Die hiesigen Behörden wurden im Zusammenhang mit den Eichmann-Unterlagen auch zu Akten bezüglich der Militärdiktatur in Argentinien von 1975 bis 1983 angefragt, da in Deutschland sowohl Flüchtlinge als auch Solidaritätsgruppen in diesem Zeitraum überwacht wurden. Auch deutsche Firmen in Argentinien waren dabei nicht unbeteiligt und der BND hält stets durch Residenten in den Botschaften Kontakt zu befreundeten Geheimdiensten und -polizeien, so auch in diesem Fall. Doch lediglich 200 BND-Seiten wurden freigegeben, von denen manche jedoch einen Verweis auf den Verfassungsschutz als Mitempfänger enthielten. Der Zugang zu den für die Freigabe nötigen Findmitteln (Kataloge) wurde jed
kann allerdings gerichtlich vorgeg

Um insgesamt mehr BND-Akter
dennoch tatsächlich gerechtfertigte Geheimhaltung zu wahren, kann die Geheimhaltungsbedürftigkeit durch den Senat in einem In-Camera-Verfahren geprüft werden, bei dem via Gerichtsverfahren Urkunden oder Akten im Einzelfall geprüft werden. Der BND versucht jedoch, bei den von Gaby Weber angeforderten Akten eine generelle Sperrerklärung des Kanzleramtes zu erwirken. Begründet wird dies mit der Notwendigkeit, die Vertrauensbasis zu erhalten, auf welcher die Geheimdienste jeweils miteinander arbeiten. Am ungestörten Fortbestehen dieser geheimen Informationsflüsse habe auch die BRD ein Interesse. In Argentinien allerdings hat sich die Regierung für eine Deklassifizierung ausgesprochen, sodass es gut möglich ist, dass eine Sperrerklärung des Kanzleramtes ausbleibt. Die Akten des BND zur *Colonia Dignidad* in Chile wurden zwar angeblich notvernichtet und im Bundesarchiv seien nur noch wenige Blätter zu finden, doch Gaby Weber gibt die Hoffnung nicht auf. Vielmehr kritisiert sie, dass all dies unter der Verantwortung des Kanzleramtes geschieht.

Die so vehemente Geheimhaltung von Akten wurde in der sich Webers Vortrag anschließenden Fragerunde klar verneint und zu deren umfassender Freigabe ein Volksentscheid vorgeschlagen. Gabi Weber stellt den Nutzen von Geheimdiensten insbesondere deshalb auch generell in Frage, weil journalistische Kor-
Regierung oft besser informieren
mit ihren jeweiligen unsäglichen
gen der Information überhaupt
mt, dass Geheimdienste wie der
BND sich größtenteils selbst vor allem aus öffentlichen Quellen informieren und das Geheimhalten von Informationen damit per se kaum begründbar ist. Drittens führt sie die Absurdität der auch internen Informationsfreigaben an: Etwa hat der Bundesrechnungshof keinen Zugang zu den Ausgaben der Dienste – eine adäquate Eigenkontrolle über Restaurantrechnungen und Bestechungsgelder für „Quellen“ erscheint allerdings doch sehr fragwürdig.

Webers Fazit für den souveränen Bürger und die souveräne Bürgerin: Wer Informationen von Behörden erhalten will, sollte die Gesetze nutzen, eine Rechtsmittelbelehrung verlangen und gegebenenfalls dafür auch vor Gericht ziehen.

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de

Sylvia Johnigk und Kai Nothdurft

We hate to say we told you so – IT-Sicherheit als Kriegshandwerk

IT-Sicherheit und Cyberwar stehen im Widerspruch zueinander, obwohl sich Militär und Geheimdienste Methoden und Wissen der IT-Sicherheit zunutze machen. Baut man Cyberwaffen und setzt sie ein, so schwächt man die Sicherheit der IT-Infrastruktur und daran angeschlossener Systeme. Für Cyberwaffen benötigt man geheim gehaltene Schwachstellen. Doch das Wissen um diese Schwachstellen bleibt nicht geheim, sondern gelangt irgendwann auch zu anderen nichtstaatlichen Kriminellen und gefährdet die IT-Sicherheit.

