

Zur Information – kein offizielles Dokument

VERBRECHENSBEKÄMPFUNG IM INTERNET

In den letzten Jahren ist das Internet explosionsartig gewachsen. Im Vergleich zu 26 Millionen Nutzern 1995, nutzen heute über 200 Millionen Menschen das Internet, um zu kommunizieren, einzukaufen, Rechnungen zu bezahlen, Geschäfte zu machen oder sogar um ärztlichen Rat einzuholen.

So wie das Internet hat sich aber auch dessen Missbrauch ausgeweitet. Sogenannte Cyber-Kriminelle schwirren grösstenteils nach Belieben durch die virtuelle Welt und begehen Delikte wie unerlaubten Datenzugriff oder "Hacking", Betrug, Computersabotage, Drogenhandel, Handel mit Kinderpornographie und Cyber-Belästigung.

Computer-Kriminelle sind so unterschiedlich wie die Delikte, die sie begehen. Sie können Studenten, Terroristen oder Mitglieder des organisierten Verbrechens sein. Wirtschaftskriminalität, wie Betrug oder Informationsdiebstahl, wird laut dem UNO-Bericht zur Verhütung und Kontrolle computerbezogener Kriminalität (1997) zu über 90 Prozent durch die jeweils eigenen Angestellten begangen.

Cyber-Kriminelle können unentdeckt über internationale Grenzen flitzen, sich hinter zahllosen "links" verstecken oder einfach verschwinden, ohne greifbare Spuren zu hinterlassen. Sie können ihre Übertragungen und kriminelles Beweismaterial in Zufluchtsorten sichern in Ländern, die die Gesetze oder die Fähigkeit nicht haben, solche Vorgänge zu verhindern.

In der Bemühung diese wachsende Bedrohung einzudämmen, wird auf dem zehnten Kongress der Vereinten Nationen für Verbrechenverhütung und die Behandlung Straffälliger, vom 10. bis 17. April in Wien, ein spezieller Workshop abgehalten. Der Workshop, der von dem in Tokio ansässigen Institut für Verbrechenverhütung und die Behandlung Straffälliger (UN Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders, UNAFEI) unter Schirmherrschaft des Zentrums für internationale Verbrechenverhütung (Centre for International Crime Prevention, CICIP) organisiert wird, wird sich auf die weltweite Ko-operation zur Untersuchung und Verfolgung von Computerkriminalität konzentrieren.

"Dieser Workshop soll als Forum zum Informationsaustausch über Dinge wie Ermittlungstechniken und Computerkriminalitätsgesetze zwischen Ländern mit einem breiten Band an Erfahrungen, Sachkenntnis und Problemnäherung dienen", sagte Christopher Ram, CICIP-Verantwortlicher für Computerkriminalität.

Hacken, Sabotage und Belästigung

Verbotenes "Hacken" mit Hilfe ausgeklügelter Techniken zum Kopieren von Kennwörtern oder das Umgehen anderer Sicherheitsmassnahmen ist ein beliebtes Cyber-Delikt geworden. Sobald Hacker Zugang zu Daten haben, können sie Viren einschleusen, beleidigende Nachrichten versenden oder wertvolle Informationen stehlen, einschliesslich Kreditkarteninformationen und Betriebsgeheimnissen.

Konsumenten verlieren nach jüngsten Schätzungen rund 520 Millionen pro Jahr an Hacker, die Kreditkarteninformationen stehlen und Informationen von Online-Konten einholen. Diese Informationen können zu ansehnlichen Beträgen an Betrüger verkauft werden, die spezielle Programme benutzen, um diese Daten auf Kredit- und Bankomatkarten-Magnetstreifen zu codieren, warnt der Bericht der Vereinten Nationen.

