Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Informatiksteuerungsorgan des Bundes ISB
Nachrichtendienst des Bundes NDB

Melde- und Analysestelle Informationssicherung MELANI
www.melani.admin.ch

INFORMATIONSSICHERUNG

LAGE IN DER SCHWEIZ UND INTERNATIONAL

Halbjahresbericht 2015/II (Juli – Dezember)

28. APRIL 2016

MELDE- UND ANALYSESTELLE INFORMATIONSSICHERUNG MELANI
http://www.melani.admin.ch

1 Übersicht / Inhalt

2 Editorial

MELANI: Fortsetzung der bisher geleisteten Aufgaben und Stärkung der Partnerschaft mit der Wirtschaft

Editorial von Jean-Pierre Therre, Executive Vice President / Head of Technology Risk & Business Continuity, Bank Pictet & Cie SA, Associate Fellow GCSP, Lead Lecturer UniGE

Die strategischen Ziele der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) mit deren Umsetzung MELANI beauftragt ist, sind die frühzeitige Erkennung der Bedrohungen und Gefahren im Cyberspace, die Reduktion der Cyberrisiken, besonders in den Bereichen Cyberkriminalität, Cyberspionage und Cybersabotage, sowie die Stärkung der Widerstandsfähigkeit der kritischen Infrastrukturen.

In diesem wichtigen Kontext, welcher die Stärkung der angemessenen operativen Widerstandsfähigkeit sämtlicher Akteure in Verwaltung und Privatwirtschaft umfasst, fokussiert MELANI sich mit Sorgfalt darauf, trotz immer noch zu limitierten Ressourcen, die gesteckten Ziele zu erreichen. Darüber hinaus unterstützt MELANI auch Initiativen verschiedener Sektoren mit dem Ziel den Austausch aussagekräftiger Informationen zwischen kritischen Infrastrukturen zu stärken.

Beispielsweise sind die halbjährlichen Treffen zwischen einer grossen Anzahl an Vertretern des Banken- und Finanzsektors zu wichtigen Anlässen geworden. Diese bieten für die teilnehmenden Experten die Gelegenheit, Informationen des ganzen Spektrums der Cyberbedrohung in der Schweiz und auch im Ausland in kondensierter Form zu erhalten.

Der Anlass « Swiss Cyber Risks 2015 », der von MELANI am 2. November 2015 im Berner Stade de Suisse organisiert wurde, widmete sich ebenfalls den Thematiken Informationsaustausch und Zusammenarbeit. Dank der Anwesenheit zahlreicher Experten aus den Bereichen Wirtschaft, Politik und Militär, konnten wertvolle Diskussionen mit dem öffentlichem Sektor und der Privatwirtschaft geführt werden

In der Tat erzielen all diese Anstrengungen in bester Weise den Ausbau eines echten Public Private Partnerships (PPP), welches von allen betroffenen Experten in diesem Bereich aufgrund der erwiesenen Zunahme, der zunehmenden Komplexität und der immer internationaler werdenden Cyber-Bedrohung gewünscht wird. Die präventiven, detektierenden und reaktiven Aktionen, sowie die Krisenbewältigung kann nicht durch isolierte Einheiten bewältigt werden, sondern vielmehr durch koordinierte und strukturierte Initiativen zwischen allen nationalen Akteuren. In diesem Sinne ist die Zusammenarbeit zwischen MELANI und dem Verein « Swiss Cyber Experts »[1] exemplarisch. Diese erlaubt es das Expertenwissen zu bündeln mit dem Ziel, im Falle eines ernsten Angriffs eine zielführende Diagnose zu liefern.

MELANI, unter der Leitung von Pascal Lamia, sei für Ihre verschiedenen Initiativen und ihrer wertvollen Arbeit bezüglich intersektorieller Koordination gedankt!

[1] https://www.swiss-cyber-experts.ch/ (Stand: 29. Februar 2016).

3 Schwerpunktthema: Der Umgang mit Sicherheitslücken

Direkt oder indirekt sind Internetnutzer dauernd irgendwelchen Sicherheitslücken ausgesetzt. Im Jahr 2015 wurden weltweit insgesamt 6419 Schwachstellen in die Datenbank von MITRE, eine non-profit Organisation, welche Schwachstellen systematisch erfasst, aufgenommen[2]. Für Schlagzeilen sorgten dabei allerdings nur die Wenigsten. Ebenfalls ist davon auszugehen, dass ein Teil der Sicherheitslücken nicht in dieser Datenbank vorhanden ist, weil diese den Herstellerfirmen, aus welchen Gründen auch immer, nicht gemeldet werden.

Auf der anderen Seite wird die Palette der ans Internet angeschlossenen Geräte, die auf Komponenten eines Betriebssystems und dazugehörige *Bibliotheken* zurückgreifen, immer breiter. Dadurch vergrössern sich auch die Auswirkungen und die Tragweite der einzelnen Sicherheitslücken. Viele dieser Systeme werden zudem in der Regel nicht automatisch auf den neuesten Stand gebracht. Hand aufs Herz: Wann haben Sie das letzte Mal die *Firmware* Ihres *Routers* erneuert oder die Software Ihres Internetradios auf den neuesten Stand gebracht? Fehlende oder nicht durchgeführte Updates bilden somit ein grosses Problem bei der steigenden Anzahl von Sicherheitslücken jedes Jahr.

3.1.1 Fehlende Update-Policies

In vielen Bereichen gehören automatische Updates mittlerweile zum Standard. Dass dies nicht überall der Fall ist zeigte die Sicherheitslücke «Stagefright», welche im Juli 2015 publik geworden ist, exemplarisch. Ein effizienter und schneller Update-Prozess für Android-Systeme fehlt. Da erstaunt es nicht, dass man in einer Studie von 2011 zum Schluss kam, dass 56% aller Android Smartphones unter einem veralteten Betriebssystem laufen.[3] Oft dauert es sehr lange, bis die Updates den Weg von Google zum Verbraucher finden. Grund hierfür ist, dass Google bei der Auslieferung der Updates sowohl auf die Smartphone-Hersteller wie Samsung oder LG als auch die einzelnen Mobilfunkanbieter angewiesen ist. Vor einer Verteilung müssen die Mobilfunkanbieter jeweils die Updates testen und zertifizieren, die Ihnen von den Herstellern angeboten werden. Im Gegensatz dazu kann Apple seine Updates direkt an die Kunden verteilen. Google kündigte nach diesem Vorfall einen monatlichen Update-Zyklus an. Einige Mobiltelefonhersteller wollen dieser Praxis folgen und sind im Gespräch mit den Netzbetreibern. Weitere Informationen zur «Stagefright»-Lücke finden sie in Kapitel 5.6.1.

Ein weiterer Problembereich sind die *Contentmanagementsysteme* (CMS). Für die grossen CMS sind zwar Updates in der Regel schnell vorhanden. Die Einspielmotivation der Betreiber lässt aber vielfach zu wünschen übrig. Dies wurde im letzten MELANI Halbjahresbericht eindrücklich gezeigt.[4]

---

2 http://www.cvedetails.com/ (Stand: 29. Februar 2016).

3 https://www.carbonblack.com/files/info-graphic-orphan-android/ (Stand: 29. Februar 2016).

4 Siehe Halbjahresbericht 1/2015, Kapitel 3 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2015-1.html (Stand: 29. Februar 2016).

3.1.2 Das lukrative Geschäft mit den Sicherheitslücken

Bevor aber eine Sicherheitslücke überhaupt geschlossen und ein entsprechender *Patch* hergestellt werden kann, muss diese dem Hersteller bekannt sein. Was so selbstverständlich klingt, ist nicht immer der Fall. Der Markt im Security Business ist hart umkämpft und der Umgang mit Informationen betreffend Sicherheit immer eine Gratwanderung. Da spielen verschiedene Interessen mit, natürlich auch finanzielle.

Der Angriff auf das italienische Unternehmen für Überwachungssoftware «Hacking Team» im Sommer 2015 und die anschliessende Veröffentlichung von vertraulichen Geschäftsdaten illustrierte dies eindrücklich. Neben Überwachungssoftware und persönlichen E-Mails wurden in den gestohlenen Daten auch diverse *Zero-Day Exploits* gefunden, welche die Firma «Hacking Team» eingekauft hatte. In einem Fall bezahlte das Unternehmen einem russischen Hacker 45‘000 Dollar für eine *Flash* Lücke.[5] Wem der russische Hacker die Lücke zusätzlich noch verkaufte, ist unbekannt.

Konkrete Geschäfte mit Überwachungssoftware, Spionage sowie die operative Seite von nationaler digitaler Aufrüstungspolitik werden nicht öffentlich diskutiert. Deshalb sind das Ausmass und die Menge der sich im Umlauf befindenden Zero-Days schwer abzuschätzen. Chaouki Bekrar, ehemaliger CEO und Chefhacker der Firma VUPEN, läuft dem Grundsatz dieser Verschwiegenheit entgegen. Bereits 2012 sagte Bekrar in einem Interview, dass er gefundene Sicherheitslücken auch für 1 Million Dollar nicht an den Hersteller der Software verkaufen würde, sondern ausschliesslich an seine eigenen Kunden – in seinem Falle spezifisch an NATO-Partner und NATO-Regierungen. Inzwischen hat Bekrar die Firma Zerodium gegründet, die sich ebenfalls auf die Überwachung von IKT-Geräten spezialisiert hat. Er schrieb in deren Namen 2015 einen mit 1 Million Dollar dotierten Wettbewerb aus, damit ihm Hacker eine Methode melden, wie man sich mittels *Jailbreak* unbemerkt auf iPads und iPhones mit dem neuesten Betriebssystem iOS 9.1 einhacken könne[6]. Er hatte damit Erfolg. Wie das Beispiel zeigt, folgt der Zero-Day Markt den gängigen Marktregeln: Je exklusiver eine Lücke ist, desto mehr wird dafür bezahlt.

Damit Forscher Sicherheitslücken an die Software-Hersteller melden und sie nicht meistbietend an Drittfirmen verkaufen, müssen einige Spielregeln definiert sowie entsprechende Anreize geschaffen werden. In der IKT-Sicherheitscommunity gibt es eine grosse Anzahl Personen, welche sich für die Formulierung solcher Best-Practices einsetzen und nicht finanziell davon profitieren wollen. Auf Seiten der Hersteller, denen Lücken gemeldet und die mit Patches Abhilfe schaffen sollten, scheint auch noch kein konsolidiertes Vorgehen absehbar. Wenn Hersteller allerdings die gemeldeten Schwachstellen nicht ernst nehmen oder noch schlimmer dem Melder sogar mit einer Anzeige drohen, ist es nicht erstaunlich, wenn solche Lücken unangekündigt veröffentlicht werden oder auf dem Zero-Day-Markt auftauchen, bevor ein Update vorhanden ist, das die Lücke schliesst.

Wie sensibel das Vulnerability Reporting (Schwachstellenreporting) sein kann, zeigt der Fall zwischen «FireEye», einem Sicherheitsdienstleister in den USA, und ERNW, einem IKT-Security Dienstleister mit Sitz in Heidelberg: Ein ERNW-Forscher fand fünf Sicherheitslücken

---

5 http://arstechnica.com/security/2015/07/how-a-russian-hacker-made-45000-selling-a-zero-day-flash-exploit-to-hacking-team/ (Stand: 29. Februar 2016).

6 https://www.zerodium.com/ios9.html (Stand: 29. Februar 2016).

im «Malware Protection System» von FireEye und meldete diese dem betroffenen Unternehmen. ENRW plante, diese Lücken nach einer Frist von 90 Tagen öffentlich zu machen. Was folgte, war ein Rechtsstreit über den Inhalt der Warnung zur Lücke, genannt Advisory, die ERNW veröffentlichen wollte. FireEye hatte die Befürchtung, dass zu viele Informationen über die Funktionsweise ihres Produktes im Advisory standen. ERNW wiederum argumentierte, dass diese Informationen für das Verständnis der Lücke notwendig seien. Zusätzlich sollte die Funktionsweise dieser Lücke an der Londoner Sicherheitskonferenz «44CON» präsentiert werden. FireEye hatte allerdings eine gerichtliche Verfügung erwirkt, so dass nur eine stark zensierte Version gezeigt werden konnte.