In unserem Vortrag auf der *FIfF-Konferenz 2016* am 27. November 2017 in Berlin haben wir exemplarisch gezeigt, wie Methoden und Werkzeuge der IT-Sicherheit zur (digitalen) Kriegsführung, dem Cyberwarfare verwendet werden. Dabei richteten wir den Blick sowohl zurück auf Prognosen, die wir in der Vergangenheit gestellt hatten, als auch in die Zukunft, mit neuen Prognosen, wie wir die weitere Entwicklung einschätzen. Wir zeigten anschließend Bezüge zwischen dem Tagungsthema *Unsichtbare Systeme* der FIfF-Konferenz 2016 und der digitalen Kriegsführung auf. Wir gaben Beispiele für teilweise Jahre zuvor von uns geäußerte Befürchtungen, die leider inzwischen eingetreten waren, bevor wir neue Prognosen stellten und einige bereits gestellte wiederholten. Schließlich erläuterten wir, warum Angriff im Cyberwarfare keineswegs die beste, sondern vielmehr eine schlechte Verteidigungsstrategie ist.

Schwachstellen

Unter Schwachstellen (engl. *vulnerabilities*) versteht man Eigenschaften eines IT-Systems, die Möglichkeiten bieten, in das System einzudringen oder eine ungewollte Veränderung vorzunehmen.

Wir sehen einige Ursachen für Schwachstellen in schlechtem Design und/oder mangelhafter Implementierung aufgrund von erheblichem Zeit- und Kostendruck. Dazu kommt Unwissenheit und mangelnde Qualifikation von Projektbeteiligten, insbeson-

dere von Entscheidern. Bei Kaufprodukten, Auftragsarbeiten und Outsourcing besteht in den seltensten Fällen eine Produkthaftung, was die Motivation schmälert, qualitativ ausgereifte Produkte zu liefern. Die Folgen von Sicherheitsmängeln tragen selten die Hersteller, manchmal sogar die Allgemeinheit.[1] Beispielsweise wurden einige von vielen Endanwendern genutzte Internet-Service-Dienstleister wie Twitter, Netflix, Spotify durch *Distributed-Denial-of-Service* (DDoS)-Attacken lahmgelegt, die durch unsichere Internet of Things (IoT)-Produkte anderer Hersteller möglich wurden.[2]

Kai Nothdurft und Sylvia Johnigk

Eine besonders gefährliche Quelle von Schwachstellen sind undokumentierte Funktionen oder versteckte Hintertüren in IT-Produkten.

Angriffe

Angriffe auf IT-Systeme können sehr unterschiedlichen Zielen dienen und unterschiedliche Schäden hervorrufen. Einige dienen der Spionage und Informationsgewinnung, bei gezielten Angriffen wird sogar kompromittierte IT in die Lieferkette eingeschleust.[3] Mit einem *Defacement*-Angriff werden die Inhalte und Darstellung von Webseiten verändert. Gegen die Verfügbarkeit richten sich *Denial-of-Service*-Attacken, aber auch weitergehende Sabotage-Angriffe, die bis zu physikalischen Schäden an der IT oder an von der IT gesteuerter Infrastruktur führen können.

Einige IT-Angriffe zielen auf Menschen selbst. Im *Information Warfare* werden *Social Bots* auch für Propaganda genutzt. Mit *Social-Engineering*-Attacken werden legitime Benutzer mit Trickbetrug dazu verleitet, dem Angreifer Zugriff auf das IT-System zu verschaffen.

IT-Angriffe gliedern sich typischerweise in mehrere Phasen: Sie beginnen mit der Informationsgewinnung, also dem Auskundschaften des anzugreifenden Systems. Neben einer Recherche von öffentlichen Quellen gehören dazu auch Port- und Schwachstellenscans. Danach erfolgt die Kompromittierung durch Ausnutzung einer Schwachstelle. Das System wird infiltriert, der Angreifer dringt ein. Hat sie oder er sich Zugang verschafft, ist das nächste Ziel, durch Privilegienerweiterung die vollständige Kontrolle zu erlangen und sich im System persistent festzusetzen. Ist der Zweck des Angriffs erreicht, werden zum Schluss noch die Spuren verwischt.