Andere Cyber-Kriminelle sabotieren Computer, um wirtschaftliche Vorteile gegenüber Konkurrenten zu gewinnen, oder sie drohen, Systeme zu zerstören, um ihre Opfer erpressen zu können. Die Täter manipulieren Daten direkt oder benutzen sogenannte "Würmer" und "Viren", die Systeme komplett zum Stillstand bringen oder Daten von Festplatten löschen können. Zufällig verbreitete Computerviren, die ursprünglich über "infizierte" Disketten von einem Computer zum nächsten weitergegeben wurden, werden heute auch über Netzwerke weitergegeben, oft verborgen in E-mails oder aus dem Internet heruntergeladenen Programmen.

Europa wurde erstmals 1990 mit einem Computervirus erpresst. Die medizinische Forschungsgemeinschaft wurde mit einem Virus bedroht, der wachsende Mengen an Daten zerstören würde, wenn kein Lösegeld für die "Heilung" bezahlt würde.

E-mails werden auch zur Belästigung anderer benutzt. Leute versenden Drohbotschaften, vor allem an Frauen. Schätzungen deuten darauf hin, dass rund 200.000 Personen pro Jahr andere mit E-mails belästigen, berichtet das Buch `Cyber-stalking: Crime, Enforcement and Personal Responsibility in the online World' von Barbara Jenson aus dem Jahr 1996.

Eine nordamerikanische Frau wurde laut Frau Jenson mehrere Jahre lang via E-mail von einer unbekanntenen Person belästigt, die ihr androhte sie zu töten, ihre Tochter zu vergewaltigen und ihre Wohnadresse anderen über das Internet bekanntzugeben.

Täter haben auch E-mails und Internet-`Chatrooms' dazu genutzt, um Opfer aufzuspüren. So haben zum Beispiel Pädophile online das Vertrauen von Kindern gewonnen und anschliessend `wirkliche' Treffen, mit dem Ziel sie zu entführen oder zu missbrauchen, vereinbart.

Zusätzlich zu Übergriffen auf private Internetseiten können Kriminelle ihre eigenen Seiten einrichten, um Internetbenutzer zu betrügen oder verbotene Güter und Dienstleistungen zu verkaufen, wie zum Beispiel Waffen, Drogen, ungeprüfte rezeptpflichtige Medikamente und Pornographie.

`CyberCop Holding Cell', ein online-Beschwerdedienst, hat vor kurzem vor einem Auto-Markt im Internet gewarnt. Für eine Gebühr von i 400 würde man eine Beschreibung des Autos des Kunden im Internet anführen und, sollte das Auto nicht innerhalb von 90 Tagen verkauft sein, das Geld zurückgeben.

Die Fahrzeuge vieler Kunden, die auf der Web-Seite angeboten wurden, wurden nicht in diesem Zeitraum verkauft, doch die Kunden konnten niemanden finden, der ihnen das Geld zurückerstattet hätte, berichtete CyberCop. Die Internetseite ist seitdem aufgelöst worden.

Cyber-Kriminelle aufgreifen

Da die Cyber-Kriminalität angestiegen ist, haben viele Staaten Gesetze verabschiedet, die die neuen Phänomene, wie zum Beispiel Hacken, unter Strafe stellen. Zusätzlich wurden alte Gesetze verbessert, um traditionelle Vergehen wie Erpressung, Vandalismus oder Sabotage auch in der virtuellen

Welt illegal zu machen.

Singapur, zum Beispiel, hat laut CNET vor kurzem seine `Akte für Computer-Missbrauch' verbessert. Härtere Strafen gelten jetzt für jeden, der sich in `geschützte Computer' B die sowohl mit nationaler Sicherheit, Banken und Finanz als auch mit Not-

Netzwerk-Schandtaten

Industriespionage

Hacker können alleine ausgeklügelte Spionage für Organisationen durchführen, indem sie von technischen Firmengeheimnissen oder Produktinformationen bis hin zu Marketingstrategien illegal kopieren.

