Model United Nations Baden-Württemberg 2019

Hauptausschuss 1

Umgang mit Cyberkriminalität

Benjamin Ziegs[1]

Einleitung

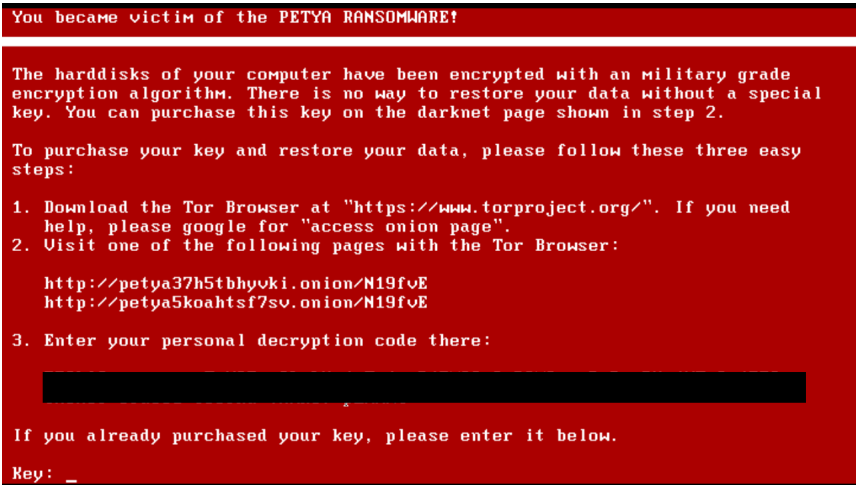
Die IT-Infrastruktur ganzer Konzerne und Regierungen mittels Erpressungs-Trojanern verschlüsseln und lahmlegen, komplett anonymen Waffen- und Drogenhandel betreiben, streng vertrauliche Nutzerdaten abgreifen, um sie missbräuchlich nutzen zu können oder per Mausklick die kombinierte Rechenleistung Hunderttausender Computer für kriminelle Zwecke verwenden – nur exemplarisch seien hier einige wenige moderne Erscheinungsformen der Computerkriminalität, auch Cyberkriminalität oder Cybercrime genannt, aufgeführt.

Sturmhaube und Dietrich haben ausgedient – längst erledigen Kriminelle ihre virtuellen Beutezüge weltweit und grenzüberschreitend über das Internet: geräuschlos, in Sekundenschnelle und oftmals, ohne Spuren ihres Eindringens zu hinterlassen. Was bleibt, ist ein hoher volkswirtschaftlicher Schaden – in Deutschland betrug dieser zuletzt rund 71,4 Mio. Euro. Tendenz steigend, denn kaum ein Deliktsbereich verzeichnet so hohe Entwicklungsraten und eine Dynamik wie die Cyberkriminalität. Insbesondere im Zeitalter von Digitalisierung und Industrie 4.0 kommt dem Thema eine besonders hohe Bedeutung zu. Dieser Bericht soll Arten der Cyberkriminalität unter Berücksichtigung aktueller Tendenzen aufzeigen sowie einen Überblick über Lösungsansätze und damit verbundene Probleme geben. Dabei wird besonders die Wichtigkeit der transnationalen Behandlung des Themas deutlich: Kriminelle agieren in zeitgleich in zahllosen Ländern, mit unterschiedlicher Gesetzgebung, anderen Exekutivgewalten und manchmal sogar ohne Strafverfolgung. Es ist sinnvoll, eine Harmonisierung UN-weiter Regularien zur internationalen Zusammenarbeit voranzutreiben.

