Deutscher Präventionstag –
der Jahreskongress seit 1995

Cyberkriminalität - die Schattenseite der digitalen Gesellschaft

von

Jörg Ziercke

Dokument aus der Internetdokumentation
des Deutschen Präventionstages www.praeventionstag.de
Herausgegeben von Hans-Jürgen Kerner und Erich Marks im Auftrag der
Deutschen Stiftung für Verbrechensverhütung und Straffälligenhilfe (DVS)

Zur Zitation:
Jörg Ziercke: Cyberkriminalität - die Schattenseite der digitalen Gesellschaft, in: Kerner, Hans-Jürgen u. Marks, Erich (Hrsg.), Internetdokumentation des Deutschen Präventionstages. Hannover 2014, www.praeventionstag.de/Dokumentation.cms/2831

DEUTSCHER PRÄVENTIONSTAG 2014

12. Mai 2014

Sonderveranstaltung Karlsruher Forum für Cybersicherheit

Cyberkriminalität – Die Schattenseite der digitalen Gesellschaft

JÖRG ZIERCKE

GLIEDERUNG:

1. BEGRÜSSUNG / EINLEITUNG

Sehr geehrte Damen und Herren,

vielen Dank für die Gelegenheit diese Sonderveranstaltung zum Thema Cybersicherheit im Rahmen des diesjährigen Deutschen Präventionstages eröffnen zu dürfen.

Zunächst eine Vorbemerkung: Zu den Zielen meines Vortrages!

1. Berichte über Cybercrime haben das Ziel der Aufklärung, nicht der Verteufelung.
2. Das Wissen über Cybercrime soll die User sensibilisieren, schützen.
3. Das Vertrauen in das Internet soll gestärkt werden.

Es geht für mich heute nicht um rechtspolitische Aspekte, die sich beispielsweise aus Kryptierung oder Anonymisierung ergeben, sondern um Prävention.

Das Internet durchdringt heute nahezu alle Lebensbereiche, für viele ist es längst zum integralen Bestandteil ihres Lebens geworden. „Always on“ ist das Schlagwort. Begriffe wie „Smart-Home“, “Internet der Dinge“ oder „Industrie 4.0“ sind Synonyme dafür, dass moderne IT, Datenverarbeitung und das Internet in Zukunft noch umfassender Einzug in unser tägliches Leben und in viele Bereiche der Wirtschaft halten werden.

Während ich diese kurzen einleitenden Worte gesprochen habe, wurden weltweit[1]

- auf Youtube rund 1,3 Mio. Videos angesehen,
- mehr als 2 Mio. Anfragen an Google gestellt,
- 6 Mio. Facebook-Einträge angesehen,
- 100.000 twitter-Nachrichten[2] und über 200 Mio. e-Mails wurden versendet, mehr als 90% davon waren allerdings SPAM-Mails.

Wo viel Licht ist, ist eben auch Schatten! Damit Sie sich vor Cyberkriminellen besser schützen können, sollten Sie etwas wissen über die Phänomene von Cybercrime!

---

[1] Bezieht sich auf eine Minute.

[2] andere Quellen sprechen von rund 300.000 Tweets

Cybercrime ist eine neue Dimension der Kriminalität. Sie verändert sich täglich. Den Tätern bieten sich unzählige potenzielle Opfer und Angriffspunkte weltweit. Das Gefahrenpotential für den einzelnen Bürger, für Wirtschafts- und Finanzunternehmen, für den Staat und seine Einrichtungen ist erheblich und allgegenwärtig, das Entdeckungsrisiko für die Täter im Vergleich zur analogen Welt hingegen gering. Cybercrime hat grenzloses Wachstums- und Schadenspotenzial. Das Internet hat die nationalen Grenzen aufgehoben. Kriminalgeographische Räume existieren in der Cyberwelt nicht. Terrorismus und Organisierte Kriminalität sind entgrenzt worden und wachsen zunehmend.

Fest steht: Internet und moderne Kommunikationsmittel haben unser Kommunikationsverhalten und unser soziales Leben maßgeblich beeinflusst. Zum einen haben sie Einzug in klassische Kriminalitätsformen gehalten, vor allem im Bereich Betrug, zum anderen beobachten wir neue Phänomenausprägungen, Kriminalität wie sie ohne die Nutzung moderner Informations- und Kommunikationstechnik nicht möglich wäre. Die Täter bedienen sich mittlerweile in nahezu allen Kriminalitätsbereichen modernster Technik und nutzen das Internet als Tatmittel. Menschen weltweit werden Opfer von Betrug, Erpressung, Eigentumsdelikten, Phishing, Diebstahl ihrer digitalen Identität, Scareware, Ransomware, Cybergrooming und –mobbing, lassen sich radikalisieren und rekrutieren, fallen auf die kriminellen Betrugsmaschen angeblicher Onlineshops, Fake Shops oder auch Callcenter herein, werden unwissend Teil eines Botnetzes, dem Tatmittel moderner Kriminalität.
Nicht nur Bürgerinnen und Bürger werden Opfer von Cybercrime. Auch Unternehmen befinden sich im Zielspektrum krimineller Aktivitäten.

