



Interpol Generalsekretariat Lyon: Interpol-Experten arbeiten an Strategien gegen Computerkriminalität.

Interpol gegen Hightech-Crime

Computerkriminalität zählt zu den Formen moderner Kriminalität, die sich am raschesten entwickeln. Interpol-Experten arbeiten an Bekämpfungsstrategien mit den nationalen Polizeiorganisationen, der Wirtschaft und Wissenschaft.

Computerkriminalität wurde lange Zeit vor allem als Angriff von Hackern auf Rechner und Netzwerke gesehen, die immer raffinierte Varianten von Viren oder Trojanern verschickt hatten. Computer werden zunehmend für altbekannte Kriminalitätsformen benutzt. Pädophile benutzen Computer und das Internet, um Filme und Fotos mit kinderpornografischem Inhalt über das Netz zu beziehen oder zu vertreiben. Organisierte kriminelle Gruppen benutzen Computer und das Internet, um Personendaten zu stehlen – wie Bank- und Kreditkarteninformationen – und damit illegale Geschäfte in Milliardenhöhe zu machen.

Diese kriminellen Gruppen sind hierarchisch organisiert. Ähnlich frühe-

rer Mafiaorganisationen benutzen sie „Dienstgrade“. Verschiedene Schichten arbeiten anonym via Internet zusammen. Hoch qualifizierte Soft- und Hardwarespezialisten entwickeln die Methoden, um Identitäten auszuspiönieren. Beginnend mit „Keyloggern“, die jede Tastaturbewegung aufzeichnen und automatisch an einen Bestimmungsort schicken, bis hin zu erstklassigen Trojanern, mit denen riesige *BotNets* entstehen, können diese kriminellen Experten nahezu alles machen, was von ihrer Organisation verlangt wird.

BotNets sind momentan die größte Gefahr in den Netzwerken. Ungeschützte Computer werden mit einem Trojaner infiziert. Diese versteckte Software ermöglicht die Fernsteuerung des Computers mit herkömmlicher

Software, wie zum Beispiel ICQ. Mit diesem Computer kann nun alles gemacht werden. Er kann als Server zur Bereitstellung illegalen Materials verwendet werden, es können Daten von diesem Computer ausgelesen werden und für illegale Einkaufstouren verwendet werden, die Identität des Besitzers kann übernommen und verändert werden.

Auf diese Weise werden viele Tausende Computer befallen. In einem der größten Angriffe im Jahr 2006 wurden 1,5 Millionen Computer für illegale Aktivitäten gekapert. Dies ermöglichte „Denial-of-Service-Attacken“. Wenn beispielsweise 1,5 Millionen Computer gleichzeitig in Sekundenabständen E-Mails an eine E-Mail-Adresse verschicken, oder wenn dieselbe Zahl an Computern Webseiten angreift, ist es





Wer ohne Virenschutz im Internet surft, läuft Gefahr, dass Kriminelle mittels Trojaner persönliche Daten ausspähen.

leicht vorzustellen, wie schnell die Server ihren Dienst versagen. Der nächste Schritt ist eine kurze E-Mail, die gegen ein bestimmtes Entgelt verspricht, die Angriffe einzustellen. Da oft illegale Glückspielseiten angegriffen werden, ist die Gefahr nicht all zu hoch, dass die Polizei eingeschaltet wird.

Money Transfer Agents. Neben den technischen Experten existiert eine unabhängige zweite Kette, die sich um den finanziellen Teil kümmert. Die Kriminellen schicken illegal erlangtes Geld, das durch gestohlene Bank- oder Kreditkarteninformationen oder durch Schutzgelderpressungen erlangt wird, oder von anderen illegalen Geschäften herrührt, über „Money Transmitter“ wie „Western Union“ über das Internet

an einen bestimmten Adressaten. Die Beträge bleiben unter dem Limit, ab dem die Vorlage eines Identitätsdokuments nötig wäre. *Mules* oder *Money Transfer Agents*, oft Arbeitslose oder Studenten, die sich schnell etwas dazuverdienen möchten, werden angeheuert, um dieses Geld zu beheben und gleich wieder auf ein anderes Konto einzuzahlen oder über einen der oben beschriebenen Wege weiterzuschicken. Geldsummen werden kreuz und quer über den Globus verschickt – und das innerhalb von wenigen Minuten. In nahezu allen Fällen werden diese Summen über Länder verschickt, in denen keine rechtlichen Schritte gegen die *Money Transfer Agents* möglich sind.