Systemsabotage

Attacken wie `Mail Bombardements' können wiederholt Nachrichten an eine E-mail-Adresse oder Web-Seite schicken und damit den legitimen Benutzern den Zugang verwehren. Der Mail-Zustrom kann das Datenverarbeitungspotential des Empfängers überfordern und damit ganze Systeme zum Stillstand bringen. Obwohl es sich um eine äusserst zerstörerische Praxis handelt, ist sie nicht unbedingt illegal.

Datensabotage und Bvandalismus

Eindringlinge können sich Zugang zu Internet-seiten oder Datenbanken verschaffen und Daten löschen oder verändern, womit sie die Daten selbst beschädigen und weiteren Schaden anrichten, wenn unkorrekte Daten später für andere Zwecke verwendet werden.

diensten und dem öffentlichen Dienst verbunden sind B einschleicht, sowie für unerlaubten Zutritt zu und Veränderung, Benutzung oder Abfangen von Computer-Material.

Einige Staaten haben spezialisierte Gruppen zur Verfolgung von Cyber-Kriminellen. Eine der ältesten ist das 1978 gegründete U.S. Air Force Office of Special Investigations. Eine andere sind die `Australian Internet Investigators', bestehend aus Mitgliedern der Exekutive und Einzelpersonen mit fortgeschrittenen Computerkenntnissen. Die australische Gruppe sammelt Beweise und reicht diese an die geeigneten Vollzugsbehörden im Ursprungsland der kriminellen Handlung weiter.

ˆ KennwortklauA, ˆ DatenschnüfflerA

Täter legen oft neue und unerfahrene Internet-Benutzer herein und bringen sie zur Bekanntgabe ihrer Kennwörter, indem sie vortäuschen, Exekutivbeamte oder Beauftragte des Providers zu sein. ˆ DatenschnüfflerA benutzen Software, um das Kennwort eines Benutzers herauszufinden, was sie dazu verwenden können, um ihre wahre Identität zu verbergen und Verbrechen zu begehen B vom unautorisierten Gebrauch von Computersystemen bis hin zu Wirtschaftskriminalität, Vandalismus oder terroristischen Akten.

ˆ SpoofingA

ˆ SpooferA (engl. Nachahmer) verwenden verschiedene Techniken, um einen Computer so zu verkleidenA, dass er elektronisch wie ein anderer aussiehtA, um Zugang zu einem normalerweise geschützten System zu gewinnen und Verbrechen zu begehen. Der berühmte Hacker Kevin Micknick benutzte diese Technik 1996, um auf den Home Computer des Sicherheitsexperten Tsutomu Shimomura zuzugreifen und dann wertvolle Sicherheitsinstrumente über das Internet zu verteilen.

Kinderpornographie

Kinderpornographie, die über das Internet rund um die Welt gesandt wird, nimmt zu. In den letzten fünf Jahren sind in einem nordamerikanischen Land die Verurteilungen für die Verbreitung oder den Besitz von Kinderpornographie von 100 auf 400 pro Jahr angestiegen. Neue Technologien, wie Kryptographie, die dazu genutzt werden kann, Pornographie oder anderes ˆ anstößigesA Material zu verstecken, verstärken das Problem.

Glücksspiel

Elektronisches Glücksspiel hat zugenommen, da der Handel die Aufnahme von Krediten und den Transfer von Geldern über das Internet ermöglicht. Probleme sind in Ländern entstanden, wo Glücksspiel verboten ist, oder wo staatliche Behörden Lizenzen verlangen. Ausserdem kann keine Fairness gegenüber den Spielern garantiert werden, wenn man die technische und juristische Beobachtung in Betracht zieht

Trotz dieser und anderer Anstrengungen stehen mit dem Gesetzesvollzug betraute Personen weiterhin vor verschiedensten ˆ Cyber-ProblemenA. Zentral dabei ist, dass diese Vergehen leicht staatliche Grenzen überschreiten können, wodurch die Ausforschung, Verfolgung und Bestrafung der Täter den Gesetzgebern und Juristen Kopfschmerzen bereitet. Wenn die Täter einmal gefunden sind, müssen die Beamten entscheiden, ob sie diese für ein Verfahren

ausliefern und Beweise B und manchmal auch Zeugen B dorthin, wo die Verbrechen begangen wurden, überbringen.