Es geht darum Daten abzugreifen, die digitale Identität des anderen für eigene kriminelle Zwecke zu nutzen, fremdes Know-How und geschützte Informationen zu erlangen.

Es geht auch um Angriffe auf Kritische Infrastrukturen, auf Staaten oder auf Unternehmen.

Um den Cyber-Bedrohungen effektiv zu begegnen, müssen alle User, insbesondere jedoch auch Unternehmen, sich aktiv mit dem Thema Cybersicherheit befassen. Nach Angaben der Sicherheitsstudie von Corporate Trust „Industriespionage 2012“ verfügen weniger als die Hälfte der befragten Unternehmen über ein

Sicherheitsmanagement mit klaren Regeln für den Informationsschutz. Und nur jedes fünfte Unternehmen hat sein schützenswertes Know-How überhaupt definiert. Studien belegen darüber hinaus immer wieder die mangelnde Bereitschaft der Unternehmen Angriffe anzuzeigen. Befragungen von IHK`n haben ergeben, dass nur 20% der Unternehmen in Deutschland erfolgte Cyber-Angriffe zur Anzeige gebracht haben! Das heißt, dass das Dunkelfeld mindestens 5x höher ist, wie die offiziell registrierten Zahlen!

Warum wurde keine Anzeige erstattet?

- Der Aufwand einer Anzeige sei zu hoch,
- der Ermittlungserfolg der Behörden demgegenüber zu unwahrscheinlich,
- oder richtige Ansprechpartner auf Seiten der Behörden nicht bekannt.

Es kommt noch ein Grund hinzu: der befürchtete Reputationsverlust. Doch: Solange die Wirtschaft die Bedrohung nicht erkennt oder erkannte Angriffe verschweigt, können die zuständigen Behörden nicht tätig werden und kein umfassendes Bild der Bedrohung zeichnen. Opfer, die Straftaten aus den unterschiedlichsten Gründen nicht anzeigen gab es schon immer. Viele Opfer sind sich der Viktimisierung nicht bewusst, viele Straftaten werden gar nicht bemerkt!

Besonders deutlich wird dies am Beispiel des Datendiebstahls: Der Diebstahl 2.0 ist das Kopieren, d.h. das entwendete Gut verlässt seinen Speicherort zu keinem Zeitpunkt! Der „Verlust“ wird häufig erst erkannt, wenn der Schaden, z.B. als Urheberrechtsverletzung oder als Produktpiraterie eingetreten ist.

2. AKTUELLE ERSCHEINUNGSFORMEN DER CYBERCRIME

Ein kurzer Blick auf aktuelle Erscheinungsformen des Phänomens Cybercrime:

2.1 Phishing

Eine der bekanntesten Varianten von Cybercrime ist sicherlich Phishing im Zusammenhang mit Onlinebanking. Die registrierten Fallzahlen sind rückläufig, liegen aber zwischen 3.000 und 4.000.

2012 waren die Fallzahlen in diesem Bereich in Deutschland deutlich rückläufig, nämlich um 46 % auf rund 3.400
(3.440; 2011: 6422). Die Dunkelziffer ist nicht bekannt. Die durchschnittliche Schadenssumme betrug dabei rund 4.000 € pro Fall. Eine Erklärung hierfür dürfte —

neben einer gewachsenen Sensibilität der Anwender — sein, dass 2012 viele deutsche Banken ihre Sicherheitssysteme weiter verstärkt haben, insbesondere durch Einführung des sog. mobile-TAN (mTAN) Verfahrens. Beim mTAN-Verfahren wird die für die Autorisierung einer Onlinetransaktion erforderliche Transaktionsnummer auf das Mobiltelefon des Bankkunden übermittelt. Der Sicherheitsgewinn resultiert aus der Einführung dieses zweiten, unabhängigen Kommunikationskanals. Eine vergleichbare Entwicklung der einschlägigen Fallzahlen haben wir schon im Jahr 2008 beobachtet, nachdem die deutschen Banken flächendeckend das sog. iTAN-Verfahren eingeführt hatten. Bereits im darauffolgenden Jahr stiegen die Fallzahlen aber wieder an und hatten im Jahr 2010 den bisherigen Höchststand des Jahres 2007 deutlich überschritten. Es bleibt abzuwarten, wie lange die neuen Sicherungssysteme ein Hindernis für Kriminelle sein werden.

Wie die Sicherheitsvorkehrungen entwickeln sich auch die Methoden der Phisher stetig weiter. Das Vorgehen der Täter aus den Anfangszeiten, als sie breit gestreut und ungezielt E-Mails versandten, in denen die Empfänger zur Preisgabe ihrer Onlinebanking-Zugangsdaten aufgefordert wurden, ist mittlerweile kaum noch zu beobachten.
Fast ausnahmslos kommt Schadsoftware zum Einsatz. Die Anzahl neuer Malware steigt sehr stark an. Alle ein bis zwei Sekunden entsteht weltweit ein neues Schadprogramm. Diese werden – zur Umgehung der Funktionalitäten von Virenschutz-Programmen – meist nur wenige Tage verwendet, bevor sie durch neue Varianten ersetzt werden.