Waren die organisierten Gruppen bis vor Kurzem auf Osteuropa beschränkt, finden sich nun ähnliche

Strukturen im Nahen Osten und in Nordafrika. Von diesen Gebieten aus werden Angriffe auf ungeschützte Ziele auf der ganzen Welt gefahren. Diese Angriffe erfolgen automatisch mit „Scanning-Systemen“ und sind, bedingt durch die Struktur des Internets, an keinerlei Grenzen oder Beschränkungen gebunden.

Eigene „Forschungsabteilungen“ entwickeln nahezu täglich neue, immer raffiniertere Anwendungen. Diese werden im Internet veröffentlicht und gegen geringes Entgelt kriminellen Gruppen zur Verfügung gestellt. So können *BotNets* mit einer definierten Anzahl von infizierten Computern auf bestimmte Zeit gemietet werden. Als zusätzlicher „Service“ werden die *BotNets* auf den Bedarf des Mieters hin zugeschnitten. Alternativ kann die Software gekauft und mit leicht zu bedienenden Benutzeroberflächen von Kriminellen an ihre Bedürfnisse angepasst werden.

Da diese Delikte nahezu immer grenzüberschreitend stattfinden, sind internationale Polizeiorganisationen wie Interpol gefordert, Gegenmaßnahmen zu installieren und die nationalen Polizeibehörden zu unterstützen.

Im Interpol Generalsekretariat in Lyon besteht die Abteilung „Financial and High Tech Crime“, in der Experten im Bereich Computerkriminalität, Finanzkriminalität und Geldwäsche zusammenarbeiten, um auf Polizeiseite diesen kriminellen Gruppen gegenüberzutreten zu können. Da alle Informationen bei grenzüberschreitender Kriminalität in einer Datenbank in Lyon zusammenlaufen, wird dort als Erstes bemerkt, wenn übereinstimmende Muster bei infizierten Computern oder bei Geldüberweisungen in verschiedenen Ländern auftreten. Diese Länder werden unverzüglich alarmiert und entsprechende Gegenmaßnahmen eingeleitet.

Experten aus den betroffenen Interpol-Mitgliedstaaten werden regelmäßig nach Lyon eingeladen, um abgestimmte Aktionen durchführen zu können. Die Erfolgsrate in der Bekämpfung steigt. Umfangreiche Polizeioperationen führten in den letzten Monaten zu zahlreichen Festnahmen in der ganzen Welt. In den Interpol-Mitgliedstaaten müssen die entsprechenden Polizeistrukturen geschaffen werden, um



Bernhard Otupal, Leiter der Abteilung „High Tech Crime“ bei Interpol.

diesen Machenschaften erfolgreich entgegenzutreten zu können. Gesetze müssen angepasst werden, nicht nur in der Computerkriminalität, auch in allen anderen betroffenen Bereichen, wie bei grenzüberschreitenden Geldüberweisungen. Im Bereich der Computerkriminalität ist die weltweite Anerkennung und Umsetzung der „Convention on Cybercrime“ der erste Schritt, der vom Europarat in Strassburg mit Unterstützung von Interpol vorangetrieben wird.

Meldesysteme. Im Bereich der Finanzkriminalität arbeitet Interpol derzeit an neuen Meldesystemen, die Daten von der Polizei, aber auch von nationalen und internationalen Finanzorganisationen auf verdächtige Transaktionen analysieren und entsprechende Alarmsysteme in Kraft setzen können.