1992 haben Hacker aus einem europäischen Land ein Computerzentrum in Kalifornien attackiert. Die polizeiliche Untersuchung wurde durch das Fehlen einer ˆ zweifachen KriminalitätA B d.h. ähnlichen Gesetzen in den zwei Staaten, die das Verhalten verbieten würden B durchkreuzt, und dadurch wurde die offizielle Kooperation nach Angaben des amerikanischen Justizministeriums blockiert.

Schlussendlich bot die Polizei aus dem Herkunftsland

Betrug

Betrügerische Angebote wurden bereits an Konsumenten im Bereich des elektronischen Handels, wie zum Beispiel Aktienhandel oder Kauf und Verkauf von Computersystemen, gemacht.

Geldwäsche

Der elektronische Handel kann B so nimmt man an B einen neuen Weg für den Transfer von Waren oder Geld bieten, um kriminelle Einkünfte reinzuwaschen, besonders wenn Transaktionen verdeckt werden können.

der Hacker ihre Hilfe an, aber kurz danach hatte das Hacken ein Ende, die Spur wurde kalt und der Fall geschlossen.

In einem ähnlichen Fall sind das U.S. Naval Criminal Investigative Service und das FBI 1996 einem anderen Hacker aus einem südamerikanischen Land auf die Spur gekommen. Der Täter stahl Kennwortinformationen und änderte Zugangsdateien in Militär-, Universitäts- und privaten Computersystemen. Viele davon enthielten sensible Forschungsergebnisse von Satelliten, über Strahlung und energiebezogenen Technologien.

Exekutivbeamte aus dem südamerikanischen Land durchsuchten die Wohnung des Hackers und beschlagnahmten seine Computerausrüstung unter Anführung möglicher Gesetzesverletzungen dieses Landes. Aber im Gegensatz zu Auslieferungsabkommen für traditionellere Verbrechen, hatten die zwei Staaten kein Abkommen für Computer--kriminalität. Schlussendlich wurde der Fall nur deshalb gelöst, weil der Hacker einem Vergleich zustimmte, der ihn dazu veranlasste, sich in den Vereinigten Staaten für schuldig zu erklären.

Vernichten und Verstecken von Beweisen

Ein weiteres Haupthindernis bei der Verfolgung von Cyber-Kriminalität ist, dass Täter leicht Beweise vernichten können, indem sie Daten verändern, löschen oder verschieben. Wenn die Exekutive sich langsamer bewegt als die Täter es tun, gehen viele Beweise verloren. Oder Daten werden verschlüsselt. Ein zunehmend populärer Weg Einzelpersonen und Unternehmen in Computernetzwerken zu schützen.

Verschlüsselung kann kriminalistische Untersuchungen behindern, aber andererseits sind Menschenrechte in Gefahr, wenn die Exekutive zu viel technische Macht erringt. Elektronische Unternehmen argumentieren, dass Privatsphäre entscheidend ist, um das Kundenvertrauen in den Marktplatz Internet zu stärken, und Menschenrechtsgruppen wollen Schutz für die Unzahl an persönlichen Daten, die heute elektronisch gesammelt werden.

Unternehmen betonen auch, dass Informationen in die falschen Hände kommen können, besonders in korrupten Ländern, wenn Regierungen Zugang zu verschlüsselten Daten haben. Wenn Regierungen den Schlüssel zu verschlüsselten Nachrichten haben, bedeutet das, dass unautorisierte Personen außerhalb der Regierung sie erwerben und benutzen könnten, sagte der Generaldirektor einer führenden nordamerikanischen Sicherheitstechnologiefirma.