[1] b.ziegs@munbw.de

Hintergrund und Grundsätzliches

Unter den Begriff „Cyberkriminalität“ zählt man im Allgemeinen (versuchte) Straftaten, die unter Ausnutzung von IuK- (Informations- und Kommunikations-)Technologien durchgeführt werden oder sich gegen derartige Technologien richten. Hiervon abzugrenzen ist der Begriff der „Internetkriminalität“. Diese unterscheidet sich in der Hauptsache dadurch, dass explizit das Internet als Tatmittel oder Angriffsziel gewählt wird, der Straftatbestand allerdings auch „analog“ zu erfüllen wäre, etwa durch Verbreitung verfassungswidriger Schriften oder (sexuelle) Belästigung, wohingegen Cybercrime vor allem Taten im Kontext elektronischer Datenverarbeitung bezeichnet. Die geschichtliche Entwicklung beginnt mit der zunehmenden „Elektronisierung“ der Gesellschaft in den 1990er Jahren, insbesondere im wirtschaftlichen Bereich. Seitdem befinden sich Kriminelle und Sicherheitsexpert*innen (s.u.) in einem „Hase-und-Igel“-Wettlauf; in den letzten Jahren werden die Methoden der Kriminellen allerdings immer ausgereifter und haben mittlerweile ein sehr hohes technisches Niveau erreicht.



Das Bundeskriminalamt unterscheidet folgende wesentlichen Handlungsfelder, in denen Cyberkriminelle aktiv werden:

Identitätsdiebstahl: mittels „Phishing“, bspw. durch Einsatz

gefälschter Websites, erhalten Kriminelle Zugriff auf die „digitale Identität“ eines*einer Nutzer*in. Diese können sie zur Begehung weiterer Straftaten nutzen oder gewinnbringend weiterverkaufen.

Einsatz von Schadsoftware (Malware): Diese Art von Software wird ebenfalls für Phishing genutzt. Sie kann Virenschutzmaßnahmen meist umgehen und nutzt Sicherheitslücken in IuK-Systemen mittels so genannter Exploits aus. Malware kann unter anderem über infizierte E-Mail-Anhänge oder so genannte Drive-By-Infektionen auf entsprechend präparierten Internetseiten auf den Rechner eines Opfers gelangen. Jedoch werden Straftäter mit jedem Tag einfallsreicher und finden weitere Möglichkeiten, Malware zu verbreiten (z. B. infizierte USB-Sticks (u. a. bei Stuxnet), präparierte e-Zigaretten u.s.w.).

Schadsoftware für mobile Endgeräte: durch die zunehmende Verbreitung von Smartphones & Co. wächst dieser Bereich besonders schnell. Angriffe zielen hier meist auf die Erlangung von Transaktionsnummern (TANs) für Online-Banking ab. Die Infektion erfolgt auf ähnlichen Wegen wie eine Malwareinfektion, aber auch über Apps.

Social Engineering: Der*die Nutzer*in gilt als schwächstes Glied in der „Sicherheitskette“. Durch gezielte psychologische Manipulation können Angreifer*innen Zugriff auf geschützte Daten erhalten oder Computer infizieren. Besonders häufig ist die Methode des so genannten „CEO Frauds“, d.h. Betrüger*innen geben sich mittels gefälschter E-Mails, Briefen oder fingierten Telefonanrufen als Mitglieder der Geschäftsführung aus und fordern die Überweisung hoher Geldsummen auf ausländische Bankverbindungen. Insbesondere in autoritär geführten Unternehmen hat diese Methode Erfolg, da Zweifel gegenüber der Geschäftsführung dort unerwünscht sind. Cyberkriminelle nutzen hierbei öffentlich zugängliche Informationen über ein Unternehmen oder Erkenntnisse aus vorangegangenen Anrufen/Betrugsversuchen, um auf den*die Mitarbeiter*in authentisch zu wirken.

Digitale Erpressung/Ransomware: Malware, die sämtliche Dateien eines IT-Systems und teilweise auch Netzwerkordner mittels starker Kryptographie verschlüsselt, fordert den*die Nutzer*in zur Zahlung teils hoher Geldbeträge zum Beispiel in der digitalen Währung „Bitcoin“ auf,

um die Daten wieder entschlüsseln zu können. Entsprechende Tools können mittlerweile als „Baukasten“ erworben werden, somit sind zur Durchführung einer Erpressung keine besonderen IT-Kenntnisse mehr erforderlich.