3.1.3 Responsible Disclosure

Verschiedene Länder und Softwarefirmen haben das Fehlen von Spielregeln und Prozessen erkannt und reagiert: Für das verantwortungsvolle Aufdecken von Sicherheitslücken haben sie sogenannte «Responsible Disclosure»-Prozesse entwickelt und Initiativen zur Identifizierung, Behebung und Bekanntmachung von Fehlern in Software, genannt *Bug Bounty*-Programme, ins Leben gerufen. Erwähnt sei beispielsweise das Bug Bounty-Programm von Microsoft und das schon im MELANI-Halbjahresbericht 2/2014[7] beschriebene «Responsible Disclosure»-Programm der niederländischen Regierung. Auf der Webseite government.nl[8] sind die genauen Schritte, beschrieben, welche nach einer Meldung veranlasst werden und was der Melder zu erwarten hat. Aber auch andere grosse Unternehmen wie Google, Facebook und Twitter unterhalten solche Programme. Neben der Definition der Spielregeln zwischen Forscher, Melder und betroffener Firma, welche beispielsweise die zeitliche Handhabung der Fehlerbehebung, die finanziellen aber auch die ideellen Aspekte beinhalten, ist für ein erfolgreiches Funktionieren ein Grundvertrauen nötig, das zuerst aufgebaut werden muss.

3.1.4 Rechtliche Lage in der Schweiz

Neben den aufgeführten freiwilligen Verhaltensregeln sind sicherlich auch klare gesetzliche Rahmenbedingungen notwendig. Dabei muss Sicherheitsforschern das Suchen solcher Schwachstellen weiterhin möglich sein, da nur so die Sicherheit der Programme verbessert werden kann. Ein Lösungsansatz dabei ist, dass nicht die Suche nach der Lücke im Fokus steht, sondern die anschliessende Verwendung einer solchen Sicherheitslücke. Auch das Schweizer Strafrecht stellt auf die Motivation des Akteurs ab: Strafbar macht sich nur, wer «Passwörter, Programme oder andere Daten, von denen er weiss oder annehmen muss, dass sie zur Begehung einer strafbaren Handlung […] verwendet werden sollen, in Verkehr bringt oder zugänglich macht […]»[9], respektive wer «Programme, von denen er weiss oder annehmen muss, dass sie [für Datenbeschädigung] verwendet werden sollen, herstellt, einführt, in Verkehr bringt, anpreist, anbietet oder sonst wie zugänglich macht oder zu ihrer

---

7 Halbjahresbericht 2/2014, Kapitel 5.5 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2014-2.html (Stand: 29. Februar 2016).

8 https://www.government.nl/topics/cybercrime/contents/fighting-cybercrime-in-the-netherlands/responsible-disclosure (Stand: 29. Februar 2016).

9 Art. 143bis Abs. 2 StGB: https://www.admin.ch/opc/de/classified-compilation/19370083/index.html#a143bis (Stand: 29. Februar 2016).

Herstellung Anleitung gibt […]»[10]. Entsprechend ist das Suchen von Sicherheitslücken zwecks Meldung an den Hersteller gemäss Schweizer Recht nicht strafbar. Auch der Austausch zwischen Sicherheitsforschern dürfte erlaubt sein. Hingegen ist die Veröffentlichung strafbar, da in dem Fall damit gerechnet werden muss, dass jemand die Lücke in strafbarer Weise ausnützt. Dem Veröffentlicher kann vorgeworfen werden, dass er dies billigend in Kauf nimmt und deshalb mit Eventualvorsatz agiert. Insofern kann man in der Schweiz einem Hersteller nicht mit der (detaillierten) Veröffentlichung einer Lücke drohen, um Druck zu machen, dass er sie schliesst. Es steht einem Forscher demgegenüber frei, in allgemeiner Form über die Existenz einer gefundenen Lücke im Internet zu berichten und dort auch allfällig nicht zufriedenstellendes Verhalten des Herstellers zu monieren.

Inwiefern von einem Hersteller ein Entgelt für das Auffinden und Melden der Sicherheitslücke gefordert werden kann, ist demgegenüber (noch) nicht etabliert und müsste wohl durch Rechtsprechung präzisiert werden. Infrage käme hier insbesondere die «Geschäftsführung ohne Auftrag»[11] respektive die Entstehung einer Obligation aus ungerechtfertigter Bereicherung[12], da der Hersteller eine Leistung erhält. Ob ein Forscher jemals einen solchen Rechtsstreit mit einem Hersteller lanciert, und damit einem Gericht die Gelegenheit zur Stellungnahme gibt, darf indes bezweifelt werden: Sicherheitsforscher dürften in ihren Augen «Besseres zu tun» haben, als sich mit Anwälten und Gerichten herumzuschlagen.

---

10 Art. 144bis Ziff. 2 StGB: https://www.admin.ch/opc/de/classified-compilation/19370083/index.html#a144bis (Stand: 29. Februar 2016).

11 Art. 419 ff. OR: https://www.admin.ch/opc/de/classified-compilation/19110009/index.html#id-2-14 (Stand: 29. Februar 2016).

12 Art. 62 ff. OR: https://www.admin.ch/opc/de/classified-compilation/19110009/index.html#id-1-1-3 (Stand: 29. Februar 2016).

4 Lage national

4.1 Cyberspionage in der Schweiz

Dieses Kapitel enthält keine Details über Schweizer Spionagefälle, anhand derer spezifische Vorfälle oder Ziele identifiziert werden können. Grund dafür ist die Anonymität, die dem Opfer und der Informationsquelle in den meisten Fällen zugesichert werden. Es wäre aber auch im Hinblick auf die Interessen des Wirtschaftsstandorts, des Staats und der getroffenen Abwehrmassnahmen kontraproduktiv solche Informationen preiszugeben. Dennoch stellt diese Übersicht die Situation der Schweiz umfassend dar. Sie baut auf Informationen auf, die aus verschiedenen in der Schweiz laufenden Fällen der letzten sechs Monate zusammengetragen wurden.

Bevor eine Typologie der beliebtesten Angriffsziele entwickelt werden kann, muss zunächst festgestellt werden, welche Arten von Informationen in den Augen eines potentiellen Angreifers von Wert sein könnten. Wir beschränken uns hier auf Angriffe, die für einen Staat von Nutzen sind. Daher können wir annehmen, dass vor allem Informationen von Interesse sind, die einem Staat beim Erreichen seiner strategischen Ziele hilfreich sein könnten. Oft handelt es sich dabei um die politische Agenda (insbesondere geplante Verhandlungen oder die Überwachung von politischen Oppositionellen im Ausland), Sicherheitsfragen (Terrorismus), militärische oder für manche Staaten auch wirtschaftliche Programme (insbesondere Innovationen, Knowhow, Details zu Handelsbeziehungen).

Weil sich auf schweizerischem Staatsgebiet viele Organisationen befinden, die diesbezüglich interessante Informationen besitzen, ist die Schweiz ein beliebtes Ziel für Cyberangriffe. Man denke insbesondere an die zahlreichen ausländischen Vertretungen, internationalen Organisationen und Gemeinschaften, die für viele Staaten von politischem Interesse sind. Aber auch das Wissen ganzer Wirtschaftszweige sowie Informationen zu deren Handelsbeziehungen oder zu laufenden Angeboten könnten verschiedenen wirtschaftlichen Akteuren aus anderen Ländern einen beträchtlichen Wettbewerbsvorteil bringen. Zudem dient die Wirtschaftsspionage in vielen Ländern einer umfassenden politischen Agenda und lässt sich manchmal sogar mit Sicherheitsüberlegungen rechtfertigen.

Cyberangriffe, die auf die Beschaffung solcher Informationen abzielen, richten sich gegen unterschiedliche Arten von Opfern. Ein Angreifer kann natürlich beschliessen, den Inhaber dieser Informationen selbst zum Ziel seiner Angriffe zu machen. Erweist sich dieses Ziel aber beispielsweise als sehr schwer zugänglich, kann der Angreifer auch in zwei Schritten vorgehen und versuchen, zunächst einen Dienstleister zu schädigen, um dadurch an sein eigentliches Ziel heranzukommen. Genau aus diesem Grund wurden 2014 und 2015 Hotels in der Genferseeregion dazu benutzt, um die dort untergebrachten Delegationen während der Verhandlungen zum Nuklearabkommen mit dem Iran abzuhören[13]. In anderen Fällen richten sich die Angriffe gegen Wartungsfirmen, die Zugang zum gesicherten Bereich eines

[13] MELANI Halbjahresbericht 1/2015, Kapitel 4.1.1 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2015-1.html (Stand: 29. Februar 2016).

Unternehmens haben, oder gegen Telekomanbieter, wie beispielsweise der Angriff gegen BICS BELGACOM gezeigt hat, der 2013 aufgedeckt wurde[14].

Manchmal gehören auch Unternehmen oder Personen zu den „kollateral“ Geschädigten und haben mit den Angriffen überhaupt nichts zu tun. Es kann sogar vorkommen, dass Dritte nur infolge eines Fehlers bei der Zielbestimmung oder anderer ungeplanter Effekte von Spionagefällen betroffen sind. Beispielsweise wurde 2015 ein Unternehmen aus dem Weinsektor mit einer Malware infiziert, die der Cyberspionage diente. Da die Absichten der Angreifer bekannt waren, ergaben die Abklärungen schnell, dass sich das Opfer in die Kategorie «Kollateralschaden» zuordnen liess.

Schlussfolgerung/ Empfehlung:

Cyberspionage gegen schweizerische Interessen ist eine Realität. In den vergangenen MELANI Halbjahresberichten wurde bereits über verschiedene Fälle berichtet. Auch der Jahresbericht des Nachrichtendienstes des Bundes (NDB) gibt einen Überblick über die Situation. Dabei ist Prävention eine wichtige, wenn nicht die wichtigste, Komponente im Kampf gegen Spionage. Hierbei ist der erste und wichtigste Schritt für ein Unternehmen. die Erkenntnis, dass es sich um eine reale und nicht um eine hypothetische Gefahr handelt. Zahlreiche Fälle, von denen MELANI Kenntnis erhielt, bestätigen dies. Damit Spionage effizient bekämpft werden kann, muss zudem der Informationsfluss gewährleistet sein. Werden Spionagefälle gemeldet, können Behörden Massnahmen ergreifen und die wesentlichen Erkenntnisse in ihrer Gesetzgebung oder auf politischer Ebene umsetzen. Vor allem aber können andere Organisationen dank diesen Informationen allfällige Angriffe auf ihre Systeme erkennen. Für die Behörden hat natürlich die vertrauliche Behandlung der Daten oberste Priorität.

MELANI setzt sich in Partnerschaft mit verschiedenen privaten Einheiten seit 10 Jahren für den Schutz vor IT-Gefahren ein. Zur Meldung von Vorfällen im Bereich der Informationssicherung stellt MELANI auf ihrer Website ein Meldeformular zur Verfügung:

MELANI Meldeformular:

https://www.melani.admin.ch/melani/fr/home/meldeformular/formulaire.html

Der Nachrichtendienst des Bundes (NDB) führt mit seinem Programm Prophylax eine Präventions- und Sensibilisierungsaktion im Bereich der Nonproliferation und der Wirtschaftsspionage durch. Sie dient zur Sensibilisierung von Unternehmen und Bildungsinstitutionen:

Programm Prophylax:

http://www.vbs.admin.ch/internet/vbs/de/home/documentation/publication/snd_publ.html

[14] MELANI Halbjahresbericht 2/2013, Kapitel 4.1
https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2013-2.html

4.2 Industrielle Kontrollsysteme

Mit dem Internet der Dinge dringt die Informations- und Telekommunikationstechnik (IKT) – und damit vernetzte industrielle Kontrollsysteme (IKS) – in immer weitere Bereiche unseres täglichen Lebens vor. Somit gewinnen Cyber-Risiken auch in diesen Anwendungsgebieten an Relevanz und Aktualität. In diesem Halbjahresbericht widmen wir uns kritischen Systemen, welche im Zusammenhang mit Mobilität stehen.

4.2.1 Offenes Parking-Management

Gebäudeautomation ist ein Teilbereich von Kontrollsystemen, den die meisten von uns täglich bewusst oder unbewusst nutzen. Ein Anwendungsgebiet in grösseren Gebäudekomplexen stellt das Parking-Management dar. Von der einfachen vernetzten Parkuhr bis hin zum stadtumspannenden Parkleitsystem kommen *IKS-Systeme* zum Einsatz. Im Oktober 2015 wurde MELANI über eine im Internet frei einsehbare Parking-Management-Oberfläche in der Schweiz informiert. Die Belegung der einzelnen Parkplätze war so für jedermann, jederzeit publik. Einbrecher könnten so beispielsweise feststellen, wann die Räumlichkeiten am ehesten leer stehen werden oder Mitarbeiter nicht zu Hause sind.