Verteidigung

Bei der Verteidigung gegen Angriffe gibt es präventive und detektive Methoden. Präventive Methoden greifen bereits vor dem Angriff und reduzieren die Angriffsfläche oder vermeiden Risiken. Dazu muss man seine IT-Systeme und die zu schützenden Informationen gut kennen, um sich auf die wichtigen Assets („Kronjuwelen“) konzentrieren zu können.

Die Ausfallsicherheit wird durch redundant ausgelegte Systeme erhöht. Segmentierung verringert die Vernetzung der Systeme untereinander und senkt die Querabhängigkeiten. Dadurch verringert sich die Komplexität (Fehleranfälligkeit) und die Größe der Angriffsfläche.

Eine sehr erfolgreiche Methode der Verteidigung ist die mehrschichtige Sicherheit (*security in depth*), bei der mehrere Sicherheitsmaßnahmen hintereinander greifen. Dies führt dazu, dass ein Angreifer mehrere Schutzmaßnahmen überwinden muss.

Häufig vernachlässigt wird ein effizientes, aktuelles und strukturiertes Identitäts- und Rechtemanagement. Nicht sauber gepflegte Zugriffsrechte bilden ein hohes Risiko.

Technische Maßnahmen wie die sichere Konfiguration von IT-Systemen (*Hardening*) oder das regelmäßige und zeitnahe Schließen von bekannt gewordenen Schwachstellen (*Patching*) müssen vollständig und mit der nötigen Sorgfalt durchgeführt werden. Regelmäßige Qualitätskontrollen wie Testen, Audits, Codereviews, Penetrationstests etc. ergänzen die obigen Maßnahmen.

Die wichtigsten Maßnahmen zur Detektierung von Angriffen, von deren Vorbereitung oder (zunächst) erfolglosen Versuchen bestehen im Aufzeichnen von sicherheitsrelevanten Ereignissen (*Logging*) wie Logon/Logoff, Veränderung von Zugriffsrechten und anderen Sicherheitsparametern. Diese „Spurensicherung“ muss aber durch regelmäßige Analyse dieser Log-Daten, durch Kontrolle und Überwachung (*Monitoring*) ergänzt werden. Der dafür nötige personelle Aufwand und die Reaktionszeiten können durch den Einsatz eines *Security Information and Event Management* (SIEM)-Systems reduziert werden. Ein SIEM-System analysiert Logfiles automatisch und reagiert regelbasiert auf Häufigkeit oder Kombination bestimmter Events durch Alarmierung. (Nur) auf bekannte Malware oder *Exploit*-Signaturen reagieren *Intrusion-Detection-Systeme* (IDS) mit Alarmen, *Intrusion-Prevention-Systeme* (IPS) blocken diese aktiv ab.

Eine besondere Form von Detektierungsmaßnahmen sind sogenannte *Honeypots*. Dabei handelt es sich um Systeme in größeren Netzwerken, die bewusst mit Schwachstellen versehen sind und Angreifern als leichte Beute erscheinen. Werden diese angegriffen, wird ein Alarm ausgelöst und die Aufmerksamkeit auf den Angreifer und seine Aktivitäten gelenkt.

Findet bereits ein Angriff statt, muss dieser abgewehrt werden; wenn er bereits erfolgreich war, sind Gegenmaßnahmen einzuleiten. Eine wichtige Basis dafür bilden klare Prozesse und Zuständigkeiten für das *Incident Handling* mit qualifiziertem Personal. Auch Krisenübungen dienen der Vorbereitung auf erfolgreiche Angriffe. Technisch kann mittels IPS oder Firewalls durch das gezielte Blocken der IP-Adressen, Geräte oder kompromittierter Accounts auf Angriffe reagiert werden.

Es gibt zudem Methoden, vermeintliche oder als tatsächliche Bedrohung identifizierte Systeme oder Benutzer zu bremsen. Gegen das automatisierte Durchprobieren von Passwörtern oder Denial-of-Service-Angriffe durch Logon-Versuche können *Captchas* eingesetzt werden, bei denen ein Rätsel gelöst werden muss, bevor der Logon erlaubt wird; nach Falscheingabe eines Passworts kann ein erneuter Eingabeversuch verzögert werden oder bestimmte Netzwerkverbindungen werden mit der Teergrubentechnik nur verzögert beantwortet.[4]