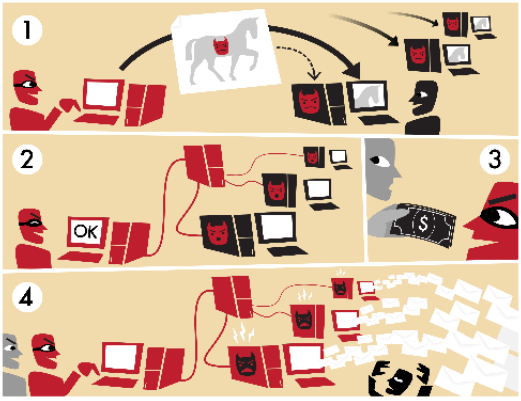
Massenhafte Fernsteuerung von Computern („Botnetz“): Eine hohe Anzahl von Computersystemen wird mit einer Schadsoftware infiziert, die anschließend auf Befehl eines Command & Control-Servers gleichzeitig aktiv werden. Botnetze werden hauptsächlich dazu genutzt, Webservices über DDoS-Attacken (Distributed Denial of Service) lahmzulegen. Gleichzeitig bietet die Software die Möglichkeit, infizierte Rechner auszuspähen oder zur Generierung von Kryptowährung zu nutzen. Auch Botnetze können, ebenfalls wie Ransomware, „schlüsselfertig“ im Darkweb erworben werden.

Als weiteres Betätigungsfeld hat sich die Manipulation oder Desinformation ganzer Bevölkerungsgruppen respektive Bürgern*innen eines Landes aufgetan. Dabei werden durch soziale Netzwerke, durch Propaganda-TV-Sendungen oder über Internetbeiträge Wahlen, Abstimmungen oder allgemein Meinungsbilder der Bevölkerung beeinflusst. Manche Nationen sehen darin einen Angriff auf ihre Souveränität und behalten sich Gegenmaßnahmen bis hin zu militärischer Intervention vor.

Der überwiegende Teil von Cybercrime-Straftaten wird von den Opfern nicht zur Anzeige gebracht. Um dennoch ein verlässliches Bild über die Lage der Cyberkriminalität in Deutschland zu erhalten, wurde das German Competence Centre against Cyber Crime (G4C) gegründet. In diesem Verein tauschen sich Banken, Versicherungen sowie Softwarehersteller mit BKA und BSI über aktuelle Entwicklungen aus und entwickeln gemeinsam Lösungen zur Prävention, Abwehr und Abmilderung von Cyberangriffen. Auch auf multinationaler Ebene werden Zusammenschlüsse von Expert*innen aus Polizei, Nachrichtendienst und Industrie formiert, so beispielsweise die ENISA der EU-Kommission oder EC3 von Europol.

Aktuelles

Nahezu täglich erfährt man in einschlägigen Fachzeitschriften und Internetseiten (bspw. heise.de) von neuen Cybercrime-Taten, deren Auswirkungen teils enorme Auswirkungen haben, als Beispiel seien hier der Datendiebstahl bei der Wirtschaftsauskunftei Equifax im Jahre 2017 genannt, welcher die Identitäts- und wirtschaftlichen Daten von bis zu 143 Millionen US-Amerikaner*innen betraf oder auch die weltweiten „WannaCry"-Attacken im Mai 2017, bei welcher ein Erpressungstrojaner (s.o., „Ransomware") genutzt wurde, um die Daten von Millionen Nutzer*innen weltweit zu verschlüsseln und nur gegen Zahlung eines Lösegelds in Form von Bitcoins wieder zu entschlüsseln. Weltweit waren mehrere Großkonzerne, darunter der Telekommunikationsanbieter Telefónica oder auch die Deutsche Bahn, tagelang betroffen.