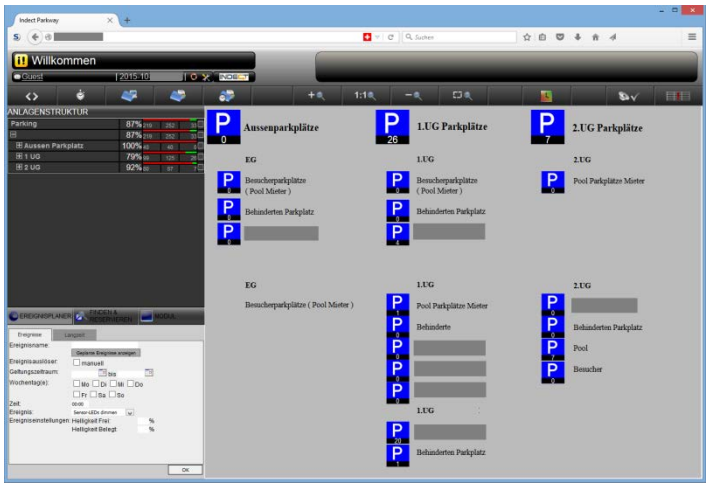

Abbildung 1: Screenshot Parkmanagement-Weboberfläche

Der Betreiber wurde von MELANI umgehend über den Sachverhalt und die potenzielle Gefährdung in Kenntnis gesetzt.

4.2.2 Verwundbare Bahninfrastruktur

Auch bei Transportsystemen wie den immer stärker mit IKT vernetzten Eisenbahn-Infrastrukturen kommen industrielle Kontrollsysteme zum Einsatz. Sie werden beispielsweise verwendet, um Signale zu steuern und Weichen zu stellen. Am 32. «Chaos Communication Congress», der vom 27.-30. Dezember 2015 in Hamburg stattfand, zeigte die russische Gruppe «*SCADA*-Strangelove»[15] allerhand mögliche Angriffe auf verschiedenste Infrastrukturen der Eisenbahnen: So lassen sich neben offensichtlichen Informationssystemen für Zugreisende auch automatisierte Stellwerke,

15 https://blog.kaspersky.com/train-hack/10946/ (Stand: 29. Februar 2016).

Überwachungskameras und Solarstationen entlang der Strecke ohne grossen Aufwand auffinden. Häufig sind solche Systeme verwundbar, weil der physische Zugang zu ihnen zu wenig gesichert ist, die Systeme und die eingesetzten Sicherheitsmechanismen veraltet sind oder weil öffentlich bekannte Standardpasswörter verwendet werden. Um Ausrüster und Anwender in dieser Problematik zu sensibilisieren und davon zu überzeugen, keine solche Standardpasswörter einzusetzen, veröffentlichte die Gruppe eine Liste mit 37 Anbietern von häufig eingesetzten Kontrollsystemkomponenten wie Server und *Switches,* deren Standardpasswörter im Internet kursieren – darunter war auch ein Schweizer Hersteller von Eisenbahn-Routern und *VPN*-Lösungen.

Schlussfolgerung/ Empfehlung:

Wir lassen uns mit dem öffentlichen Verkehr befördern und bestellen Güter online, die am besten am Folgetag bei uns eintreffen sollen. Die Logistik von und um uns wird immer effizienter. Dies ist nur durch intelligente Transportsysteme aber auch roboterunterstützte Lagerbewirtschaftung möglich. Mit der stärkeren Vernetzung von Alltagsgegenstände, werden Industrielle Kontrollsysteme in ihrer ganzen Ausprägung ein immer wichtigerer Bestandteil unseres täglichen Lebens.

Dadurch sind auch immer mehr Personen von den Risiken betroffen, die damit einhergehen. MELANI bietet auf ihrer Website eine Checkliste mit Massnahmen zum Schutz industrieller Kontrollsysteme an:

DOKU

Checkliste mit Massnahmen zum Schutz industrieller Kontrollsysteme:

https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/massnahmen-zum-schutz-von-industriellen-kontrollsystemen--ics-.html

4.3 Angriffe auf Websites: DDoS, Defacements

Privatpersonen und Unternehmen in der Schweiz sind weiterhin das Ziel verschiedener Arten von Angriffen. Ein Angriffsziel stellen insbesondere Websites dar. Vor allem für Unternehmen, die auf eine verlässliche Präsenz im Internet angewiesen sind, kann sich die Verwundbarkeit gegenüber *DDoS-Angriffen* und *Defacements* als problematisch erweisen. Im zweiten Halbjahr 2015 wurden vermehrt Angriffe auf Websites als Mittel zum Zweck beobachtet, um anschliessend Schadsoftware zu verbreiten.

4.3.1 Werbenetzwerke

Angreifer suchen immer wieder nach Möglichkeiten, möglichst viele Geräte potenzieller Opfer auf einfache Art und Weise infizieren zu können. Früher setzten sie vor allem E-Mails ein mit darin enthaltenen Links oder Anhängen. Der Versand solcher E-Mails benötigt wenig technisches Wissen. Die Erfolgsaussichten nehmen jedoch laufend ab, weil Internetnutzer besser sensibilisiert sind und nicht mehr auf jeden Anhang oder Link klicken. Zusätzlich hat eine solche E-Mail-Kampagne eine grosse Sichtbarkeit zur Folge und die zu verbreitende Schadsoftware landet sehr schnell in den Datenbanken der Antivirenhersteller. Deshalb gewinnen heute Website-Infektionen, so genannte *Drive-By-Infektionen,* als Verbreitungsmethode von Schadsoftware immer mehr an Bedeutung. Um eine grossflächige Verbreitung von Schadsoftware zu erreichen, hacken Kriminelle mit Vorliebe Websites mit

grosser Reichweite. Besonders beliebte Ziele sind dabei Portale von Zeitungen sowie sogenannte Werbenetzwerke. Die Spezialität von Werbenetzwerken ist es, Werbeinhalt zentral zu verwalten und dann an eine Vielzahl von Kunden wie beispielsweise Online-Zeitungen auszuliefern. Eine Infektion auf einem dieser zentralen Systeme kann deshalb gravierende Auswirkungen haben und zu einer grossen Zahl an Infektionen führen.

Gleich zwei solche Fälle wurden MELANI in der aktuellen Berichtsperiode zur Kenntnis gebracht:

4.3.1.1 Webseiten-Infektion auf Tageszeitung

Eine erste Infektion wurde MELANI am 11. September 2015 von einem Sicherheitsforscher gemeldet. Ein Schweizer Werbenetzwerk führte die Besucher auf das *Exploit-Kit* «Niteris». Das Werbenetzwerk wird auch von einer Seite verwendet, welche die Online-Ausgaben diverser Tageszeitungen beliefert. Deshalb dürfte die Zahl potenzieller Opfer entsprechend hoch gewesen sein. Besuchte ein Internetnutzer eine Webseite mit dieser kompromittierten Werbeeinblendung, ermittelte die Schadsoftware zunächst die Spracheinstellungen des Endgerätes. Waren diese Deutsch oder Französisch, wurde der Computer nach Schwachstellen im Internet Explorer (z. B. CVE-2014-6332), Firefox (z.B. CVE-2013-1710), Java (z.B. CVE-2013-2465) oder Adobe Flash (z.B. CVE-2015-5119) untersucht. Während die Sicherheitslücken der Browser von 2013 respektive 2014 stammten und somit relativ alt waren, war für diejenige von Adobe Flash erst seit dem 7. Juli 2015 ein Update verfügbar. Computer, welche diese Programme nicht auf dem aktuellsten Stand hatten, wurden infiziert. Bei der installierten Schadsoftware handelte es sich um die bekannte E-Banking-Schadsoftware «GOZI ISFB», die durch verschiedene kriminelle Gruppen betrieben und weltweit für Angriffe auf Finanzinstitute verwendet wird. Eine Woche später, am 18. September 2015 begannen die Kriminellen unerwartet, die Schadsoftware auf den infizierten Computern wieder zu löschen. Die Gründe für dieses Vorgehen können vielfältig sein. Allenfalls hatte die Gruppe bemerkt, dass die Operation aufgeflogen war und wollte damit die Rückverfolgung erschweren.

Schlussfolgerung:

Neben all den Vorteilen und der Kosteneinsparung, die eine Zentralisierung von Webinhalten bietet, sollte sich jede Firma auch der damit verbundenen Risiken bewusst sein. Ausser der Gefahr von Schadsoftware-Infektionen auf Computern der Websitebesucher besteht bei einem Vorfall auch das Risiko des Vertrauensverlustes in die Firma.

Zwingend sollte das Vorgehen im Falle von kompromittierten Inhalten von Drittanbietern schon im Vorfeld definiert sein. Hat die Firma Zugriff auf die Drittinhalte, respektive kann sie diese im Notfall beeinflussen und unterbinden? Vor allem sollten schon im Vorfeld die Kontakte zu den IKT-Sicherheitsabteilungen der Drittfirmen abgeklärt und etabliert werden. Dadurch können die richtigen Leute bei einem Vorfall zeitnah benachrichtigt und rasch geeignete Gegenmassnahmen eingeleitet werden.

4.3.1.2 TV-Medienportal ebenfalls betroffen

Ein weiterer Vorfall aus dieser Kategorie betraf ein TV-Medienportal. Dort wurde am 3. Dezember 2015 ebenfalls eine Website-Infektion festgestellt, welche allerdings das «Angler

Exploit Kit» auslieferte. Die Infektion beschränkte sich auch hier nicht nur auf die Website. Der Inhalt der manipulierten Webseite wurde auch mit Medienpartnern anderen Online-Zeitungen geteilt, darunter eine Gratiszeitschrift. Dies erhöhte die Reichweite und den potenziellen Opferkreis erheblich. Glücklicherweise war nur eine Unterseite betroffen. MELANI informierte die Betreiber der Website, damit der Schadcode entfernt werden konnte.

Webseiten-Infektionen oder sogenannte Drive-By-Infektionen gehören mittlerweile zum Standardrepertoire der Angreifer, um möglichst viele Geräte zu infizieren. Das in diesem Vorfall verwendete «Angler-Exploit Kit» trat Ende 2013 zum ersten Mal in Erscheinung und erfreut sich seither steigender Beliebtheit bei den Angreifern. In der Regel ist die Vorgehensweise der verschiedenen Tätergruppen fast identisch: Das Exploit Kit selbst prüft das Zielgerät oft mit JavaScript auf die installierten Plug-Ins und ihre Versionen, um eine Sicherheitslücke zu finden und diese mit dem passenden Exploit anzugreifen. Interessant ist, wie rasch die entsprechenden Exploit Kits beim Erscheinen von neuen Sicherheitslücken über passende Exploits verfügen. Dabei verfügen nicht alle Exploit Kits über dieselben Exploits, es gibt eine relativ grosse Variation. Darüber hinaus kommt es immer öfter vor, dass die Exploit Kits selbst über 0-day Exploits verfügen.

4.3.2 Defacement auf LeMatin.ch : Virus IRAQ

Der Inhalt von Drittanbietern sorgte in einem weiteren Fall für Schlagzeilen: Auf der Website der Fernsehzeitschrift von «lematin.ch» wurde am 8. Juli 2015 ein Bild einer islamischen Hackergruppe mit dem Namen «Virus IRAQ» eingeblendet.[16] Gehackt wurde allerdings nicht «Le Matin» selbst, sondern der eigentliche Anbieter «Guide Loisirs», der Webseiteninhalte für verschiedene Kunden ausliefert. Beim Angriff handelt es sich nicht um einen gezielten Angriff, sondern um eine unspezifische Webseitenverunstaltung, genannt Defacement, die täglich tausendfach passiert. Die sich in diesem Fall bekennende Gruppe «Virus IRAQ» ist schon länger aktiv. Laut der Website zone-h.org, die diese Art von Angriffen erfasst, hat die Gruppe im Jahr 2015 über 300 Webseiten auf diese Weise angegriffen. Die Ziele werden dabei zufällig ausgewählt. So befinden sich angegriffene Webseiten unter anderem in der Ukraine, den Niederlanden, Deutschland, Frankreich, Tschechien und der überwiegend grosse Teil in den USA.

Schlussfolgerung:

Websites werden dauernd und systematisch nach Sicherheitslücken durchforscht. Wird eine gefunden wird diese auch ausgenützt. Oft werden bei den Defacements politische oder religiöse Inhalte eingeblendet. Zudem herrscht ein Wettbewerb zwischen den einzelnen Aktivistengruppen, wer die meisten Angriffe durchgeführt hat.

