie sein schwächstes Glied. In Bezug auf Online-Sicherheit ist das schwächste Glied der Mensch. Darum sind Techniken des Social Engineering heute Schlüsselemente bei der Verbreitung von Malware. Dazu gehören so einfache Methoden wie das Versen-

den von Links via E Mail oder Instant Messaging (IM), die angeblich von einem Freund stammen.

Diese Links sehen so aus, als ob sie zu interessanten Webseiten weiterleiten würden, doch in Wahrheit handelt es sich um Links, die zu infizierten Seiten führen. E Mail-Nachrichten können Skripte enthalten, auf deren Basis ohne jegliches Zutun des Benutzers eine Verbindung mit infizierten Websites hergestellt wird. Selbst gut informierte und vorsichtige Personen, die niemals auf nicht angeforderte Links klicken, können durch einen sogenannten Drive-by-Download infiziert werden. Häufig werden im Betreff von infizierten E-Mails aktuelle Ereignisse genannt – meist kurz nach dem eigentlichen Ereignis. Solche Kampagnen sind natürlich überaus effektiv.

Auch Phishing ist immer noch eine ernstzunehmende Gefahr, obwohl Banken und andere Unternehmen, die im Internet finanzielle Transaktionen ausführen, entsprechende Gegenmaßnahmen umgesetzt haben. Es gibt weiterhin zu viele unbedarfte Opfer, die sich überzeugen lassen, auf interessante Links zu klicken und offiziell aussehende E Mails als legitim zu akzeptieren.

Abschließende Betrachtungen

Um Cyberkriminalität wirksam bekämpfen zu können, müssen wir verschiedene Sicherheitsstrategien entwickeln und umsetzen. Selbstverständlich sind Security-Software und Strategien für das Risikomanagement auf allen Ebenen unverzichtbar.

Ich glaube nicht, dass wir Cyberkriminalität jemals vollständig unterbinden können – genauso wenig wie Kriminalität in der realen Welt... Mit einer starken Gemeinschaft können wir Cyberkriminelle jedoch in den meisten Fällen besiegen.

Eugene Kaspersky

Ich glaube jedoch, dass eine erfolgreiche Bekämpfung der Cyberkriminalität darüber hinaus einer gemeinschaftlichen Anstrengung bedarf. So muss eine funktionsfähige Internet-Interpol eingerichtet werden. Außerdem sind kontinuierliche Informationskampagnen für

Benutzer erforderlich – ähnlich der Kampagne zur Verwendung des Sicherheitsgurts im Auto. Gesetze sollten eingeführt werden, damit sich Menschen im Internet sicher und legal verhalten, und rechtliche Konsequenzen sollten die Durchsetzung dieser Gesetze unterstützen. Genauso wie beim Thema Sicherheitsgurt ist eine anhaltende Informationskampagne notwendig, um in der Bevölkerung das Bewusstsein für die Gefahren und eine breite Akzeptanz für diese Maßnahmen zu erreichen.

Ich glaube zwar nicht, dass wir Cyberkriminalität jemals vollkommen unterbinden können – genauso wenig wie Kriminalität in der realen Welt –, doch können wir das Internet in jedem Fall sicherer machen. Dazu werden allerdings mehr als die genannten Maßnahmen erforderlich sein, die von einzelnen Unternehmen oder Regierungen umgesetzt werden. Denn jeder muss seinen Teil zur Bekämpfung der Cyberkriminalität beitragen. Mit einer solchen gemeinschaftlichen Anstrengung können Cyberkriminelle in den meisten Fällen besiegt werden. Und das ist ein Ziel, für das es sich zu kämpfen lohnt.

Kaspersky Lab

Kaspersky Lab reagiert im weltweiten Vergleich von Antivirus-Herstellern meist am schnellsten auf IT-Sicherheitsbedrohungen wie Viren, Spyware, Crimeware, Hacker, Phishing-Attacken und Spam. Die Produkte des global agierenden Unternehmens mit Hauptsitz in Moskau haben sich sowohl bei Endkunden als auch bei KMUs, Großunternehmen und im mobilen Umfeld durch ihre erstklassigen Erkennungsraten und minimalen Reaktionszeiten einen Namen gemacht. Neben den Stand-Alone-Lösungen des Security-Experten ist Kaspersky-Technologie Bestandteil vieler Produkte und Dienstleistungen führender IT-Sicherheitsunternehmen. Mit den Kaspersky Hosted Security Services bietet das Unternehmen darüber hinaus Dienstleistungen im Bereich Malware- und Spam-Schutz sowie Content-Kontrolle für Unternehmen jeder Größe an.

Kontakt

Kaspersky Labs GmbH
Steinheilstr. 13
85053 Ingolstadt

Telefon: +49 (0)841 981 89 0
Telefax: +49 (0)841 981 89 100

info@kaspersky.de
www.kaspersky.de