Sind die rechtlichen Grundlagen und die Meldesysteme geschaffen, ist es auf Polizeiseite erforderlich, geschultes und ausgestattetes Personal bereitzustellen. In den meisten Industrieländern ist die nötige Infrastruktur bereits geschaffen, die nur mehr auf dem letzten technischen Stand gehalten werden muss. In Entwicklungsländern ist die Problematik viel größer. Während kriminelle Organisationen Infrastrukturen entwickeln können, steht der Polizei manchmal nicht einmal ein Telefonnetz zur Verfügung, schon gar nicht ausgebildete und ausgerüstete Experten zur Bekämpfung der Computerkriminalität.



Bundeskriminalamt: Die österreichischen Experten in den Arbeitsgruppen sind anerkannte Vertreter mit großem Einfluss auf die internationale Ermittlungsarbeit.

Handbuch. Interpol arbeitet seit einigen Jahren an einem Projekt „Training and Operational Standards Initiative“ (TOPSI), an der Entwicklung von standardisierten Ermittlungsmethoden und entsprechender Trainingsmodule. Diese werden vor allem in Europa entwickelt und allen Interpol Regionen zur Verfügung gestellt. Die Inhalte für diese Kurse werden hauptsächlich dem *Interpol IT Crime Manual* entnommen.

Das 2.000 Seiten starke Handbuch steht allen Mitgliedsstaaten zur Verfügung. In Zusammenarbeit mit der Industrie wird in diesem Projekt versucht, Staaten, die finanzielle Unterstützung benötigen, zu helfen, ihre Polizei auf einen Mindeststandard zu bringen. Die Einbindung von akademischen Organisationen soll eine Betriebsblindheit verhindern und hochwertige Qualität sicherstellen.

Ein wichtiger Bereich ist die Öffentlichkeitsarbeit. Jeder Computernutzer sollte über die Gefahren informiert sein, die die Nutzung des Internets mit ungeschützten Computern mit sich bringt. Auch hier versucht Interpol mit der Privatwirtschaft und regionalen Internet-Organisationen wie der Euro-ISPAs Bewusstseinsbildungs-Veranstaltungen abzuhalten.

Das Büro 5.2 (Computer- und Netzwerkkriminalität) des Bundeskriminalamts in Österreich hat schon sehr früh den Kampf gegen diese neue Kriminalität begonnen. Es gab eine gemeinsa-

me Aus- und Fortbildung mit den entsprechenden Stellen in den Bundesländern. Mitarbeiter des Büros 5.2 nahmen an internationalen Workshops teil, um auf dem neuesten Stand der Polizeitechnik zu bleiben.

Die österreichischen Experten in den internationalen Arbeitsgruppen sind anerkannte Vertreter mit großem Einfluss auf die internationale Ermittlungsarbeit. Das Büro 5.2 ist Gründungsmitglied eines schnell operierenden internationalen Netzwerks, das die Geschwindigkeit der Polizeiarbeit im Bereich Computerkriminalität der technischen Entwicklung angleichen soll. In der forensischen Beweismittelsicherung hat diese Abteilung einen international exzellenten Ruf.

Der Kampf gegen die organisierte Kriminalität, die moderne Technologien missbraucht um ihre Machenschaften umzusetzen, ist schwer. Dieser Entwicklung kann ein Riegel vorgeschoben werden durch enge Zusammenarbeit der verschiedenen Abteilungen innerhalb der Polizeiorganisationen, durch rasche Kommunikation und Kooperation zwischen nationalen Polizeiorganisationen, gemeinsam mit der Privatwirtschaft und Universitäten.

Moderne Ausrüstung und ständige Aus- und Fortbildung der Polizei auf allen Ebenen im Zusammenspiel mit internationaler Gesetzgebung wird die Ermittlungsarbeit erleichtern und beschleunigen.

Bernhard Otupal