Laut einer aktuellen Studie von Symantec, einem Hersteller von Sicherheitssoftware, waren im Jahre 2017 978 Millionen Menschen von Cyberkriminalität betroffen. Die finanziellen Auswirkungen von Cybercrime werden nicht bloß durch Erpressungstrojaner hervorgerufen: 38% der Betroffenen erlebten eine missbräuchliche Nutzung ihrer Kreditkarten- oder Bankdaten oder fielen auf betrügerische Online-Shops herein. Im Schnitt entstand ihnen dadurch ein Pro-Kopf-Schaden in Höhe von 142 $ sowie 24 entgangene Arbeitsstunden – also drei volle Arbeitstage. Die Demografie der Opfer ist sehr heterogen – junge Leute, d.h. Digital Natives, sind gleichermaßen betroffen wie Digital Immigrants.

Für die zukünftige Entwicklung erwartet das Bundeskriminalamt komplett neue, qualitativ eher niederschwellige, Angriffsvektoren – insbesondere ist hier die rasche Verbreitung des so genannten Internets der Dinge (IoT) zu nennen. Gewöhnliche Haus- und Haushaltsgeräte

sind heute in der Lage, ihre Funktionalität über das Internet zu erweitern. Das Problem liegt darin, dass die Hersteller den Fokus nicht unbedingt auf die (Cyber-)Sicherheit ihrer Produkte legen, was dazu führt, dass „Things" ebenfalls tausendfach für ein Botnetz instrumentalisiert werden können – 2016 wurde ein entsprechender Angriff durch die Schadsoftware Mirai bekannt. Weitere Dimensionen sieht das BKA in Geldwäsche durch die Verbreitung von Kryptowährungen wie Bitcoin sowie Kriminelle, die ihre Dienste anbieten (angelehnt an das oben angesprochene Baukastensystem; dies wird „Crime-as-a-Service" genannt.

Innerhalb der Vereinten Nationen ist Cyberkriminalität selbstverständlich auch ein vielbeachtetes und -diskutiertes Thema. Federführend ist hier das UNODC (United Nations Office on Drugs and Crime), wie auch viele nationale Nachrichtendienste wie der GCHQ in Großbritannien. Als problematisch wird hier. insbesondere das Auftreten von Cyberkriminalität als transnationales und komplexes Verbrechen angesehen – das Internet bzw. der virtuelle Raum (Cyberspace) kennt keine nationalen Grenzen, was einerseits die globale Zusammenarbeit und Entwicklungen wie Globalisierung fördert, andererseits die Strafverfolgung stark erschwert, zumal Cyberkriminalität mittlerweile auch oftmals ein Tätigkeitsfeld der organisierten Kriminalität darstellt. Das UNODC nimmt hier global ähnliche Aufgaben wie das bereits erwähnte G4C wahr – in Kooperation mit den lokalen Strafverfolgungsbehörden stellt es technische und fachliche Unterstützung zur Verfügung, koordiniert Präventions- und Awareness-Maßnahmen und führt im Rahmen internationaler Kooperation Analysen und Forschungsprojekte zum Thema Cybercrime durch. Als Ausprägungen sind hier das Global Programme on Cybercrime, die Expert*innengruppe zum Thema Cybercrime sowie das UNODC Cybercrime Repository, eine zentrale Datensammlung für Rechtsvorschriften und Lessons Learned zum Thema Cyberkriminalität, zu nennen.

Bei einer Versammlung des UNODC in Wien im Mai 2018 wurde ebenfalls die besondere Bedeutung der Bekämpfung von Cyberkriminalität hervorgehoben mit dem Erfordernis, dass die Strafverfolgungsbehörden der Mitgliedsstaaten entsprechende Kapazitäten zur Prävention und Bekämpfung von Cybercrime zur Verfügung gestellt bekommen – denn

Cybercrime ist nach Ansicht des Generalsekretärs António Guterres ein Feld, in dem es viel zu tun gibt, ohne dabei Zeit zu verlieren, denn Cyberkriminalität betrifft, wie jede Art der Kriminalität, vor allem die schützenswertesten Personen, denen eigentlich die Vorteile der digitalen Revolution, wie Big Data oder Analytics, zugutekommen sollten.