Aktuell bevorzugen Phisher folgende Varianten zur Verbreitung ihrer Schadsoftware:

1. „Drive-by-Infection“

   Unerwünschtes Herunterladen der Schadsoftware allein durch Aufruf einer von der Täterseite präparierten Webseite.

2. Verteilung der Schadsoftware über Soziale Netzwerke[3], in denen das spätere Opfer dem Täter vertraut und dann gutgläubig infizierte Anhänge öffnet bzw. entsprechenden Links folgt.

3 z. B. Facebook, Studi-VZ, Wer-Kennt-Wen

3. „Spear-Infection“
   Gezielte Kontaktaufnahme zu bestimmten Personen mittels persönlich adressierter Phishing- oder Infektionsmails, um auf diesem Wege in den Besitz der zur Durchführung weiterer Aktionen erforderlichen Daten zu gelangen bzw. den Rechner zu infizieren.
   Ein Grund für die Nutzung dieses Modus Operandi besteht darin, dass viele Internetnutzer bei ungewollt erhaltenen anonymen E-Mails zunehmend skeptisch reagieren und vorsichtiger geworden sind, jedoch bei persönlich an sie adressierten E-Mails weniger sensibel reagieren.

Mittlerweile werden 2/3 der Schadcodes mittels Drive-by-Infection verteilt. Nach Angaben der Branche[4] werden weltweit pro Tag 13.000 infizierte Websites ins Netz gestellt.[5] Zudem versuchen Hacker gezielt, Webseiten mit hohen Besucherzahlen zu manipulieren, um dadurch eine schnellere und deutlich umfassendere Verteilung der Schadsoftware zu erreichen. Auf diese Weise können die Täter z. B. Trojaner verteilen, die in der Lage sind, sich in die Abwicklung von Online-Banktransaktionen „zwischenzuschalten“ und Überweisungsdaten zu verändern.

Trotz zuletzt gesunkener Fallzahlen bleibt das Onlinebanking eines der Hauptangriffsziele. Die Täterseite hat auch bereits auf die Einführung des mTAN-Verfahrens reagiert und verzeichnet erste Erfolge.

Sie verfahren dabei wie folgt:

1. Täter spähen mittels „klassischem Phishing“ Zugangsdaten für Onlinebanking aus.
2. Dann richten sie ohne Wissen des Bankkunden das mTAN-Verfahren ein; für den Empfang der mTAN wird eine Mobilnummer der Täter hinterlegt.
3. Der von der Bank per Post zugestellte Aktivierungscode wird von den Tätern abgefangen.
4. Damit sind die Täter in der Lage, Überweisungen vom Konto des Bankkunden zu initiieren.

---

4 IT-Dienstleister Symantec

5 dpa-Meldung vom 02.03.2010

Doch auch diese Masche gehört schon wieder der Vergangenheit an. Mittlerweile beobachten wir ein technisch anspruchsvolleres Angriffsszenario, bei dem das mTAN-Verfahren auf Smartphones mit dem Betriebssystem Android mittels einer Schadsoftware attackiert wird.
Damit wird die Infektion eines PC überflüssig. Die Täter reagieren damit nicht nur auf die mittlerweile fast flächendeckende Einführung des mTAN-Verfahrens durch deutsche Banken, sondern auch auf die zunehmende Nutzung von Smartphones und Tablet-Computern für das Onlinebanking.

Diese Entwicklung zeigt, dass die Täter stetig bemüht sind, sich dem Markt der Sicherheitsanwendungen anzupassen. Wie marktorientiert die Täter arbeiten, zeigt auch die Tatsache, dass Geräte mit dem Betriebssystem Android angegriffen werden. Im Bereich der mobilen Endgeräte hat Android weltweit mit einem Marktanteil von 75 % eine dominierende Position.

- Allein die Plattform „Google Play Store“ bietet fast 1 Mio. Apps für dieses Betriebssystem, Angebote von Drittanbietern kommen noch hinzu. Die Gefahr, auf ein „schwarzes Schaf“ und u. U. Schadsoftware zu stoßen, ist sehr groß.
- Anfang dieses Jahres waren fast 700.000 auf Android-Geräte abzielende Schadsoftwarevarianten bekannt.

Viele Android-Geräte verwenden noch ältere Versionen dieses Betriebssystems. Zumeist bestehen keine Support-Verträge und somit keine Verpflichtungen zur Bereitstellung von Updates durch die Gerätehersteller.
Die Folge: Nach Kauf der Geräte bekannt werdende Sicherheitslücken werden nicht geschlossen, die Geräte sind oftmals schlecht geschützt.