Von einigen im IT-Sicherheitsbereich arbeitenden Personen wird auch die Ansicht vertreten, dass das Angreifen eines identifizierten Angreifers zu den Verteidigungsmaßnahmen gehört. Durch Exploiten und Ausschalten greift man selbst das IT-System des vermeintlichen Angreifers mit einem Gegenangriff an und nennt dies Verteidigung. *Diese Ansicht wird von uns jedoch nicht geteilt.* Wir halten dies schon deshalb für extrem problematisch, weil insbesondere kurzfristig bei einer zeitnahen Gegenreaktion die tatsächliche Quelle eines Angriffs nicht zuverlässig identifiziert werden kann und die Wahrscheinlichkeit sehr hoch ist, dass nicht der eigentliche Angreifer, sondern ein von ihm als Angriffsbasis benutztes Opfersystem Ziel der Gegenmaßnahme wird. Dass Hacking-Angriffe nur schwer eindeutig einem Verursacher zugeordnet werden können, wird als *Attributierungsproblem* bezeichnet.

Häufig sind Verteidigungsmaßnahmen leider ineffizient. Dies liegt zum Teil daran, dass Maßnahmen falsch kombiniert oder mit einer inkonsequenten Strategie umgesetzt werden. Es gibt zahlreiche Standards und Prüfvorschriften, an denen sich Verantwortliche in Behörden und Unternehmen orientieren und die für offizielle Zertifizierungen verwendet werden. Problematisch wird dies, wenn ausschließlich auf die Einhaltung der Vorschriften geachtet wird, dabei aber wichtige Aspekte, die nicht explizit oder spezifisch gefordert sind, übersehen oder nicht berücksichtigt werden (*Security by Compliance (only)*). Ein plakatives Beispiel dafür war die Anschaffung einer Firewall, die dann aber gar nicht in Betrieb genommen wurde.

Ein weiteres Problem ist die Strategie, immer neue und teurere Security-Tools anzuschaffen, ohne gleichzeitig ausreichend viele qualifizierte Fachleute zu bezahlen, die diese auch bedienen können.

Außerdem existieren zahlreiche Produkte, die keine oder nur eine sehr eingeschränkte Schutzwirkung besitzen (*Snake-Oil*-Produkte), wie „Virenscanner" oder IDS-/IPS-Produkte, die ausschließlich signaturbasierte Malware-Erkennung verwenden und deshalb nur einen Bruchteil der Malware erkennen. Es existiert zudem eine Reihe von *Closed-Source*-Produkten, die mit herstellerabhängiger Beratung angeschafft oder implementiert werden, deren Schutzwirkung nicht überprüft werden kann. Dies ist insbesondere problematisch, wenn die Hersteller aus Staaten stammen, die nachweislich Wirtschaftsspionage oder Cyberwarfare betreiben, und damit von potenziellen Angreifern zur Kooperation genötigt werden können oder die Hersteller sogar deren strategische Partner sind.

NSA Strategic Partnerships, Folie aus den Dokumenten von Edward Snowden

Nebel des Krieges – unsichtbare Systeme

Die digitale Kriegsführung weist mehrere Bezüge zum Tagungsthema *Unsichtbare Systeme* auf: Schwachstellen werden geheim gehalten, um Exploits dafür in Cyberwaffen oder Staatstrojanern zu verwenden, infiltrierte Systeme dienen als stille Reserve von Angriffs-Bots, Überwachung und Spionage fanden lange unbemerkt und vor allem nicht offensichtlich und schwer wahrnehmbar statt. Die militärische Nutzung behindert eine freie IT-Sicherheitsforschung wegen der ihr zugrunde liegenden Geheimhaltungsinteressen. Die NSA hat heimlich offizielle Verschlüsselungsstandards geschwächt, indem mit Dual_EC_DRBG ein schwacher Zufallszahlen-Generator promotet wurde.[5]

Wie bereits erwähnt, werden häufig intransparente Sicherheitsmechanismen in Hardware und Closed-Source-Software eingesetzt oder absichtlich *Backdoors* in Hard- und Software zu Spionagezwecken oder *Lawful Interception* eingebaut. Mit der zunehmenden Verbreitung von IoT-Geräten können Schwachstellen in Haushaltsgeräten für DDoS-Angriffe genutzt werden, wobei die IoT-Geräte kaum als IT-Systeme wahrgenommen werden.