4.3.3 Übernahme von IP-Adressen. Grundsätzliches zur BGP Problematik

Das Internet besteht aus Zehntausenden von Netzwerken (sogenannten «*autonomen Systemen*» – kurz «AS»), die miteinander verbunden sind und Datenpakete untereinander

[16] http://www.tagesanzeiger.ch/digital/internet/Hacker-platzieren-SchockBilder-auf-Website-von-Le-Matin/story/27762519 (Stand: 29. Februar 2016).

austauschen können. Für den Austausch dieser Informationen wird ein Protokoll mit dem Namen *Border Gateway Protocol (BGP)* verwendet, das den Routern mitteilt, über welche Route, welche Netzwerke erreichbar sind. Das Protokoll ist beinahe so alt wie das Internet selbst und wurde zuletzt 1991 überarbeitet (RFC 1269). Leider hat das Protokoll seit jeher seine Schwächen. Beispielsweise können Angriffe unter Vorspiegelung falscher Identitäten (sogenannte *Spoofing*-Angriffe) durchgeführt werden. So ist es jedem AS möglich zu behaupten, Besitzer eines Netzwerkes zu sein, auch wenn ihm das propagierte Netzwerk überhaupt nicht gehört. Es gibt aus technischer Sicht keine Möglichkeit zu überprüfen, ob eine Route legitim ist oder nicht. Die AS vertrauen also darauf, dass der Gesprächspartner nur korrekte Routen propagiert.

Spamhaus, einer der weltweit grössten Sperrlisten-Provider, informierte MELANI im letzten Jahr gleich zweimal, dass Adressräume von Schweizer AS «übernommen» und von Spammern für den Versand von *Spam* E-Mails verwendet wurden. Der erste Fall wurde MELANI im Juni 2015 gemeldet, als der Adressraum eines Kantons entführt wurde. Der zweite Fall ereignete sich im September 2015, als Teile des Adressraumes einer Pharmafirma entführt wurden. In beiden Fällen informierte MELANI die betroffene Organisation.

Empfehlung:

Falls Sie einen eigenen öffentlichen Adressraum besitzen, empfehlen wir Folgendes:

- Stellen Sie sicher, dass das zu Ihrem Adressraum gehörende Objekt bei Ihrer Regional Internet Registry (RIR) z. B. RIPE aktuell ist und eine gültige *Abuse Mailbox* besitzt.
- Falls Sie einen Adressraum besitzen, den Sie derzeit nicht popagieren, empfehlen wir Ihnen, diesen zu propagieren, selbst wenn Sie diesen derzeit nicht verwenden. Dies erschwert den Spammern das Entführen von ungebrauchten Adressräumen.
- Verwenden Sie ein BGP-Monitoring für Ihre Adressräume, um benachrichtigt zu werden, falls ein fremdes AS Ihren Adressraum propagiert. Es gibt kommerzielle Firmen, welche solche Dienstleistungen anbieten, falls Sie dies nicht selber tun wollen oder können.

Weitere Informationen zur Problematik bei BGP und IP Übernahme finden Sie im GovCERT.ch Blog:

INFO

GovCERT.ch Blog:

http://www.govcert.admin.ch/blog/11/cantonal-ip-space-in-switzerland-hijacked-by-spammers

4.3.4 Erpressung mittels DDoS: Nach DD4BC kommt Armada collective

Auch im zweiten Halbjahr 2015 war Erpressung eine beliebte Praktik der Cyber-Kriminellen, die auf einen schnellen finanziellen Gewinn aus sind. Neben den mittlerweile zahlreichen Familien von Verschlüsselungs-Schadsoftware (s. Kapitel 4.5.1 dieses Halbjahresberichts) wurde erneut mittels *DDoS-Angriffen* versucht, die Verfügbarkeit von Websites zu stören und

dann von einem Opfer Geld zu erpressen. Nachdem Mitte 2015 vor allem die Gruppe «DD4BC» aktiv war, tauchte in der zweiten Hälfte des Jahres die Gruppe «Armada Collective» auf. Die beiden Gruppen gingen identisch vor. Die Angriffe von Armada Collective waren unter anderem gegen E-Mail und Hosting-Provider gerichtet. Besonders der Angriff im November 2015 auf «Protonmail», einen Schweizer Anbieter verschlüsselter E-Mail-Kommunikation, machte dabei auch international Schlagzeilen.

DDoS-Angriffe sind schon lange bekannt. In 2015 häuften sich rein finanziell motivierte Angriffe. Die Täter suchten sich dabei vornehmlich Unternehmen aus, bei deren Geschäftsmodell die Verfügbarkeit der Website besonders wichtig ist und die deshalb ein entsprechendes Erpressungspotenzial aufweisen. Unter dem Druck einer drohenden Nichterreichbarkeit der eigenen Website und der Hoffnung auf eine «schnelle» Lösung, ziehen einige Unternehmen auch eine Zahlung in Betracht. Mit einer Zahlung gibt man den Tätern jedoch finanzielle Mittel, um ihre Angriffsinfrastruktur zu stärken und die Angriffe zu intensivieren. Ausserdem gibt es keine Garantie, dass die Angriffe nach erfolgter Zahlung aufhören. Oft verwenden Angreifer sogenannte *Booter- oder Stresser-Dienste*. Dies sind Werkzeuge, welche gegen Bezahlung DDoS-Angriffe auslösen (ein «DDoS as a service»). Je mehr Geld ein Angreifer zur Verfügung hat, desto mehr Angriffsvolumen (sowohl in Bezug auf die Intensität wie auch in Bezug auf die Länge) kann er sich bei einem solchen Dienstleister beschaffen. Werden keine Lösegelder bezahlt, verfällt hingegen das Geschäftsmodell der Verbrecher. Die Lösegeldzahlung ist somit höchstens eine kurzfristige Symptombekämpfung ohne Garantie und trägt nicht zur langfristigen Resilienz der eigenen Infrastruktur sowie der Sicherheit des Internets gegenüber DDoS-Angriffen bei.

Empfehlung:

Trifft ein DDoS-Angriff eine Firma unvorbereitet, ist es meistens zu spät, um rasch und effizient reagieren zu können. Gerade bei Internet-Diensten deren Webauftritt den eigentlichen Verkaufskanal bildet, muss notgedrungen die Sicherung dieses höchst kritischen Geschäftsprozesses absolute Priorität geniessen. Deshalb sollte in erster Linie eine Strategie für den Fall einer DDoS-Attacke entwickelt werden. Die zuständigen internen und externen Stellen sowie weitere Personen, die im Falle eines Angriffs agieren können, müssen bekannt sein. Idealerweise befasst sich ein Unternehmen im Rahmen des allgemeinen Risikomanagements schon vor einem Angriff auf Stufe der Geschäftsleitung mit der DDoS-Problematik und etabliert auf Betriebsebene eine gewisse DDoS-Abwehrbereitschaft. Ein DDoS-Angriff kann jede Organisation treffen. Sprechen Sie mit Ihrem Internet-Anbieter über Ihre Bedürfnisse und angemessene Vorkehrungen. Eine vollständige Checkliste und Anleitung mit Massnahmen gegen DDoS-Angriffe finden Sie auf den Seiten von MELANI:

Checkliste und Anleitung mit Massnahmen gegen DDoS-Angriffe:

https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/massnahmen-gegen-ddos-attacken.html

4.3.4.1 Angriff auf Protonmail

Eine Ausnahme, sowohl bezüglich Publizität als auch bezüglich oben beschriebener Vorgehensweise, bildete der DDoS-Angriff auf den E-Mail-Provider «Protonmail». Dieser von

CERN-Forschern entwickelte E-Mail-Dienst bietet *End-to-End-Verschlüsselung* an. Die Firma wurde im Jahre 2013 aufgrund der Enthüllungen rund um Edward Snowden gegründet. Der Hauptsitz ist in Genf und die Firma wird durch Crowdfunding finanziert.[17]

In der Nacht auf den 3. November 2015 registrierte Protonmail DDoS-Angriffe auf seine Systeme. Vermutet wurde, dass «Armada Collective» für die Angriffe verantwortlich sei. Danach folgten gemäss den Aussagen von Protonmail täglich weitere Angriffe. Dies ist untypisch für Armada Collective: Die Gruppierung beschränkt sich normalerweise auf einen einzigen Demonstrationsangriff und hofft auf die umgehende Einschüchterung des Opfers und auf dessen Zahlung. Protonmail ging allerdings in den ersten Tagen davon aus, dass es sich nur um einen einzigen Angreifer handelte. Diese Angriffe hatten kollaterale Auswirkungen auf andere Kunden im Rechenzentrum. Man entschied sich, nach Rücksprache mit diesen Firmen, zur Zahlung des Lösegelds. Erst als die Angriffe nach der Bezahlung nicht aufhörten und sich sogar Armada Collective selbst von den Angriffen distanzierte, ging man bei Protonmail von einem zweiten Angreifer aus.[18]

Von Anfang an kommunizierte Protonmail sehr offen über die Vorkommnisse und es wurde der Verdacht geäussert, dass ein Staat hinter den Angriffen stecken könnte[19]. Dies konnte allerdings nie bewiesen werden. Jedoch liegt die Vermutung nahe, dass ein Trittbrettfahrer die Situation ausgenützt hat. Die vom ersten Augenblick an offene Kommunikation über die DDoS-Angriffe könnte mit ein Grund gewesen sein, dass ein Trittbrettfahrer von diesem Angriff erfuhr, die Gelegenheit ausnutzte und parallel zu Armada Collective ebenfalls sein Unwesen trieb.

4.3.4.2 Verhaftung bei DD4BC

Viele der im Jahr 2015 beobachteten DDOS-Erpressungsversuche gingen auf das Konto der Gruppe DD4BC (DDoS for BitCoin). Am 15. und 16. Dezember führte das High-Tech Crime Department der Republik Srpska (Entität von Bosnien Herzegowina) eine Operation mit dem Namen «Pleiades» gegen die Gruppe DD4BC durch. Begleitet wurde die Operation von Polizeibeamten diverser Europäischer Länder und von Europol. Die Aktion wurde von Österreich initiiert und vom European Cybercrime Center (EC3) unterstützt. Auch die Schweiz unterstützte diese Operation, welche zur Verhaftung des mutmasslichen Kopfes der Bande und einer weiteren Person geführt hat. Ein 32-jähriger bosnischer Staatsangehöriger steht unter Verdacht, eine führende Rolle bei DD4BC gespielt zu haben.

4.3.5 Anonymous-Drohung in Lausanne

Internationale Bekanntheit erhielt die lose Gruppierung «Anonymous» vor allem im Zusammenhang mit grossen und internationalen Auseinandersetzungen wie beispielsweise der Verteidigung der Aktivitäten des WikiLeaks-Gründers, Julian Assange, oder dem aktuellen Konflikt mit «ISIS»-Sympathisanten im Internet (siehe hierzu auch Kapitel 5.4.2 des aktuellen Halbjahresberichtes). Dass es bei Anonymous nicht nur um internationale Themen

---

17 https://en.wikipedia.org/wiki/ProtonMail (Stand: 29. Februar 2016).

18 https://protonmaildotcom.wordpress.com/2015/11/05/protonmail-statement-about-the-ddos-attack/ (Stand: 29. Februar 2016).

19 https://twitter.com/ProtonMail/status/661683054866429798 4 (Stand: 29. Februar 2016).

geht, zeigte ein Beispiel aus der Westschweiz, welches im Juli 2015 für Schlagzeilen sorgte. Eine Gruppe mit dem Namen «Anonymous Schweiz» drohte der Stadt Lausanne mit einem Hackerangriff auf ihre IKT-Systeme, wenn diese nicht mehr Rücksicht auf die Bewohner des Hochhauses «Tour de la Sallaz» nehmen. Hintergrund dieser Drohung waren Emissionen, welche durch Bauarbeiten ausgelöst wurden und unter denen die Bewohner des Hochhauses gelitten haben sollen. Gegen die Drohung wurde Klage eingereicht. Zudem wurden Vorkehrungen getroffen, um die IKT der Stadt gegen Angriffe zu schützen.

Schlussfolgerung:

Ob diese Drohung tatsächlich mit der Anonymous-Bewegung in Verbindung steht oder es jemand war, der sich unter zu Hilfenahme des Namens Anonymous eine grössere Wirkung erhoffte, wird sich nur schwierig klären lassen, da es sich bei Anonymous nicht um eine definierte Gruppe handelt. Die lockere Anbindung resultiert in einer Reihe unkoordinierter, mehr oder weniger spektakulärer Ankündigungen und Angriffe. Da es strukturinhärent keine Mitgliedschaft bei Anonymous gibt und keine offiziellen Sprecher oder sonst wie für die gesamte Bewegung verantwortliche Personen existieren, kann prinzipiell jeder im Namen von Anonymous Mitteilungen veröffentlichen und so ein Medieninteresse generieren.