Probleme und Lösungsansätze

Betrachtet man die vorangegangenen Kapitel, so kommt man zu dem Schluss, dass Cyberkriminalität ein globales, sehr ernstzunehmendes Problem darstellt. Die jüngsten Entwicklungen, insbesondere Crime-as-a-Service zeigen auf, dass ein*e Angreifer*in mittlerweile nicht einmal mehr fortgeschrittene IT-Kenntnisse benötigt, um mit Malware einen immensen Schaden anzurichten. Insbesondere in hochgradig digitalisierten Unternehmen kommt der Ausfall der IuK-Infrastruktur einem Super-GAU gleich, der die Produktion vollständig zum Erliegen bringen kann – mit entsprechenden wirtschaftlichen Folgen. Auch im alltäglichen Kontext kann die Manipulation bspw. des Betriebssystemes eines Kernkraftwerkes oder allgemeiner Verkehrseinrichtungen, wie Ampeln, Tunneln oder Gleisanlagen, zu – nachvollziehbaren – gravierenden Problemen führen. Doch Cyberkriminalität zielt nicht immer nur auf Vermögensschäden ab – sind, wie zuletzt bei der WannaCry-Attacke 2017, auch Institutionen wie Krankenhäuser betroffen, bekommt Cyberkriminalität auch eine humanitäre Seite. Der britische National Health Service (NHS) musste Patienten in den Notaufnahmen abweisen, da die IT-Systeme ebenfalls betroffen waren.

Möchte man die Schuldfrage im Angesicht von Attacken wie WannaCry klären, so wäre es zu einfach, die Schuld komplett bei den Cyberkriminellen zu verorten. Vielmehr handelt es sich hier um eine Kombination aus mehreren Faktoren: zum einen ist in vielen Bereichen die IT-Infrastruktur völlig überaltert – als Microsoft im April 2014 die Versorgung von Windows XP mit Sicherheitspatches einstellte, besaß es noch einen weltweiten Marktanteil von 30%. Problematisch ist insbesondere, dass gerade im militärischen oder medizinischen Bereich

Windows XP-Systeme für „mission critical“-Anwendungen genutzt werden und die Systeme zumeist in andere Hardware (Industriesteuerungen, Geldautomaten) integriert sind und dementsprechend so gut wie nie Updates erhalten, die Sicherheitslücken schließen, da der Hersteller ansonsten eine Funktionalität nicht mehr gewährleisten kann. Zum anderen sind Anwender*innen „patchfaul“, das heißt, sie führen Updates nicht durch, die eine schwere Sicherheitslücke schließen würden, was dazu führte, dass WannaCry mit entsprechenden Auswirkungen im Mai 2017 aktiv werden konnte, obwohl seitens Microsoft bereits seit März 2017 ein Patch für ebendiesen Angriffsvektor zur Verfügung stand.

Eines der schwerwiegenderen Probleme ist jedoch auf staatlicher Seite zu benennen, genauer in der Arbeit der nationalen Geheimdienste. Institutionen wie die US-amerikanische National Security Agency (NSA), die im Zuge der Snowden-Enthüllungen im Sommer 2013 weltweit in die Schlagzeilen geriet, nutzen für ihre Arbeit mittlerweile ebenfalls Sicherheitslücken in Computersystemen aus, um Verdächtige auszuspähen. Dies führt dazu, dass diese Behörden „staatlich gesponserte“ Hackergruppen beschäftigen, um Lücken aufzuspüren und „Hacking-Tools“ zu entwickeln (insbesondere Zero-Day-Exploits, für die es bei Bekanntwerden noch keinen Patch seitens des Herstellers gibt, sind hier interessant). Hier lässt sich wieder ein Bezug zu WannaCry anbringen: die zugrundeliegende Lücke war der NSA mindestens seit 2012 unter dem Namen ETERNALBLUE bekannt und wurde für geheimdienstliche Zwecke eingesetzt, bevor sie Anfang 2017 an Microsoft gemeldet wurde. Es muss also in Zukunft abgewogen werden – ggf. mittels einer Resolution - , was wichtiger ist: die Möglichkeit der Geheimdienste, weiterhin durch den Einsatz von „staatlicher“ Schadsoftware (hierbei wäre neben Tools wie ETERNALBLUE auch der deutsche Bundestrojaner als Beispiel zu nennen) Aus- und Inlandsaufklärung in Form von Kriminalitätsbekämpfung zu betreiben oder im Interesse der Bürger*innen und Unternehmen Sicherheitslücken sofort bei Bekanntwerden zu melden und so die Cybersicherheit zu verbessern und die finanziellen und humanitären Auswirkungen von Cybercrime abzumildern.