We hate to say, we told you so

Folgende unserer Befürchtungen (in kursiv) sind inzwischen leider eingetreten:

- *Jeder kann Opfer werden, auch Informatiker.innen und Administrator.innen (SIGINT 2012).* Admins der Belgacom wurden durch den GCHQ gezielt angegriffen.

- *Risiken steigen, kritische Infrastrukturen werden angegriffen:* Cyberwaffen gelten als nicht letal, die Einsatzschwelle ist niedriger, ein Cyberangriff gilt inzwischen als Bündnisfall

nach Art. 5 des NATO-Vertrags, *der Trend zum asymmetrischen Krieg wird verstärkt, besonders die industrialisierten Staaten sind durch Cyberwar bedroht*: Beispiel TV5-Hack.

- *Angriffe auf kritische Infrastrukturen:* fehlende, wegfallende Redundanz bei VoIP.

- *Attributierungsprobleme: Cyberattacken können* remote *aus großer Distanz, durch Anonymisierung oder indirekten Missbrauch von bereits kompromittierten Zwischensystemen Dritter ausgeführt werden, Spurenverwischung z. B. durch* Onion Routing *oder* Mixe*, keine physikalischen Spuren, nur Indizien, kein manipulationssicherer Nachweis möglich,* Information Warfare *beinhaltet auch Desinformation und Propaganda – das schließt ein, als Täter jemand anderen als den Angreifer zu diffamieren.* Nordkorea wird für den Angriff auf Sony verantwortlich gemacht, Russland für diverse Angriffe ohne handfeste Belege.

- *Risiken steigen, kritische Infrastrukturen:* In der *Shodan*-Suchmaschine für verwundbare Systeme tauchen französische Atomkraftwerke auf.[6]

- *IT-Insecurity: Informationssicherheit ist schwach verglichen mit steigenden Gesamtrisiken der IT:* Kein vertrauenswürdiges System, keine vertrauenswürdigen Komponenten, da (fast) alles kompromittiert und angreifbar ist, Hardware, Betriebssysteme, Lieferketten, Software.

- *Netzwerke sind verletzlich – durch falsche Bedienung oder Missbrauch.*

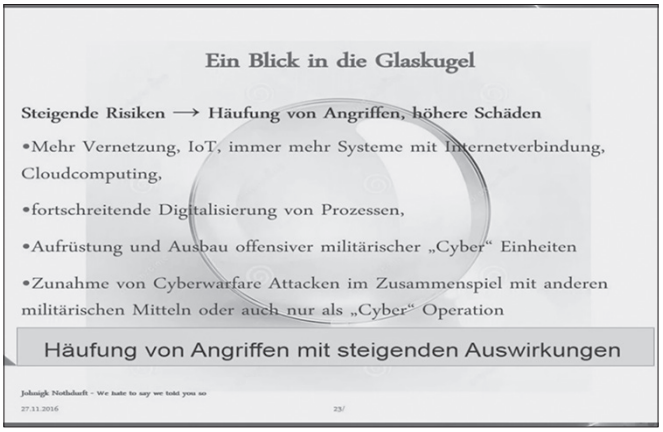
- *Ältere Internet-Protokolle oder -Dienste, die Angriffsfläche ist groß, Hardware und Software sind oft von außen angreifbar, IT-Projekte folgen der Zielsetzung in Budget, in Time, in Function, Verhinderung von unerwünschten Effekten (Absicherung gegen Angriffe) ist, wenn überhaupt, nur ein indirektes Ziel, das in Konkurrenz zu den anderen Projektzielen steht (Sigint 2012).* Der DDoS-Angriff auf Internet-Service-Dienstleister mittels IoT nutzte veraltete Protokolle und unsicher designte IoT-Geräte (siehe 2).

- *Vermischung von Cybercrime und Cyberwar, Kriminalität/Strafverfolgung und Cyberwarfare haben unterschiedliche Motivationen und unterschiedlich geeignete Gegenmaßnahmen (SIGINT 2012 Cyberpeace).* Es wird diskutiert, die Bundeswehr im Inneren zur Abwehr von Cyberangriffen einzusetzen und IT-Sicherheitsexperten aus der Wirtschaft zur Unterstützung zu verpflichten.