2.2 Digitale Identität

Cyberkriminelle sind an allen Arten von Zugangsdaten interessiert, mit denen sie letztlich zu Lasten Dritter und zum eigenen Vorteil Verfügungen im Internet vornehmen können. Die digitale Identität ist die Summe aller Möglichkeiten und

Rechte des einzelnen Nutzers sowie seiner Aktivitäten innerhalb der Gesamtstruktur des Internets. Konkret: alle Arten von Nutzer-Accounts inkl. Passwörter.[6]

Die deutschen Behörden beschäftigt ganz aktuell ein Fall, bei dem im Rahmen von Ermittlungen gegen Cyberkriminelle eine Datensammlung von ca. 16 Mio. deutschen und anderen
E-Mail-Adressen mit Passwörtern entdeckt wurde. Bislang ist nicht bekannt, wie die Täter an diese Daten gelangten, ob sie ggf. schon missbräuchlich genutzt wurden und welche Schäden evtl. bereits entstanden sind. Sie haben bestimmt davon gehört: Das Bundesamt für Sicherheit in der Informationstechnik hat in diesem Zusammenhang Anfang des Jahres 2014 im Internet die Seite „www.sicherheitstest.bsi.de“ eingerichtet. Dort können Internetnutzer überprüfen, ob ihnen zuzuordnende Daten betroffen sind. Rund 30 Mio. Mal haben Bürgerinnen und Bürger dieses Angebot genutzt. In rund 1,6 Mio. Fällen erfolgten Treffermeldungen an die jeweils Anfragenden, d. h. die angefragten E-Mail-Adressen befanden sich unter den*
16 Mio. „gestohlenen“ Datensätzen.[7] Unlängst ist ein zweiter großer Fall mit erneut 16-20 Mio. gestohlenen E-Mail-Account-Daten bekannt geworden.

2.3 Carding

Darüber hinaus sind insb. auch Kreditkartendaten einschließlich der Zahlungsadressen und weiterer Informationen Bestandteil der digitalen Identität. Nach unserer Schätzung waren in den letzten Jahren mindestens 200.000 Kreditkartenbesitzer pro Jahr in Deutschland von betrügerischen Kreditkartenumsätzen betroffen – Tendenz steigend. Wir sprechen hier von „Carding“.

Der Schaden lag nach unserer Einschätzung allein für die deutsche Finanzwirtschaft im mittleren dreistelligen Millionen-Euro-Bereich – ca. 70 % dieser Schäden resultieren aus dem Internet-Geschäft! Weltweit wurden nach Angaben von Interpol allein im Jahr 2010 über 160 Mio. verlorene Kreditkartendatensätze registriert – mit einer Kaufkraft von über 5 Mrd. US-$.

---

[6] Beispiele: Email- und Messengerdienste, soziale Netzwerke, E-Commerce (Onlinebanking, Onlinebrokerage, Vertriebsportale wie z. B. eBay, Buchungssysteme für Flüge, Hotels usw.), Homeoffice-Accounts mit Zugriff auf firmeninterne Ressourcen, E-Government, Cloud-Computing
[7] Stand 12.02.2014: 29,7 Mio. Anfragen, 1,58 Mio. Treffer

Ein Beispiel für den gewinnbringenden Einsatz von Kreditkartendaten durch Cyberkriminelle:

Vor genau einem Jahr fand einer der größten Banküberfälle moderner Prägung statt: Nach erfolgreichen Hackingangriffen hoben Kriminelle mit gefälschten Kreditkarten innerhalb von zwei Tagen bei 17.000 Abhebungen in insgesamt 23 Staaten weltweit rund 40 Millionen US-Dollar ab. Deutschland war mit 2,3 Mio. Euro in 8 Städten betroffen.

2.4 Scareware, Ransomware

Ein weiteres Beispiel für den Variantenreichtum der Täter ist der Einsatz sog. Scareware – Software, die Angst erzeugen soll. Der Nutzer wird auf eine Webseite geleitet, die ihm vorgaukelt, dass auf seinem Computer ein Systemscan zu Viren, Trojanern etc. vorgenommen und eine große Anzahl Schadsoftware gefunden wurde. Ihm wird dann ein Tool zur Entfernung der Schadsoftware angeboten. Bei der Ausführung des Tools auf dem Rechner installiert sich eine angebliche Antiviren-Lösung. Diese müsse nach der Installation noch bezahlt und registriert werden. Der von Angst um die Sicherheit seiner Daten beeinflusste Kunde gibt seine Kreditkarteninformationen zur Bezahlung preis. Im Zuge dieses Vorgangs werden weitere Informationen zur Anschrift bzw. zur
E-Mailadresse des Kunden gefordert.
Was der Kunde nicht weiß:
Das installierte Tool, mit dessen Hilfe er vermeintliche Gefahren für seinen Rechner abwenden wollte, sorgt dafür, dass sich Schadsoftware auf seinem System installiert.