Erfassung globaler Kriminalität

Die Herausforderungen, denen der Gesetzesvollzug weltweit gegenübersteht, verweisen auf den dringenden Bedarf nach einer globalen Kooperation bei der Aktualisierung von nationalen Gesetzen, Untersuchungstechniken, juristischer Unterstützung und Auslieferung, um mit den Cyber-Kriminellen Schritt zu halten. Einige Anstrengungen wurden bereits unternommen.

Der UNO-Bericht von 1997 fordert die Staaten dazu auf, Gesetze zu harmonisieren und bei der Bekämpfung des Problems zu kooperieren. Die

Europäische Arbeitsorganisation für Verbrechen innerhalb der Informationstechnologie (European Working Party on Information Technology Crime, EWPITC) hat ein Computerkriminalitäts-Handbuch herausgegeben, das relevante Gesetze in verschiedenen Staaten auflistet und Untersuchungstechniken beschreibt, ebenso wie Wege der Suche und Sicherung von elektronischen Materialien.

Das Europäische Institut für Anti-Virus-Forschung (EICAR) kooperiert mit Universitäten, Industrie und Medien sowie technischen Sicherheits- und Rechtsexperten aus Regierung, Exekutive und Datenschutzorganisationen, um Computerviren oder sogenannte "Trojanische Pferde" zu bekämpfen. Es arbeitet auch an der Bekämpfung von Computerbetrug und die Ausnutzung persönlicher Daten.

1997 haben die G-8-Staaten eine bahnbrechende Strategie zur Bekämpfung von "high tech"-Kriminalität aufgenommen. Die Gruppe vereinbarte die Entwicklung von Wegen der schnellen Verfolgung von Computerattacken und der Identifizierung von Hackern, der Benutzung von Videoverbindungen, um Zeugen jenseits der Grenzen zu vernehmen, und der gegenseitigen Unterstützung bei Ausbildung und Ausrüstung. Sie vereinbarte ausserdem gemeinsam mit der Industrie, die Kräfte zu vereinen, um Instanzen zur Sicherung von Computertechnologien einzurichten, Informationssysteme zur Feststellung von Netzwerkmissbrauch zu entwickeln, Täter zu verfolgen und Beweise zu sammeln.

Die G-8 hat nun Kontaktpunkte eingerichtet, die der Exekutive 24 Stunden täglich zur Verfügung stehen. Diese Punkte verbessern die Untersuchungen eines Staates, indem sie notwendige Informationen zur Verfügung stellen oder in juristischen Fragen helfen, wie zum Beispiel der Vernehmung von Zeugen oder der Sammlung von Computerdaten als Beweismittel.

Ein wesentliches Hindernis bei der Aufnahme einer G-8-ähnlichen Strategie auf internationaler Ebene ist, dass manchen Staaten die technische Sachkenntnis oder Gesetzgebung fehlt, die es der Exekutive ermöglichen würde, schnell Beweise an elektronischen Schauplätzen zu suchen bevor sie verloren gehen oder sie an einen Ort zu bringen, wo gegen die Täter vorgegangen wird.

**Zwecks weiterer Auskünfte
kontaktieren Sie bitte:**

Sandro Tucci
Sprecher des Exekutivdirektors
Büro für Drogenkontrolle und
Verbrechensverhütung
Tel: (43-1) 26060-5629
Fax: (43-1) 26060-5875
E-mail: sandro.tucci@undcp.org
Web-Seite: <http://www.odccp.org>

Für deutschsprachige Auskünfte:

Peter Vanoverveld
Verantwortlicher für deutschsprachige Presse
Informationsdienst der Vereinten Nationen Wien
Tel: (43-1) 26060-3713
Fax: (43-1) 26060-5899
E-mail: peter.vanoverveld@unis.un.or.at
Web-Seite:
http://www.unis.unvienna.org/german/german_page.htm