- *Illegales wird nachträglich legalisiert (INDECT Vortrag 2011).* Beispielsweise legalisiert das neue BND-Gesetz vormals illegale Praktiken.

Wir erwarten für die Zukunft folgende Entwicklungen:

1. *Das Gesamtrisiko steigt, da sich Angriffe häufen und jeweils höhere Schäden verursachen werden.*
   Ursachen dafür sind: eine immer stärkere Vernetzung bisher isoliert betriebener Systeme; Anschluss von schlecht gesicherten Haushaltsgeräten an das Internet (IoT), wodurch immer mehr Systeme mit Internetverbindung, aber ohne Security-Support existieren; Cloud-Computing-Lösungen als *Single Point of Failure* (SPOF) und attraktive Angriffsziele; fortschreitende Digitalisierung von Prozessen; Aufrüstung und Ausbau offensiver militärischer „Cyber"-Einheiten; Zunahme von Cyberwarfare-Attacken im Zusammenspiel mit anderen militärischen Mitteln oder auch nur als „Cyber"-Operation.



2. Es wird einen Trend zur Einschränkung freier Sicherheitsforschung geben. Das IT-Sicherheitsgesetz fordert akkreditierte IT-Sicherheitsunternehmen für die Beratung von KRITIS-Unternehmen (Betreiber kritischer Infrastrukturen). Nicht akkreditierte „Hackerbuden" oder unabhängige Untersuchungen werden dadurch benachteiligt. Anti-Hacking-Gesetze werden auf nationaler und internationaler Ebene ständig verschärft. Dies führt zu stärkerer Reglementierung (Erlaubnisvorbehalt für Sicherheitsüberprüfungen, Erhöhung des Strafmaßes, Absenkung der Strafbarkeitsschwelle). Dadurch wird eine unabhängige Sicherheitsanalyse und -forschung kriminalisiert.

3. Die aktuelle „Cyber"-Sicherheitspolitik der Bundesregierung und anderer Staaten gefährdet die IT-Sicherheit mehr als sie sie stärkt. Staatliche Stellen (BKA, Geheimdienste) kaufen weiterhin Schwachstellen für Staatstrojaner und Cyberwaffen. In vielen Staaten gibt es Einschränkungen in der Nutzung starker Kryptografie oder eine Pflicht zur Herausgabe von Schlüsseln (z. B. Frankreich, Großbritannien). Die Ausbildung von „Cyberkriegern" an den Bundeswehrhochschulen und das Verpflichten von Reservisten aus zivilen Bereichen für militärische Operationen führen dazu, dass diese Fachkräfte zur Verteidigung fehlen.

Risiken durch Geheimhaltung von Schwachstellen

Im letzten Teil des Vortrags erläuterten wir, warum wir die offensive Nutzung von Schwachstellen und Exploits für extrem gefährlich halten. Grundsätzlich erfordern *Zero-Day-Exploits* für Cyberwaffen geheim gehaltene Schwachstellen, um in offensiven Szenarios effektiv zu wirken. Geheimhaltung von Schwachstellen bedeutet aber gleichzeitig, dass nicht nur der Gegner, sondern auch die eigene Infrastruktur des offensiv agierenden Militärs sowie die Wirtschaft und Zivilgesellschaft des eigenen Landes gegenüber der Schwachstelle verwundbar bleiben (*Dual-Use-Dilemma*).

Geheim gehaltene Schwachstellen sind besonders gefährlich,

- da keine Gegenmaßnahmen ergriffen werden können, die Schäden vermeiden oder begrenzen,
- weil sie sehr lange existieren können,
- da sie sich dadurch in viele Implementierungen ausbreiten,
- da sie in Basiskomponenten eingebettet werden,
- da sie selbst bei Entdeckung dann nicht mehr kurzfristig beseitigt werden können, weil zu viele Abhängigkeiten bestehen und erheblicher Aufwand benötigt würde.