Zur Dimension von Straftaten mittels Scareware: Allein Microsoft hat nach eigenen Angaben in einem Jahr mehr als 13 Millionen Rechner von Scareware gesäubert. Auch „digitale Erpressungen“ sind – in verschiedenen Varianten – ein zunehmendes Phänomen, dem sowohl Privatpersonen wie auch Unternehmen zum Opfer fallen können. Einige Beispiele:

- Kompromittierte Daten, die dem ursprünglichen Berechtigten „gestohlen“ wurden, werden zum Rückkauf angeboten.
- Der Angreifer droht damit, den erfolgreichen Angriff auf die Daten bzw. IT-Infrastruktur eines Unternehmens publik zu machen.
  Das betroffene Unternehmen wird zur Zahlung eines „Schweigegeldes“ aufgefordert.

- Die Erpressung von Schutzgeld erfolgt z. B. durch die Androhung von DDoS-Angriffen auf die IT-Infrastruktur eines Unternehmens. Bei Ablehnung erfolgen tatsächlich entsprechende Attacken – dazu später mehr.

Eine ähnliche Systematik steckt hinter der sog. Ransomware[8]. Diese infiziert z.B. beim Surfen im Internet den Computer des Opfers. Danach öffnet sich ein Pop-Up-Fenster, in dem behauptet wird, der Computer sei für strafbare Handlungen verwendet worden. Deshalb sei der Computer gesperrt worden.
Zur Entsperrung soll der Benutzer des Computers eine "Strafe" in Höhe von 100 € mittels eines digitalen Bezahldienstes entrichten. Sollte er nicht zahlen, würde die Festplatte gelöscht. Es werden vergleichsweise geringe Summen gefordert, um einen möglichst großen Anteil der Infektions-Opfer zu einer Zahlung zu bewegen. Um den Eindruck einer polizeilichen Handlung zu erwecken, nutzen die Täter die Logos von Polizeibehörden sowie von verschiedenen bekannten Antiviren-Herstellern. In einem konkreten Fall ergab sich, dass ein Täter in Deutschland in lediglich 6 Tagen 200.000 Infektionen verursachte und dabei über 32.000 Mal erfolgreich war.

Mittlerweile sind weltweit zahlreiche Staaten von diesem Phänomen betroffen. Angepasste Versionen der Ransomware sind zwischenzeitlich z. B. auch in Nord- und Südamerika im Umlauf.
Der Grund: (Den Quellcode der) Schadsoftware kann man (seit Ende 2011) in der sog. Underground Economy kaufen.

2.5 Botnetze

Cyberkriminelle bedienen sich bei ihren Taten oftmals sog. Botnetze — von Cyberkriminellen mit Malware infizierte und darüber gesteuerte Computer meist ahnungsloser Opfer. Einmal infiziert wird der Rechner des Opfers zur Angriffsressource der Täter, zum Tatmittel!

Welche Dimensionen Botnetze annehmen können, zeigt ein Beispiel aus Spanien. Ein 23-jähriger „Bot-Herder“ kontrollierte ein weltweiten Botnetz („Mariposa“) mit 12 Mio. infizierten Rechnern.

Anfang Juni 2013 wurden ausgehend von den USA Maßnahmen gegen die Infrastruktur der sog. Citadel-Botnetze durchgeführt.

---

8 to ransom: auslösen, freikaufen

In mehr als 80 Ländern wurden etwa 1.000 von insgesamt geschätzten 1.400 Comand & Control-Servern, die Server, über die die Bots gesteuert werden, abgeschaltet. Weltweit sollen (nach Angaben von Microsoft) bis zu 5 Millionen PC von der Citadel-Schadsoftware befallen sein.[9]

Nach den PC-Systemen rücken mittlerweile zunehmend Smartphones in das Visier von Cyberkriminellen. Die Infizierung erfolgt mittels manipulierter Apps. Ist ein Gerät infiziert, wird es Teil eines Botnetzes; Schadsoftware mit weiteren Funktionen kann jederzeit nachgeladen werden. Aus Sicht der Täter ist das Smartphone der bessere Bot!
Moderne Smartphones sind leistungsfähige Rechner, immer eingeschaltet und über moderne Hochgeschwindigkeitsnetze permanent mit dem Internet verbunden – „Always on"!

Gerade dieses Beispiel verdeutlicht:
Kriminelle analysieren neue Technologien hinsichtlich möglicher illegaler Anwendungsmöglichkeiten, finden deren Schwachstellen und entwickeln in kürzester Zeit Methoden diese für ihre Zwecke nutzbar zu machen.

2.6 Underground-Economy

Im Internet hat sich ein eigener Markt etabliert, für alles, was Cyberkriminelle zur Tatbegehung benötigen. Die Angebote der „Underground Economy" reichen von

1. Schadsoftware über
2. Serverkapzitäten,
3. anonyme oder verschlüsselte Kommunikationswege,
4. Services zur Erstellung falscher Identitäten,
5. Kreditkartendaten bis hin zu
6. anonymen Zahlungssystemen.