4.4 Social Engineering, Phishing

Neben den technischen Angriffen sind auch Methoden, welche die menschlichen Schwächen ausnützen, bei den Angreifern beliebt.

4.4.1 Phishing-Statistik

In den vergangenen Jahren ist die Zahl der durch MELANI bearbeiteten Anfragen bezüglich *Phishing* stark angestiegen. Um die Vielzahl der eingehenden Meldungen betreffend Phishing effizienter bearbeiten zu können, hat MELANI im Jahr 2015 die Website «antiphishing.ch» aufgeschaltet, auf welcher Phishing-Seiten gemeldet werden können. Insgesamt wurden im ersten Jahr 2500 Phishing-Seiten gemeldet, wobei die Anzahl über die Zeit stark variiert. Die Gründe hierzu sind sehr verschieden: Zum einen gibt es ferienbedingte Schwankungen, da in der Ferienzeit weniger Phishing-Seiten gemeldet werden (und auch die Angreifer in die Ferien gehen). Zum anderen verschieben die Angreifer ihre Angriffe regelmässig von Land zu Land.

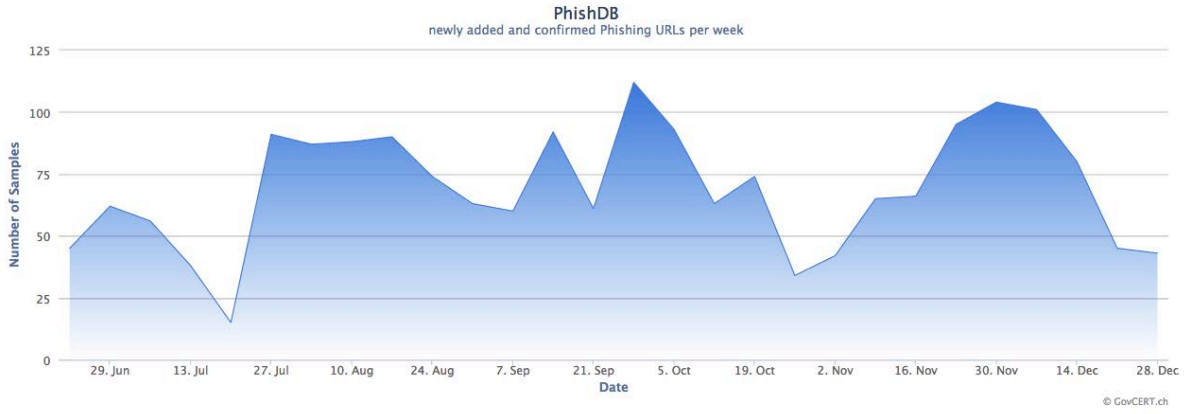

Abbildung 2: Gemeldete und bestätigte Phishingseiten pro Woche auf antiphishing.ch

4.4.2 Logo der Bundesverwaltung gleich mehrfach missbraucht (Teil 1)

Das Logo der Schweizer Bundesverwaltung erfreut sich bei Betrügern grosser Beliebtheit. Gleich zweimal wurde dieses für Phishing und einmal für Malware-Verbreitung (siehe auch Kapitel 4.5.2) missbraucht. Die Angriffe gingen dabei nicht gegen die Bundesverwaltung. Die missbräuchliche Verwendung des Logos hatte alleine den Zweck, den Opfern Seriosität vorzugaukeln.

Auch im zweiten Halbjahr 2015 versuchten Betrüger wiederholt, als Bundesamt für Energie (BFE) getarnt, per E-Mail an Kreditkartendaten von Internet-Nutzenden zu gelangen. Die ersten Fälle wurden bereits 2014 beobachtet. Die Empfänger wurden dabei mit einer angeblichen Rückerstattung geködert, die ihnen noch zustehen würde. Um die Auszahlung zu ermöglichen, sollte man sich auf die angegebene Webseite begeben. Auf der täuschend echt aussehenden Webseite wurde jedoch nicht nur Name und Adresse verlangt, sondern auch die Kreditkartennummer inklusive Verfallsdatum und Prüfziffer.

In einem zweiten Fall wurde Ende September 2015 ein weiteres Mal der Name der Eidgenössischen Steuerverwaltung (ESTV) missbraucht. Die Betrüger versuchten, per E-Mail an Konto- und Kreditkarteninformationen sowie an Kopien von Pässen von Steuerpflichtigen zu gelangen. Die ESTV wurde hier missbräuchlich als Absender verwendet.[20]

4.4.3 Phishing mit Werbung

Seit April 2015 beobachtete MELANI eine neue Vorgehensweise bei Phishingangriffen gegen Schweizer Finanzinstitute. Hacker versenden dabei keine Phishing E-Mails mehr, sondern schalten kostenpflichtige Werbe-Anzeigen bei Suchmaschinenbetreibern wie Google, Yahoo oder Bing. Zu diesem Zweck kaufen die Betrüger Stichworte (Keywords) bei den Suchmaschinenbetreibern, die im Zusammenhang mit dem angegriffenen Finanzinstitut stehen: Haben es die Phisher beispielsweise auf Kunden der «Bank XY» abgesehen, schalten diese Phishing-Werbeanzeigen für das Stichwort «XY» oder «XY Bank».

Werbeanzeigen in Suchmaschinen werden üblicherweise zuoberst und gut sichtbar vor den eigentlichen Suchresultaten angezeigt. Die Wahrscheinlichkeit, dass ein Benutzer anstelle des tatsächlichen Suchresultats auf die Werbeanzeige klickt, um auf die Seite der «Bank XY» zu gelangen, ist also gross.

[20] https://www.estv.admin.ch/estv/de/home/allgemein/aktuell/warnung--phishing.html (Stand: 29. Februar 2016).

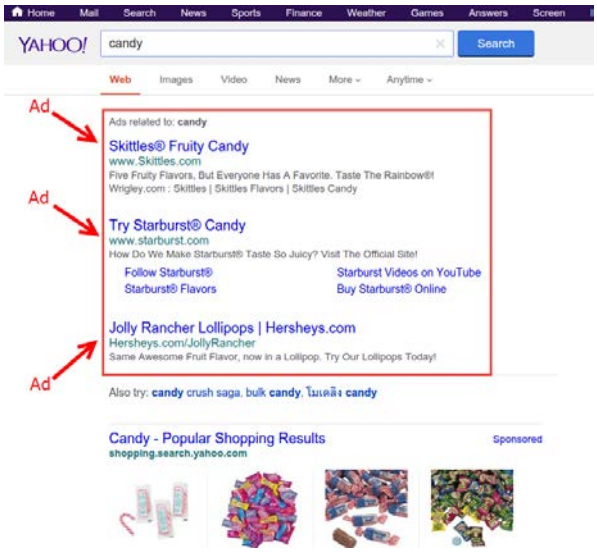

Abbildung 3: Beispiel einer Werbeanzeige auf Yahoo

Diese Tatsache machen sich Betrüger zu Nutze, um ahnungslose Internet-Benutzer auf Phishing-Webseiten zu leiten. Phishing-Angriffe mittels Werbeanzeigen auf bekannten Suchmaschinen haben aber noch weitere Vorteile für die Angreifer:

- Es ist für IKT-Sicherheitsdienstleister und *CERTs* schwierig, Phishing-Werbeanzeigen auf Suchmaschinen als solche zu identifizieren.
- Die Angreifer müssen sich keine Sorgen um Spam-Filter oder zuverlässige Empfänger-E-Mail-Adresslisten machen, da bei dieser Vorgehensweise keine E-Mails zum Einsatz kommen.
- Zumindest einige der Suchmaschinenbetreiber führen keine oder eine ungenügende Prüfung der Neukunden durch, so dass Angreifer jederzeit ein neues Benutzerkonto auf der Werbeplattform eröffnen können, um betrügerische Werbeanzeigen zu schalten.

MELANI trat mit allen drei grossen Suchmaschinenbetreibern in der Schweiz in Kontakt, um die Problematik anzugehen. Tatsächlich waren zwei der drei grössten Suchmaschinenbetreiber von den beschriebenen Phishing-Angriffen betroffen.

Empfehlung:

Weitere Informationen zu Phishing mittels Werbeanzeigen finden Sie im GovCERT.ch Blog:

INFO

GovCERT.ch Blog:

http://www.govcert.admin.ch/blog/16/ads-on-popular-search-engine-are-leading-to-phishing-sites

4.4.4 Phishing mit PDF-Dateien

Eine weitere Vorgehensweise, welche MELANI im zweiten Halbjahr 2015 vermehrt beobachtete, war Phishing unter Zuhilfenahme von PDF-Dateien. Dazu werden die üblichen Phishing-E-Mails versendet. Jedoch enthalten diese anstelle eines HTML-Links, welcher jeweils auf die eigentliche Phishing-Webseite verweist, einen Dateianhang mit der Dateiendung .pdf. Die PDF-Datei enthält Anweisungen, die das Opfer dazu verleiten, auf den in der PDF-Datei angegebenen Link zu klicken. Dieser führt dann zu der eigentlichen Phishing-Webseite.

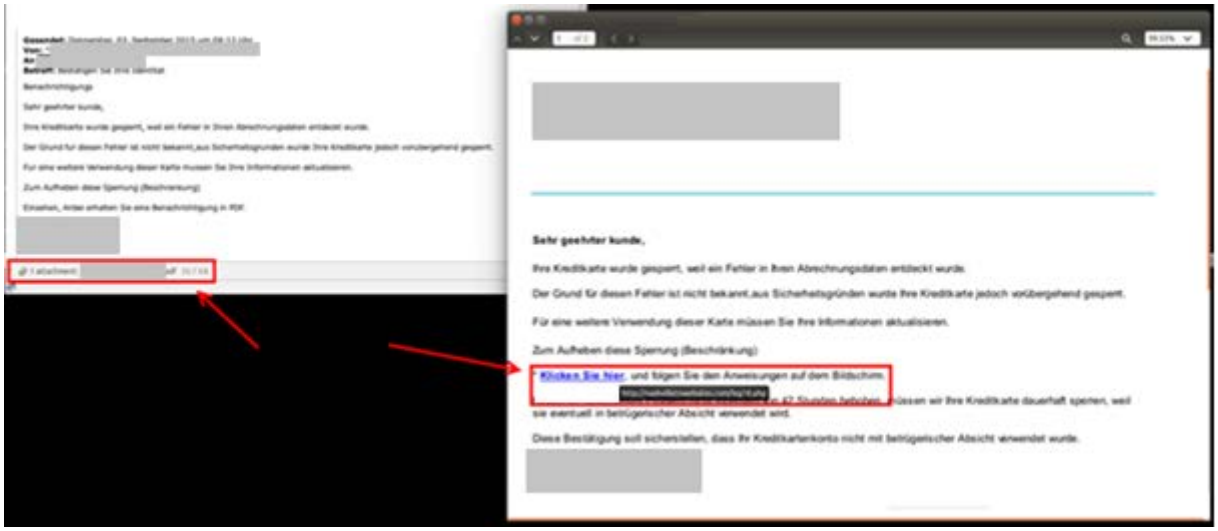

Abbildung 4: Beispiel E-Mails mit Link auf ein einen Dateianhang mit der Dateiendung .pdf

Schlussfolgerung:

Während es für den Empfänger einer Phishing-E-Mail keinen grossen Unterschied macht, ob die Phishing-Seite direkt in der Phishing-E-Mail oder in einem Dateianhang versteckt ist, birgt diese neue Praktik einen wichtigen Vorteil für die Angreifer: Durch Verwendung von PDF-Dateien werden E-Mail-Filter ausgehebelt, die in der Regel nur in der E-Mail selbst nach gefährlichem Inhalt Ausschau halten. Internetkriminelle scheinen dies realisiert zu haben und setzen daher vermehrt auf diese Masche.