Des Weiteren ist es dringend notwendig, dass sich die internationale

Gemeinschaft auf gemeinsame Standards, Vorgehensweisen und Protokolle einigt. Nur somit kann der wachsenden Bedrohung nicht nur wirtschaftlicher Interessen sondern auch menschlicher Leben entschlossen gegenübergetreten werden. Hierbei sollten sich die Staaten auf einige altbewährte Mittel setzen, sich aber auch auf neue Lösungsansätze besinnen.

Durch gemeinsame Datenbanken zum Informationsaustausch über Sicherheitslücken, neue Angriffsmuster oder Modi Operandi, können Angriffen besser und schneller entgegengetreten werden. Auch die Investition in multinationale Forschung, Förderung von neuen IT-Systemen und der Aufbau effizienterer Warn- und Abwehrsysteme kann zu einem neuen Bollwerk gegen erneute, weltweite Cyberattacken dienen.

Die Verbesserung der Zusammenarbeit der Strafverfolgungsbehörden und die Nutzung von Filter- und Blacklistsystemen zur Warnung und Abschirmung der Nutzer*innen vor infizierenden und betrügerischen Websites sollte der Effizienz wegen eine internationale Angelegenheit werden, die durch die Staatengemeinschaft gefördert und stetig verbessert wird.

Hierbei ist es nicht zwingend notwendig, dass sämtliche Punkte neu „erdacht“ werden, da viele Einzelstaaten diese Aufgaben bereits erfolgreich gelöst und entsprechende Systeme implementiert haben. Es ist darum naheliegend, diesen Best-Practice-Beispielen zu folgen und ggfs. international gestützt einzuführen.

Punkte zur Diskussion:

- Wie kann der wirtschaftliche Schaden von Cybercrime wirkungsvoll Wie kann der wirtschaftliche Schaden von Cybercrime wirkungsvoll eingegrenzt werden? (auch beachten: „Daten sind das Gold des 21. Jahrhunderts“)
- Sollten Geheimdienste weiter für eine effektive Arbeit Sicherheitslücken „horten“ dürfen?

- Welche Anforderungen kommen auf Soft- und Hardwareherstellern bei der Konzeption neuer Produkte zu (insbes. IoT), um Cybercrime bereits im Anfangsstadium wirkungslos zu machen? (Stichwort: „security by design“)
- Welche Rolle kommt dem UNODC kurz-, mittel-, langfristig im Kontext veränderter Angriffsvektoren und immer ausgereifterer Attacken zu?

Wichtige Dokumente

UN Resolutionen 65/230 – 67/189 - 22/7 – 22/8

Quellen und weiterführende Links

- https://de.wikipedia.org/wiki/Computerkriminalit%C3%A4t
- https://www.heise.de/newsticker/meldung/BKA-70-Millionen-Euro-Schaden-durch-Cybercrime-im-Jahr-2017-4177083.html
- https://www.heise.de/thema/Cybercrime#liste
- https://www.unodc.org/unodc/en/cybercrime/index.html
- https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html
- https://sherloc.unodc.org/cld/v3/cybrepo/
- https://www.unodc.org/unodc/en/cybercrime/egm-on-cybercrime.html
- https://news.un.org/en/story/2018/05/1009692
- https://de.wikipedia.org/wiki/Internetkriminalit%C3%A4t
- https://de.wikipedia.org/wiki/Social_Engineering_(Sicherheit)
- https://de.wikipedia.org/wiki/CEO_Fraud
- https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2017.pdf

- https://www.heise.de/newsticker/meldung/Kommentar-zu-WannaCry-Staatliche-Dienste-muessen-Erkenntnisse-teilen-3713450.html
- https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html