Dies verdeutlicht, wie professionell organisiert und lukrativ Cybercrime ist.

[9] Reuters v. 06.06.2013

2.7 Angriffe auf Kritische Infrastrukturen

Das Internet und die darüber verfügbaren Dienste sind längst selbst zur kritischen Infrastruktur geworden. Angriffe können, wie bereits skizziert, fatale Auswirkungen auf Wirtschaft und Gesellschaft haben. Die Grenzen zwischen Kriminalität, Spionage und Terrorismus sind dabei unscharf.[10]

Wie weitreichend die Folgen von Cyberangriffen sein können, die Schwachstellen im System missbrauchen, zeigt eine seit 2010[11] weltweit festgestellte Reihe von Angriffen auf Industrieanlagen o. a. Kritische Infrastrukturen mittels Schadsoftware.

Oder: Als Kollateralschaden können die Folgen eines DDoS-Massenangriffs auf eine Organisation gegen unerwünschte Internetwerbung, die SPAMHAUS-Gruppe, im März 2013 gewertet werden. SPAMHAUS erstellt u. a. Echtzeit-Blacklists von Spam-Versendern, um Internetanbietern das Herausfiltern der Urheber zu ermöglichen. Der Angriff blockierte jedoch nicht nur den Zugriff auf die Web-Site von SPAMHAUS, sondern führte zeitweise zum Ausfall des zentralen Internetknotens Großbritanniens, und bremste darüber hinaus weite Teile des gesamten Internet.

2.8 Cybermobbing

Es sind aber auch die alltäglichen Fälle von Cybermobbing zu erwähnen.

Cybermobbing ist das absichtliche Beleidigen, Bedrohen oder Belästigen von meistens Schülern über das Internet oder per Handy über einen längeren Zeitraum. Die Täter(innen) nutzen Internet- und Mobiltelefondienste zum Bloßstellen und Schikanieren ihrer Opfer. Hierzu zählen im Internet E-Mail, Online-Communities, Mikrobloggs, Chats (Chatrooms, Instant Messenger), Diskussionsforen, Gästebücher und Boards, Video- und Fotoplattformen, Websites und andere Anwendungen. Mobiltelefone werden für Mobbingaktivitäten genutzt, um die Opfer mit Anrufen, SMS, MMS oder E-Mails zu tyrannisieren. Die multimediale Ausstattung der Mobiltelefone mit Foto- und Videokamera, Sprachaufzeichnungsmöglichkeit und Internetzugang gibt im Kontext des Mobbings leicht nutzbare Technologien an die Hand.

Das Internet scheint die Hemmschwelle für Mobbingaktivitäten zu senken. Viele trauen sich in der scheinbar anonymen virtuellen Welt eher, Andere anzugreifen, zu

---

[10] FAZNET 07.02.2011; De Maiziére während der Münchener Sicherheitskonferenz
[11] Erstmals im Juli 2010 wurde der Trojaner Stuxnet entdeckt

beleidigen oder bloßzustellen. Die psychologische Hemmschwelle bei direktem Kontakt gibt es nicht mehr! Dabei gibt es einen fließenden Übergang von "Spaß" zur Gewaltausübung im Sinne von Mobbing. Mit Aussagen wie "Das war doch nicht ernst gemeint, das war nur Spaß" verdeutlichen die „Spaßvögel“, dass ihnen häufig das notwendige Unrechtsbewusstsein, die erforderliche Sensibilität für ihr eigenes Handeln fehlt.

Da das Internet nichts vergisst, also selbst sogenannte „gelöschte Inhalte“ immer wieder auftauchen können, ist es möglich, dass das Opfer selbst nach einer Beendigung des Konfliktes mit dem Täter immer wieder mit den Veröffentlichungen konfrontiert wird. Cybermobbing kann bisweilen tragische Folgen haben, so gibt es bereits Suizide von Schülerinnen, als Folge von Cybermobbing.

Im Jahr 2011 wurden 25.000 europäische Kinder- und Jugendliche zwischen 9- und 16 Jahren im Rahmen der EU Kids Online-Studie zu ihrer Erfahrung mit Cyber-Mobbing repräsentativ befragt. Europaweit gaben hierbei 6 Prozent der befragten Kinder und Jugendlichen an, dass sie innerhalb der letzten 12 Monate entweder als Opfer oder als Täter Erfahrungen mit Cyber-Mobbing gemacht haben. Mit 5 Prozent entsprechend betroffener Kinder liegt Deutschland hier knapp unterhalb des Durchschnitts im europäischen Vergleich.

3. BEKÄMPFUNGSSTRATEGIEN

Die Bedrohungen durch Cybercrime sind vielfältig. Das Internet bietet Straftätern unzählige Tatgelegenheiten, unzählige potenzielle Opfer und Angriffspunkte. Das Gefährdungs- und Schadenspotenzial ist hoch — und wird unserer Einschätzung nach in den kommenden Jahren noch zunehmen. Technische Entwicklungen hin zu einer Gesellschaft „Always on“ werden verstärkende Wirkung haben. Entscheidenden Einfluss wird dabei u. a. die zunehmende Verbreitung von Smartphones und mobilen Computern wie Tablets haben.