4.5 Crimeware

Crimeware ist eine von Wirtschaftskriminellen weiterentwickelte Form der Schadsoftware, die kriminologisch zur Computerkriminalität zählt und rechtlich unter Internetbetrug anzusiedeln ist. In Sachen Crimeware sind E-Banking-Trojaner weiterhin sehr verbreitet, wie die untenstehende Statistik zeigt. Bei einem Grossteil der infizierten Systeme in der Schweiz, die MELANI gemeldet worden sind, handelt es sich um E-Banking-Trojaner wie «Torpig», «Dyre», «Tinba», «Gozi» oder «ZeuS». Nachdem im ersten Halbjahr «Tinba» die verbreitetste E-Banking-Schadsoftware war, hat im zweiten Semester 2015 «Gozi» diese unrühmliche Trophäe erhalten. Dies dürfte unter anderem mit der im Kapitel 4.3.1 beschriebenen Verbreitungsmethode über infizierte Werbenetzwerke zusammenhängen. Der grösste Teil an Infektionen geht aber wie im ersten Halbjahr 2015 immer noch auf das Konto von «Downadup» (auch bekannt als «Conficker»). Der Wurm existiert bereits über acht Jahre und verbreitet sich über eine im Jahr 2008 entdeckte und ebenso lange geschlossene Sicherheitslücke in Windows Betriebssystemen.

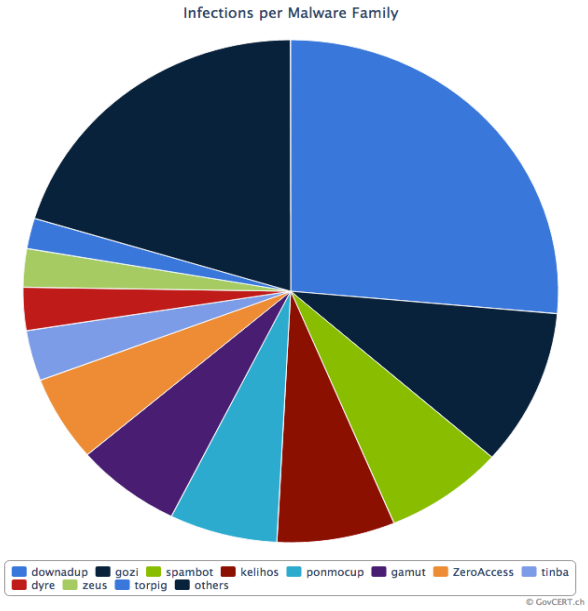

Abbildung 5: Verteilung der Schadsoftware in der Schweiz, welche MELANI bekannt ist. Stichtag ist der 31.Dezember 2015. Aktuelle Daten finden Sie unter: http://www.govcert.admin.ch/statistics/dronemap/

Wie im ersten Halbjahr 2015 weisen die beiden Kantone Zürich und Wallis auch im zweiten Halbjahr eine höhere Infektionsrate auf als andere Kantone (unter Berücksichtigung der Anzahl Einwohner). Während bei Zürich die höhere Rate auf eine hohe Computerdichte zurückzuführen sein dürfte, ist der Grund der Infektionsrate im Kanton Wallis momentan nicht ersichtlich.

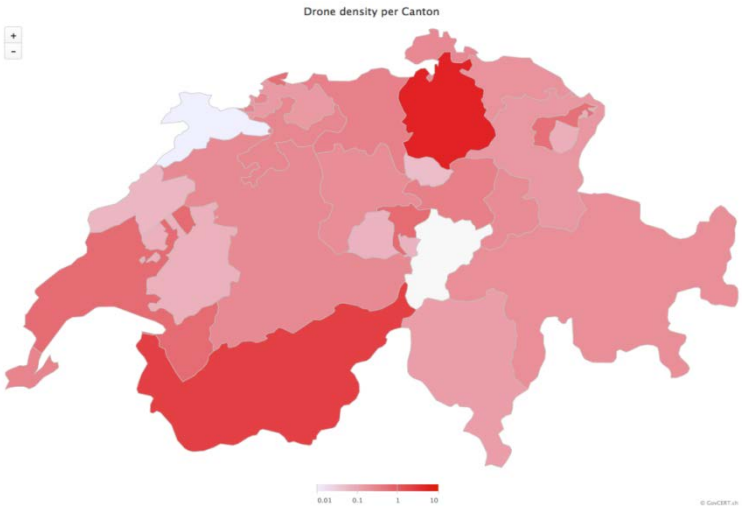

Abbildung 6: Anzahl Infizierungen pro Kanton unter Berücksichtigung der Einwohnerzahl. Stichtag ist der 31.Dezember 2015. Aktuelle Daten finden Sie unter: http://www.govcert.admin.ch/statistics/dronemap/

4.5.1 Verschlüsselungstrojaner – weiterhin stark verbreitet

Auch im zweiten Halbjahr 2015 gab es etliche Meldungen, über Krypto-Trojaner. Dabei handelte es sich meist um Fälle mit der *Ransomware* «Teslacrypt», aber auch Fälle mit anderen Trojaner-Familien wie beispielsweise «Cryptowall» wurden MELANI gemeldet. Betroffen sind sowohl Privatpersonen als auch Firmen sämtlicher Branchen und Grössen. Wer im Falle eines Angriffs vorgängig kein oder nur ein veraltetes Backup zur Hand hat, verliert alle oder zumindest einen Teil der Daten.

Empfehlung:

Auf dem Computer abgelegte Daten sollten regelmässig auf externe Speichermedien kopiert werden (*Backup*). Diese sollten nur während des Backupvorgangs am Computer angeschlossen sein und an einem sicheren Ort aufbewahrt werden.

INFO

Massnahmen gegen Verschlüsselungstrojaner:

https://www.melani.admin.ch/melani/de/home/themen/Ransomware.html

4.5.2 Logo der Bundesverwaltung gleich mehrfach missbraucht (Teil 2)

Gemäss der Koordinationsstelle zur Bekämpfung der Internetkriminalität KOBIK beim Bundesamt für Polizei (fedpol) wurden Anfang Juli 2015 mittels E-Mail und angeblichem Absender fedpol die Empfänger aufgefordert, auf einer Webseite Dokumente einer fiktiven Gerichtsverhandlung herunterzuladen. Eine weitere Betrugswelle wurde im Januar 2016 beobachtet. Der Text war so gewählt, dass der Empfänger eingeschüchtert und unter Zeitdruck gesetzt wird: Für Personen, die innerhalb von 15 Tagen die gewünschten Daten nicht zur Verfügung stellen, werde die Gerichtsverhandlung in deren Abwesenheit stattfinden. Der Link führte auf eine Fälschung der Internetseite von fedpol. Der Anwender wurde anschliessend aufgefordert, einen Sicherheitscode (*Captcha*) einzugeben und Dateien herunterzuladen. Wer die Anweisungen der Webseite bzw. E-Mail befolgte, installierte jedoch unwissentlich die Verschlüsselungsschadsoftware «Cryptolocker» auf seinem Gerät.

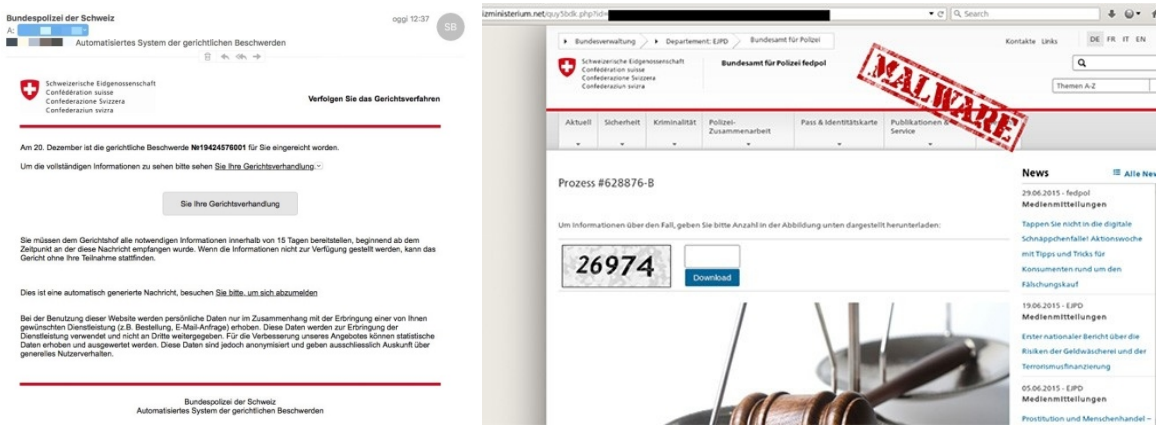

Abbildung 7: Missbrauch der Webseite des Bundesamtes für Polizei für die Verbreitung des Verschlüsselungstrojaners «Cryptolocker» Quelle: KOBIK/fedpol

Anfang Februar 2016 wurde bei einer weiteren Betrugsvariante das Logo des Bundesamtes für Polizei missbraucht und dem Internetbenutzer der Bildschirm/Browser gesperrt. Diesem wurde vorgeworfen, sich illegaler Aktivitäten auf dem Internet schuldig gemacht zu haben. Mit einer Geldbusse, zahlbar mit einer «PaySafeCard», könne der Browser wieder entsperrt und eine Strafverfolgung umgangen werden. Solche Fälle tauchten in den letzten Jahren immer wieder auf. Im Gegensatz zum vorgängig erwähnten Krypto-Trojaner handelt es sich um eine nicht sehr professionelle Betrugsvariante. Je nach Betriebssystem und Browser lässt sich das gesperrte Browser-Fenster wieder schliessen und es kann verhindert werden, dass die zuletzt besuchten Seiten automatisch wieder geöffnet werden (damit sich der Vorgang nicht wiederholt). Bitte konsultieren Sie hierzu die Anleitung der betroffenen Software. Bei Windows beispielsweise erfolgt die Schliessung über den Task-Manager (Ctrl-Alt-Del).

Nicht nur Desktop- oder Laptop-Computer sind von den Browservarianten betroffen. Zunehmend wird auch festgestellt, dass durch die Täterschaft Code mit der gleichen Funktionalität auch für Mobile-Browser von Geräten wie Smartphones und Tablets eingebaut werden.

Abbildung 8: Gefälschte Sperrseite mit dem Logo des Bundesamtes für Polizei Quelle: KOBIK/fedpol

4.5.3 E-Banking-Trojaner: Retefe und Tinba

Ende November 2015 hat sich MELANI in Absprache mit ihren Partnern und den betroffenen Finanzinstituten dazu entschlossen, die vom E-Banking-Trojaner «Retefe» verwendete *Command&Control-Infrastruktur* abzuschalten. MELANI hat dazu bei den verantwortlichen Hosting-Providern und Domain-Registraren im Ausland interveniert und diese darum gebeten, die von Retefe verwendeten Server und Domainnamen abzuschalten. Vom Takedown betroffen waren über 30 Server und Domain-Namen in Europa. MELANI konnte in den darauf folgenden Wochen weder Neuinfektionen noch neue Spamwellen im Zusammenhang mit Retefe feststellen. Der *Botnet* Takedown erwies sich als Erfolg, bis Ende Dezember 2015 neue Spamwellen auftauchten, welche mit denjenigen identisch waren, die in den Monaten zuvor im Zusammenhang mit Retefe beobachtet worden waren. Eine Analyse des Dateianhanges lieferte jedoch überraschende Ergebnisse: Bei der verwendeten Schadsoftware (Malware) handelte es sich nicht etwa um Retefe, sondern um einen anderen weit aus bekannteren E-Banking-Trojaner namens «Tinba» (auch bekannt unter dem Namen «Tiny Banker»). Die Gruppierung hinter Retefe hat also offensichtlich das Tatwerkzeug gewechselt und verwendet seit Dezember 2015 Tinba und damit eine neue Command&Control-Infrastruktur.

Die beiden Trojaner, Retefe und Tinba, unterscheiden sich wesentlich: Während Retefe offenbar eine Eigenentwicklung der Angreifer war und ausschliesslich für E-Banking-Betrug in der Schweiz, Österreich, Schweden und vereinzelt auch Japan eingesetzt wurde, handelt es sich bei Tinba um ein bekanntes «*Crimeware Kit*», welches in Untergrundforen verkauft wird. Ein weiterer Unterschied ist die Funktionsweise der beiden Trojaner: Während Retefe die DNS- oder Proxy-Einstellungen des befallenen Computers ändert, nistet sich Tinba im System ein und kommuniziert regelmässig mit einer zentralen Command&Control-Infrastruktur. Dies erlaubt es den Urhebern, jederzeit auf den Computer des Opfers zuzugreifen und über diesen E-Banking-Betrug zu begehen.