Ein weiteres Risiko besteht darin, dass behördliche Geheimnisträger die geheim gehaltenen Schwachstellen für „private" Zwecke verwerten können. Ihr „Marktwert" und die Replizierbarkeit stellen eine große Versuchung dar, sie weiter zu verkaufen. Wir wiesen bereits 2015 darauf hin, dass von staatlichen Stellen geheim gehaltenes Wissen um Schwachstellen nicht dauerhaft exklusiv und ausschließlich auf den Staat beschränkt bleibt (Conference Troopers, 19. März 2015). Im Oktober 2016 wurde bekannt, dass nach Snowden erneut ein NSA-Mitarbeiter Dienstgeheimnisse aus einem Zeitraum von 16 Jahren zu Hause gelagert hatte.[7] Ebenso erwähnten wir bereits 2010 das Risiko, dass Technologien auch an repressive Staaten geliefert werden könnten (SIGINT 2010 Indect, SIGINT 2012 Cyberpeace). 2015 wurde bekannt, dass die Firma *Hacking Team* über Jahre Spionagesoftware an autoritäre Staaten geliefert hatte.[8]

Angriff oder Verteidigung?

Schwachstellen veröffentlichen

Wir fordern deshalb, Schwachstellen zu veröffentlichen statt sie geheim zu halten. Es sollte sogar eine gesetzliche Pflicht zur Offenlegung bestehen. Dabei soll einer *Responsible Disclosure Policy* gefolgt werden, bei der den Verantwortlichen eine kurze Frist für die Behebung der Schwachstelle vor der Veröffentlichung eingeräumt wird, damit diese Patches bereitstellen und verteilen können. Das Melden von Schwachstellen an Behörden ist dabei nicht mit der geforderten Veröffentlichung zu vergleichen, solange die Behörden statt der Veröffentlichung auch die Geheimhaltung praktizieren.

Angriff ist nicht die beste, sondern schlechte Verteidigung

Wir kamen zu dem Schluss, dass Angriff im Cyberwarfare eine schlechte Verteidigung bedeutet:

- Krypto-Standards werden geschwächt (Dual_EC_DRBG in NIST),
- zahlreiche Systeme kompromittiert,
- um sie als Angriffs-Bot zu missbrauchen,
- oder um deren Informationen auszuspähen,
- Ressourcen und Knowhow werden für Angriffe statt für Verteidigung eingesetzt,
- freie Sicherheitsforschung wird behindert,
- Geheimhaltung von Schwachstellen verhindert das Patchen der eigenen Infrastruktur und den Schutz der Zivilgesellschaft des eigenen Landes,
- eine offensive Politik führt zu Eskalation und in eine Rüstungsspirale,
- und nationale Egoismen widersprechen globalem Handeln und internationaler Kooperation.

Rererenzen

1 *https://www.heise.de/security/meldung/DDoS-Untersuchung-Angriffe-werden-zum-Problem-fuer-die-Allgemeinheit-3631903.html*
2 *https://www.heise.de/newsticker/meldung/DDoS-Attacke-legt-Twitter-Netflix-Paypal-Spotify-und-andere-Dienste-lahm-3357289.html*
3 *Glen Greenwald: No Place to hide, S. 149, https://nsa.imirhil.fr/documents/no-place-to-hide.pdf*
4 *https://de.wikipedia.org/wiki/Teergrube_(Informationstechnik)*
5 *https://de.wikipedia.org/wiki/Dual_EC_DRBG*
6 *http://www.golem.de/news/it-security-atomkraftwerke-oft-ungeschuetzt-am-netz-1510-116694.html*
7 *https://www.heise.de/security/meldung/Juengster-NSA-Leak-16-Jahre-Geheimnisse-mitgenommen-3355278.html*
8 *https://netzpolitik.org/2015/hacking-team-wird-zu-hacked-team-400-gb-interne-daten-von-ueberwachungssoftware-hersteller-veroeffentlicht/*

Sylvia Johnigk und Kai Nothdurft

Sylvia Johnigk forscht und arbeitet seit über 25 Jahren im Bereich IT-Sicherheit, seit 2009 ist sie selbständige Beraterin in Großkonzernen. Ebenfalls seit 2009 ist sie im Vorstand des FIfF e. V.

Kai Nothdurft arbeitet als *Information Security Officer* in einer großen deutschen Versicherung. Seit 2009 ist Kai Nothdurft im Vorstand des FIfF e. V. aktiv. Seit Jahren hält er Vorträge und schreibt Artikel, die sich kritisch mit seinem Fachgebiet IT-Sicherheit beschäftigen.