3.1. Global-Player-Initiative

Die veränderten Erscheinungsformen der Kriminalität zeigen deutlich: An einer ganzheitlichen Bekämpfungsstrategie führt kein Weg vorbei.

Neben einem konsequenten behördenübergreifenden operativen Handeln ist dabei entscheidend, auch die Wirtschaftsunternehmen in ein Netzwerk der Informationen einzubeziehen. Das BKA hat in den vergangenen Jahren die Zusammenarbeit mit

der Wirtschaft stetig ausgebaut. Wir haben die Initiative zu einem intensiven direkten Dialog mit der Wirtschaft, hier insbesondere mit weltweit tätigen deutschen Global Playern ergriffen. Mittlerweile haben sich 58 Unternehmen für die Zusammenarbeit mit uns entschieden.

Unternehmen verfügen oftmals über wichtige Informationen, die unsere Erkenntnisse ergänzen und in unsere Früherkennungsstrategien einfließen können. Im Gegenzug können wir Unternehmen für Gefährdungslagen sensibilisieren. Diese können dann entsprechende Schutzvorkehrungen ergreifen.

3.2. IPPP

Bei der Bekämpfung der Cyberkriminalität soll die in Unternehmen, Forschungsinstituten, Wirtschaft und Wissenschaft vorhandene Fachkompetenz noch viel umfassender als bisher einbezogen werden. Darüber hinaus wollen wir dem Wunsch zahlreicher Wirtschaftsunternehmen und Verbände nach einem zentralen Ansprechpartner für alle Fragen zur Cybercrime entsprechen.

Als ersten Schritt haben wir mit zentralen Akteuren aus dem Bankensektor für den Bereich Cybercrime eine Kooperation in Form einer institutionalisierten Private Public Partnership (iPPP) geschlossen.[12] Diese neue Kooperationsplattform mit dem von großen deutschen Banken gegründeten „German Competence Center for Cybercrime“ (G4C) ist operativ ausgerichtet. An dieses Center angebunden sind Cybercrime-Spezialisten des BKA. Damit sollen die Belange einer wirksamen Strafverfolgung in diesem Deliktsfeld gestärkt werden.

3.3. Handlungsempfehlungen in Fällen von Cybercrime

Für die Wirtschaft gilt:

Cybercrime kann jeden treffen: Eine Studie[13] zeigt, dass insbesondere kleine und mittelständische Unternehmen im Fokus der Cyberkriminellen stehen:
50 Prozent aller Cyberangriffe zielen auf Unternehmen mit weniger als 2.500 Mitarbeitern, ein Drittel auf Unternehmen mit weniger als 250 Mitarbeitern ab.

---

[12] Unterzeichnung der Kooperationsvereinbarung mit dem Verein G4C ist für den 21.01.2014 vorgesehen

[13] Symantec Corporation: Internet Security Threat Report 18/2013.

Gerade weil diese Unternehmen glauben, uninteressant für Cyberkriminelle zu sein, stoßen die Täter hier auf unzureichende Sicherheitsvorkehrungen. So nachvollziehbar die Begründungen der Unternehmen, Angriffe nicht anzuzeigen auf den ersten Blick erscheinen, so kontraproduktiv sind die Folgen für die Gemeinschaft: Solange Unternehmen erkannte Angriffe verschweigen, gibt es keinen Ermittlungsansatz für die zuständigen Behörden und damit keinen validen Überblick über die gesamte Bedrohungslage.
Die Schadenspotenziale vergrößern sich durch Nichtanzeige!

In diesem Zusammenhang sollte auch die im politischen Raum angedachte Meldepflicht für Cyberangriffe gesehen werden, die in Kreisen der Wirtschaft weitgehend abgelehnt wird.

Die Polizeibehörden der Länder und das BKA haben „Handlungsempfehlungen für die Wirtschaft in Fällen von Cybercrime“ erarbeitet. Diese Leitlinien sollen betroffenen Unternehmen konkrete Hinweise zum Verhalten bei Cyber-Angriffen geben und zudem Unsicherheiten im Zusammenhang mit der Anzeige solch strafrechtlich relevanter Vorfälle nehmen. Berücksichtigt werden daher sowohl die Belange der Strafverfolgungsbehörden als auch der Wirtschaftsunternehmen. U. a. werden

- Gesetzesgrundlagen vorgestellt,
- Verhaltensempfehlungen für Firmenleitung und Systemadministratoren gegeben,
- Möglichkeiten und Grundsätze der polizeilichen Ermittlungsarbeit dargestellt
- und zentrale Ansprechstellen bei der Polizei in Bund und Ländern benannt.