4.5.4 Botnetz: Dridex / Bugat

Im Oktober 2015 führte die US-Justiz zusammen mit dem FBI einen Schlag gegen das «Bugat»-Botnetz durch. Bugat, besser bekannt unter dem Namen «Dridex», ist ein E-Banking-Trojaner, der Kunden von dutzenden Finanzinstituten auf der ganzen Welt im Visier hat. Die US-Justiz beschuldigte einen 30-jährigen Moldawier, das Botnetz administriert zu haben. Trotz den Versuchen des FBI, das Bugat-Botnetz zu stören und die involvierten Personen zu verhaften, ist Bugat bis heute aktiv und versucht auch heute noch täglich, Geräte ahnungsloser Internet-Benutzenden in den USA und Europa mit Hilfe von Spam-Kampagnen zu infizieren.

Empfehlung:

MELANI empfiehlt Internetbenutzenden, keine verdächtigen E-Mail-Anhänge zu öffnen, auch wenn diese von vermeintlich vertrauenswürdigen Absendern stammen. Zusätzlich sollte sichergestellt werden, dass ein Virenschutz installiert ist und dieser stets auf dem aktuellen Stand gehalten wird.

Verhaltensregeln E-Mail:

https://www.melani.admin.ch/melani/de/home/schuetzen/verhaltensregeln.html

4.5.5 Razzia gegen Droidjack-Käufer

Remote Access Tools für Android (RAT) werden im Cyber-Untergrund immer beliebter. Solche RATs ermöglichen die Überwachung eines Smartphones[21]. Unter anderem lässt sich der Datenverkehr überwachen, Telefongespräche sowie Umgebungsgeräusche können heimlich abgehört werden und die Kamera lässt sich anzapfen. Auch die Feststellung des Standortes ist möglich. Unter der Initiative der deutschen Strafverfolgungsbehörden wurde Ende Oktober gegen Verkäufer der RAT «Droidjack» eine Razzia gestartet. In den Ländern UK, USA, Frankreich, Deutschland, Belgien und auch in der Schweiz wurden zeitgleich Hausdurchsuchungen durchgeführt. Den Käufern der Schadsoftware wird das verbotene Ausspähen von Daten und Computerbetrug vorgeworfen. Verkauft wurde das Tool online für

[21] http://www.symantec.com/connect/blogs/droidjack-rat-tale-how-budding-entrepreneurism-can-turn-cybercrime (Stand: 29. Februar 2016).

210 US-Dollar. Mit Hilfe der Indizien erhofft man sich Erkenntnisse über die Autorenschaft, die bei dieser Razzia nicht im Fokus stand. Spuren zur Autorenschaft führen nach Indien.

4.6 Weitere Themen

4.6.1 Domänenmanagment als geschäftskritischer Prozess

Domainnamen sind nicht nur Adressen, unter welchen Websites erreicht werden können. Bei Unternehmen bilden sie meistens auch den hinteren Teil von E-Mail-Adressen der Mitarbeitenden und können beispielsweise Teil der Infrastruktur für Fernzugänge der Angestellten in die internen Netze sein. Domainnamen sind Adressierungselemente im Fernmeldeverkehr, haben insofern eine Vielzahl von Anwendungen und sind nicht zuletzt auch Marke der Firma. In Anbetracht der verschiedenen Funktionen, für die Domainnamen insbesondere bei Unternehmen verwendet werden, kann deren Management einen geschäftskritischen Prozess darstellen: Beispielsweise, weil die Website wie auch die E-Mails für die Geschäftstätigkeit zentral sind, oder weil die Konfiguration der IKT-Infrastruktur nur mit erheblichem Aufwand auf andere Domainnamen geändert werden kann.

Domainnamen können jedoch nicht «gekauft» werden – sie werden registriert. Das heisst, der Registrant erhält ein zeitlich limitiertes Nutzungsrecht am entsprechenden Adressierungselement und wird zu dessen Halter. Dieses Recht muss regelmässig erneuert werden. Geht dies vergessen, ist die Website plötzlich nicht mehr erreichbar und auch E-Mails werden nicht mehr zugestellt – dies sind nur die offensichtlichen technischen Konsequenzen.

Die Vergabe von Schweizer Domainnamen wurde 2015 umgestellt:[22] Die Pflicht der Registerbetreiberin, Domainnamen der *Top Level Domain* «.ch» direkt an Endkunden (Domain-Halter respektive Registranten) zu vergeben, wurde abgeschafft. Darüber hinaus wurde verfügt, dass die Registerbetreiberin nach einer Übergangsfrist das Endkundengeschäft vollständig aufgeben muss. Die Registerbetreiberin muss sich nun auf die technische Verwaltung der .ch-Domain beschränken, während die Vergabe von Domainnamen und die Endkundenadministration im Sinne einer vollständigen Entbündelung des Domainmarktes nur noch von so genannten Registraren vorgenommen wird. Dies hatte zur Folge, dass die Registranten, welche ihren Domainnamen bislang direkt bei der Registerbetreiberin SWITCH bezogen hatten, sich einen Registrar suchen mussten, der die Domainregistrierung für sie administriert. Bei der Auswahl des Registrars mussten sich die Registranten über ihre Bedürfnisse bewusst sein und ein passendes Angebot wählen.

Bei MELANI haben sich Ende 2015 mehrere Registranten beschwert, dass sie von ihrem neuen Registrar nicht in für sie geeigneter Frist und Form über den anstehenden Ablauf ihres Domainregistrierungsvertrags informiert worden seien. Ihre Domainnamen seien in der Folge abgeschaltet worden – mit den oben beschriebenen Konsequenzen für ihr Geschäft. Glücklicherweise werden abgelaufene .ch Domainnamen nicht unmittelbar zur erneuten Registrierung freigegeben, wodurch die (ehemaligen) Registranten ihre Domainnamen mit

[22] Aufgabentrennung bei der Verwaltung von .ch-Internetadressen: http://www.bakom.admin.ch/themen/internet/00468/04167/04981/index.html (Stand: 29. Februar 2016).

etwas administrativem Aufwand und der Hilfe ihrer Registrare wieder zurückerhalten konnten.

Empfehlung:

Einem Unternehmen muss bekannt und bewusst sein, wie viele und welche Domainnamen es registriert hat, wofür diese verwendet werden, und insbesondere wann die entsprechenden Registrierungen erneuert werden müssen. Sprechen Sie mit Ihrem Registrar über Ihre Bedürfnisse und seine Angebote. Etablieren Sie Prozesse und Mechanismen zum Schutz Ihrer Domainnamen vor unbeabsichtigten und mutwilligen Änderungen auf administrativer wie auch auf technischer Ebene.

Merkblatt IT-Sicherheit für KMUs

https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/checkliste-online-auftritt-kmu.html

5 Lage International

5.1 Spionage

5.1.1 Hacking Team gehackt

Dem italienischen Hersteller von Überwachungssoftware, «Hacking Team», wurde bei einem Hackerangriff eine grosse Menge an Daten gestohlen. Am 5. Juli 2015 wurden über 400 Gigabytes der gestohlenen Daten veröffentlicht. Die Firma Hacking Team produziert Überwachungssoftware für Strafverfolgungsbehörden, Nachrichtendienste und private Unternehmen. Auch die Kantonspolizei Zürich gehört zu den Kunden.[23] Die Produkteliste umfasst Überwachungssoftware für Windows, MacOS, Linux und sämtliche Smartphone-Betriebssysteme. Die von der Firma Hacking Team produzierte Überwachungssoftware ermöglicht Zugriff auf Smartphones und Computer und beispielsweise das Mitlesen von *SMS* oder das Abhören von Telefon- und auch Skype-Gesprächen.

Im Geschäft mit der Überwachung steht die Vertraulichkeit an oberster Stelle. Der Angriff hatte somit nicht nur für die gehackte Firma einen immensen Reputationsschaden zur Folge, sondern auch Konsequenzen für deren Kunden. Die veröffentlichten Daten enthielten beispielsweise E-Mails, Kundenlisten und andere vertrauliche Dokumente. Sie wurden höchstwahrscheinlich nicht nur durch zahlreiche Journalisten und Sicherheitsdienstleister durchforstet, sondern auch durch Gruppen, die Profit aus den nun bekannten Sicherheitslücken und Hintertüren schlagen wollen. Die eingesetzten und von den Kunden bezahlten Programme wurden im besten Fall schnell wirkungslos, konnten aber im schlimmsten Fall von unberechtigten Drittpersonen mitverwendet werden. Die Firma warnte daraufhin vor dem Missbrauch der Software durch Kriminelle und Terroristen.[24] Verschiedene Software-Anbieter hatten deshalb begonnen, die ausgenutzten Lücken zu schliessen. Die Zürcher Kantonspolizei, welche die Software «Galileo» von der Firma «Hacking Team» für knapp eine halbe Million erworben hatte, erklärte ebenfalls, auf den Einsatz dieser Überwachungssoftware zu verzichten. Dieser Vorfall zeigt sehr deutlich, wie schwierig und gefährlich der Umgang mit Sicherheitslücken und Hintertüren ist (siehe hierzu die Kapitel 3 und 5.1.2 (Juniper)).

Die Liste der Länder, aus welchen die Kunden stammen ist lang[25] und umfasst neben Staaten wie der Schweiz, den USA und Deutschland auch Staaten wie den Sudan, wo eigentlich ein UNO Waffenembargo gilt. Dies dürfte wiederum die Diskussionen anheizen, inwieweit ein Computerprogramm unter dem Begriff Waffenexport zu subsumieren ist.

Auch auf politischer Ebene sorgte die Veröffentlichung der internen Daten der Firma Hacking Team für einige Turbulenzen: Der Chef des zypriotischen Nachrichtendienstes, Andreas Pentaras, trat zurück, nachdem bekannt geworden war, dass er Software von Hacking Team

---

23 http://www.heise.de/newsticker/meldung/Hacking-Team-Kantonspolizei-kaufte-Ueberwachungssoftware-trotz-Bedenken-des-Bundesgerichts-2911887.html (Stand: 29. Februar 2016).

24 http://www.heise.de/newsticker/meldung/Hacking-Team-Terroristen-koennten-geleakte-Schnueffeltechnik-nutzen-2746071.html (Stand: 29. Februar 2016).

25 http://www.watson.ch/Digital/Best%20of%20watson/477908232-Die-uns%C3%A4glich-peinliche-Geschichte-der-gehackten-Hacker-(und-Kapo-ZH-Lieferanten)-in-25-Tweets-erz%C3%A4hlt (Stand: 29. Februar 2016).

gekauft hatte. Kommunikationsüberwachung ist in Zypern verboten. Das zypriotische Parlament hatte zwar vor fünf Jahren die Verfassung revidiert und die Überwachung unter gewissen Voraussetzungen erlaubt. Die gesetzlichen Grundlagen wurden aber noch nicht umgesetzt.[26] Pentaras beteuerte, es seien alle Vorgaben eingehalten worden, trat dennoch aber zurück, um möglichen Schaden beim zypriotischen Nachrichtendienst abzuwenden.

In der Schweiz kam Mario Fehr, Chef der Kantonspolizei Zürich, unter Beschuss. Fehr hat der Bestellung von Software der Firma Hacking Team zugestimmt. Die Beschaffung der Software erfolgte auf dem üblichen Weg durch eine Verfügung der Sicherheitsdirektion und ausschliesslich im Rahmen der Strafverfolgung.[27] Demgegenüber erfolgt der Einsatz technischer Überwachungsmassnahmen auf Anordnung des für die Bewilligung der Überwachung zuständigen Zwangsmassnahmengerichts. Die Jungsozialisten des Kantons Zürich haben gegen Fehr Strafanzeige eingereicht. Laut den Juso soll der Kauf gegen das Verfassungsrecht auf persönliche Freiheit und Privatsphäre verstossen haben. Die Zürcher Staatsanwaltschaft eröffnete jedoch kein Verfahren.

5.1.2 Spionage mit Juniper , Synful Knock und ein exportierbares Zertifikat

Der Netzausrüster Juniper hat bei einer internen Softwareüberprüfung «nicht autorisierte Programmzeilen» in seinem Betriebssystem «ScreenOS» gefunden. Juniper, mit Sitz in den Vereinigten Staaten, ist hinter Cisco der weltweit zweitgrösste Netzwerkausrüster und produziert High-End-Router, welche bei Internet-*Backbones* eingesetzt werden. Vor Weihnachten 2015 wurden zwei Lücken publiziert, zu denen gleichzeitig auch das entsprechende Update veröffentlicht wurde. Die betroffenen Versionen sind zwar nicht so weit verbreitet, werden aber für sichere Unternehmenskommunikation genutzt.