Diese Handlungsempfehlungen stehen in gedruckter Form sowie als Online-Version auf unserer Homepage www.bka.de zur Verfügung.

Aber auch für Jedermann gilt, dass man sich vor Gefahren im Internet schützen kann.

1. Schutz des PC
An oberster Stelle steht eine gute Sicherheitsausstattung für Ihren Computer mit Anti-Viren Programmen und einer Firewall. Da Schadsoftware zunehmend über externe Datenträger wie CDs oder USB-Sticks verbreitet wird, sollten diese vor der Nutzung auf Viren geprüft werden.

2. E-Mails und Chat

Öffnen Sie nur E-Mails, die von vertrauenswürdigen Absendern stammen. Dubiose Mails von Unbekannten möglichst sofort löschen. Schadprogramme verbergen sich oft in Grafiken oder E-Mail Anhängen. Verdächtige Dateien sollten Sie auf keinen Fall öffnen!

3. Software

Achten Sie darauf, welche Software oder Zusatzprogramme („Plug-Ins“) Sie installieren. Gesundes Misstrauen hilft: Wenn Zweifel an der Seriosität bestehen, besser auf Download und Installation einer Software verzichten.

4. Tauschbörsen

Wer im Internet mit Unbekannten Dateien tauscht, riskiert eine Infektion seines PCs mit Schadprogrammen. Zudem ist der Tausch von urheberrechtlich geschützten Musik-, Film- oder Software-Kopien strafbar und kann gegebenenfalls neben Geld- und Freiheitsstrafen zu Schadenersatzansprüchen der Rechteinhaber führen.

5. Online-Shopping

Auf vielen Shopping-, Preisvergleich- und Auktionsseiten werden Händler beurteilt. Gute Bewertungen können ein Hinweis auf seriöse Geschäftspraktiken sein. In jedem Fall ist jedoch eine Portion gesundes Misstrauen angebracht – vor allem auf Webseiten mit Angeboten weit unter dem tatsächlichen Wert.

6. Bezahlung im Web

Beim Kauf von Waren im Internet ist allgemein Vorsicht geboten, insbesondere bei Vorauszahlung. Zur Bezahlung sollten Konto- oder Kreditkartendaten über eine verschlüsselte Verbindung übertragen werden.

7. Online-Banking

Die Verbindung zum Bankcomputer muss wie bei Bezahlvorgängen verschlüsselt sein, Es gibt immer wieder neue Schutzverfahren wie iTAN, eTAN und HBCI. Sie sollten ihre Bank fragen und das modernste Verfahren wählen.

8. Private Infos und Passwörter

Verwenden Sie nicht das gleiche Passwort für mehrere Dienste – etwa E-Mail Konto, Online-Shops und Communitys. Je länger ein Passwort, desto schwerer ist es zu knacken.

9. Angebote als Waren- oder Finanzagenten

Angebote im Internet oder per E-Mail als Waren- oder Geldvermittler zu arbeiten,

sind konsequent abzulehnen. Wenn Sie sich auf dubiose Angebote einlassen und Waren oder Gelder weiterleiten, betreiben Sie Beihilfe zum Betrug oder der Geldwäsche und müssen mit strafrechtlichen Folgen und Schadenersatzansprüchen rechnen.

10. Apps und Abofallen

Seien Sie sich bewusst, dass Apps Kosten verursachen sowie sensible Nutzerdaten übertragen können. Seien Sie daher besonders bei kostenlosen Apps vorsichtig. Achtung geboten ist zudem bei Online-Diensten bei denen eine Registrierung erforderlich ist. Neben der breiten Masse der seriösen Werbeangebote gibt es auch Fallen, bei denen versteckt Bestellungen oder Abo-Verträge abgeschlossen werden.

Ich appelliere daher an Sie: Der verantwortungsvolle Umgang bei der Benutzung des Internets liegt bei Ihnen!

4. SCHLUSS

Das Internet ist eine inzwischen unverzichtbare Stütze weltweiter ökonomischer, politischer und gesellschaftlicher Informations- und Kommunikationsprozesse, zugleich aber auch ein Feld vielfältigen kriminellen Handelns.

Das Internet darf kein strafverfolgungsfreier Raum sein; Kriminalitätsbekämpfung muss auch dort möglich sein, um langfristig das Vertrauen in das Internet zu stärken und dessen Vorteile zu erhalten.

Um die international agierende und vernetzte Cybercrime wirksam bekämpfen zu können, bedarf es der vertrauensvollen Kooperation der Sicherheitsbehörden. Wir stehen vor gemeinsamen Herausforderungen, gegen die wir gemeinsam und aufeinander abgestimmt agieren und zu denen wir unser Wissen austauschen müssen.

Es bedarf aber auch dem Bewusstsein und der Eigenverantwortung der Unternehmen und letztlich der Bürgerinnen und Bürgern. Deshalb begrüße ich diese Sonderveranstaltung zum Thema Cybersicherheit im Rahmen des Deutschen Präventionstages sehr.