Die eine Lücke umfasste die Implementation eines Masterpasswortes im Programmcode und soll seit 2013 im Betriebssystem vorhanden sein. Während vor dem Update nur wenige (Angreifer) im Besitz dieses Passepartouts gewesen sein dürften, konnte nach der Veröffentlichung mit geringem Aufwand die Stelle herausgefunden werden, wo sich das Passwort befindet. Es dauerte dann auch nur wenige Stunden, bis dieses auch im Internet publiziert wurde. Entsprechende Angriffe liessen nicht lange auf sich warten.

Die zweite Lücke ist komplexer. Konkret handelt es sich um eine Hintertür in der Verschlüsselung, welche es einem Angreifer ermöglicht, VPN-Verbindungen abzuhören. Auf diese Weise können auch gespeicherte Netzwerkdaten im Nachhinein entschlüsselt werden. Die Lücke basiert auf dem schon seit Snowden in den Schlagzeilen stehenden Zufallsgenerator «EC_DRBG», der die Zahlen nicht so zufällig liefert, wie er es eigentlich sollte. Anstatt diesen Zufallsgenerator als Ganzes auszutauschen, hat Juniper lediglich die in der Kritik stehenden Schlösser ersetzt. Ein Angreifer hat diese Schlösser kurzerhand noch einmal zu seinen Gunsten geändert.

---

[26] https://intelnews.org/tag/cyprus-intelligence-service/ (Stand: 29. Februar 2016).

[27] http://www.kapo.zh.ch/internet/sicherheitsdirektion/kapo/de/aktuell/medienmitteilungen/2015_07/1507071c.html (Stand: 29. Februar 2016).

Schlussfolgerung:

Besonders bei der zweitgenannten Lücke liegt ein staatlicher Akteur als Täterschaft nahe. Diese Lücken zeigen einmal mehr das enorme Interesse von Angreifern an zentralen IKT-Komponenten. Ein weiterer Aspekt, der dieses Beispiel deutlich macht, ist das Risiko mit dem ein bewusstes Verbauen von Hintertüren und Schwachstellen verbunden ist. Dritte können jederzeit diese Hintertüren finden und für ihre Zwecke ausnutzen.

Auch der weltweit grösste Netzwerkausrüster «Cisco» hatte laut «FireEye» einen Angriff auf Netzwerk-Hardware zu verzeichnen.[28] Bei dem unter dem Namen «SYNful Knock» bekannt gewordenen Vorfall wurden mindestens 14 Router in der Ukraine, auf den Philippinen, in Mexiko und in Indien kompromittiert und Hintertüren angebracht. Die Anzahl der infizierten Geräte dürfte allerdings wesentlich höher sein.[29] Im Gegensatz zu dem Juniper-Vorfall wurde hier aber keine Sicherheitslücke ausgenutzt, um auf die Systeme zu gelangen: Der Zugriff erfolgte ganz normal über ein Admin-Passwort. Danach wurden Teile der *Firmware* mit Schadsoftware überschrieben. Die Passwörter kamen über verschiedene Wege in die Hände der Angreifer. In verschiedenen Fällen haben die Angreifer Standardpasswörter benutzt, was einmal mehr zeigt, dass es oft an grundlegenden Sicherheitsüberlegungen mangelt.

Am 23. November 2015 wurde bekannt, dass Dell ein eigenes *Root-CA-Zertifikat* im Windows-Zertifikatspeicher als «vertrauenswürdige Stammzertifizierungsstelle» hinterlegt. Mit diesem Zertifikat ist es jedem möglich, gültige Zertifikate für Dell-Geräte auszustellen. Die Problematik besteht darin, dass das Zertifikat zwar als nicht exportierbar markiert ist, sich aber trotzdem mit wenig Aufwand exportieren lässt. Somit lassen sich verschlüsselte Verbindungen von Programmen, die das *Crypto-API* von Dell benutzen, mittels «*Man in the Middle*» einfach abhören. Dies ist für fast alle Windows-Programme der Fall. Aber auch Schadsoftware kann auf diesem Weg erleichtert auf einem Dell-Computer installiert werden. Eine ungültige Signatur verhindert normalerweise die Installation von nicht vertrauenswürdiger Software oder fragt mindestens beim Benutzer nach, ob dieser die Software tatsächlich installieren will. Dieser Sicherheitsmechanismus fällt weg, wenn der Angreifer im Besitz des Root-CA-Zertifikates ist und somit beliebige (Schad-)Software mit einer gültigen Signatur signieren kann. Dell hat auf diese Entwicklung reagiert und ein Update zur Verfügung gestellt, welches das Zertifikat entfernt.

[28] https://www.fireeye.com/blog/threat-research/2015/09/synful_knock_-_acis.html (Stand: 29. Februar 2016).

[29] http://www.theregister.co.uk/2015/09/22/synful_knock_spreads_embaddened_boxen_in_31_countries/ (Stand: 29. Februar 2016).

Schlussfolgerung:

Die obigen Beispiele verdeutlichen zwei fundamentale Dinge: Erstens werden Staaten auch weiterhin versuchen zu nachrichtendienstlichen Zwecken Kommunikation abzufassen. Zweitens gibt es dafür zwei prinzipiell unterschiedliche Ansätze. Zum einen kann dieses Mithören dadurch etabliert werden, in dem Staaten auf die Hauptknoten und Leitungen der weltweiten Kommunikation sitzen. Oder aber sie fassen Informationen durch gezielte, individuell angepasste Operationen auf den Endpunkten (beispielsweise dem PC eines Verdächtigen) ab. Abgesehen von den politisch und rechtlichen Grundproblemen die sich bei der ersten Methode stellen (siehe HJB 2013 I und II), nimmt mit zunehmender Verschlüsselung der Kommunikation die Brauchbarkeit der so abgefassten Daten ab. Der einzige Weg den ersten Ansatz in die Zukunft zu retten, ist dabei Komponenten und Verschlüsselungen von vornherein zu verbieten oder zu schwächen. Der zweite Ansatz setzt mit seinem gezielten Vorgehen bereits auf den Punkt vor oder nach der Verschlüsselung. Er ist dabei auf Grund des Ressourcenaufwandes, Komplexität und der mit jeder individuellen Operation verbundenen Risiken de facto Selbstregulierend und -limitierend.

Die Diskussion in Sachen pro und contra Schwächung wird bereits international geführt und eine Verschärfung ist abzusehen. In diesem Sinne werden gerade Rechtsstaaten die im Rahmen der inneren- und äusseren Sicherheit auf die Möglichkeit der Kommunikationsüberwachung nicht verzichten wollen früher oder später ein klares Commitment zum einen oder anderen Ansatz abgeben müssen.

5.2 Datenabflüsse

5.2.1 Talk Talk

TalkTalk ist ein britischer Anbieter für Telefonie, Internet und Bezahl-Fenrsehen. Am 21. Oktober 2015 wurde das Unternehmen Opfer eines Angriffs, bei dem Datensätze von fast 157 000 Kundinnen und Kunden gestohlen wurden. Bei über 15 000 dieser Daten waren auch Bankdaten betroffen. Das war nicht der erste Vorfall bei der Firma Talk Talk: Bereits im Dezember 2014 und im Februar 2015 hatten Datendiebstähle dazu geführt, dass TalkTalk-Kundinnen und Kunden Ziel von Betrugsversuchen durch Social-Engineering-Techniken wurden.

Das Unternehmen wurde nicht nur aufgrund der Handhabung des aktuellen Falls und seiner internen Prozesse scharf kritisiert, sondern auch, weil es keine Lehren aus den vergangenen Fällen gezogen hatte. Insbesondere die mangelnde Verschlüsselung beim Speichern der persönlichen Daten wurde beanstandet.

Mehrere Fachleute kamen zum Schluss, dass der Angriffs durch eine *SQL-Injection* ausgelöst wurde. Interessant ist, dass TalkTalk gleichzeitig auch Opfer eines DDoS-Angriffs war. Es wurde vermutet, dass Letzterer als Ablenkungsmanöver diente: Während TalkTalk damit beschäftigt war, die Verfügbarkeit des Dienstes wiederherzustellen, konnten die

Angreifer das System kompromittieren[30]. In der Folge wurden die gestohlenen Daten wie in solchen Fällen üblich auf Untergrundmärkten verkauft und schliesslich dazu verwendet, gezielt Kundinnen und Kunden von TalkTalk zu betrügen.

Schlussfolgerungen

Dieser Vorfall zeigt, wie wichtig es ist, dass Unternehmen, welche persönliche Daten speichern, eine Risikoanalyse durchführen. Dabei müssen sie sich die Frage stellen, mit welchen Mitteln ein Angreifer auf diese Informationen zugreifen könnte und welche Risiken ein solcher Vorfall für die betroffenen Kundinnen und Kunden mit sich bringt. Als Ergebnis dieser Überlegungen müssen Schutzmassnahmen wie etwa die Verschlüsselung ergriffen werden. Ausserdem sollte eine klare Vorgehensweise für den Fall eines Angriffs festgelegt werden. Diese muss insbesondere regeln, wie die Benachrichtigung der Angriffsopfer (sprich, der Kundinnen und Kunden) sowie der zuständigen Behörden abläuft.

5.2.2 Weitere Datenabflüsse

Zwei Wochen lang soll es Angreifern gelungen sein, Kundendaten des britischen Telekommunikationskonzerns «Carphone Warehouse» zu stehlen. Entdeckt wurde der Vorfall am 5. August 2015. Insgesamt sollen auf den Carphone-Warehouse-Portalen wie beispielsweise OneStopPhoneShop.com, e2save.com und mobiles.co.uk bis zu 2.4 Millionen Datensätze unerlaubt wegkopiert worden sein. Darunter sollen sich auch bis zu 90‘000 Kreditkartendaten befunden haben. Betroffene Kunden wurden informiert. Für besorgte Kunden wurde eine Hotline eingerichtet.

Bei einem Angriff gegen das irische Dienstleistungsunternehmen «Experian», das die Kreditwürdigkeit von T-Mobile-Kunden prüft, sollen zwischen dem ersten September 2013 und sechzehnten September 2015 insgesamt 15 Millionen Datensätze gestohlen worden sein. Entwendet wurden Informationen wie Sozialversicherungs- oder Führerscheinnummern. Diese wurden zwar verschlüsselt abgelegt, könnten aber durchaus entschlüsselt werden. Daten von Bankkonten und Kreditkartendaten sollen nicht betroffen gewesen sein

Auch die Crowdfunding Plattform «Patreon» war am 28. September 2015 Opfer eines unerlaubten Datenabflusses. Dabei sollen verschlüsselte Passwörter, Steuerdaten und Sozialversicherungsnummern kopiert worden sein. E-Mail-Adressen wurden hingegen im Klartext abgezogen. Zudem befanden sich unter den gestohlenen Informationen auch Nachrichten aus dem internen Messaging-System. Trotz der Versicherung der Betreiber, Passwörter nur verschlüsselt abgespeichert zu haben, hat der Betreiber den Nutzern empfohlen, die Passwörter zu ändern. Auslöser des erfolgreichen Angriffs war, dass ein Datenbank-*Backup* der Produktionssysteme auf einem Test-Server abgelegt war. Anscheinend war dieser Server dann über eine Web-Applikation vom Internet her zugänglich, was die Angreifer ausnutzten. Die erbeuteten 2.3 Millionen E-Mail-Adressen wurden im Internet veröffentlicht. Bemerkenswert war auch ein in diesem Zusammenhang aufgetauchtes Erpresserschreiben. Die Täter drohten den E-Mail-Adressaten, weitere

[30] Obwohl dies nicht bestätigt wurde, wurde davon gesprochen, dass auch Erpressung im Spiel war.

sensible Daten zu veröffentlichen, sollten diese nicht innerhalb von 48 Stunden 1 *Bitcoin* bezahlen. Inwiefern die Angreifer wirklich solche Daten besassen oder einfach nur aufs Geratewohl die nun öffentlich bekannten E-Mail-Adressen anschrieben, ist nicht bekannt.

5.3 Industrielle Kontrollsysteme

Auf die Gefahr, die von ungenügend geschützten industriellen Kontrollsystemen (*IKS oder auch SCADA genannt*) ausgeht, wird seit Langem hingewiesen. Über die oftmals frei aus dem Internet zugänglichen *Programmable Logic Controller (PLC bzw. SPS),* die Teil eines vernetzen SCADA-Systems sein können, werden Angreifern verschiedene Möglichkeiten geboten, Schadsoftware beispielsweise zum Spionieren in Industrie-Systeme zu schmuggeln. Die dafür nötige Software steht frei zum Download bereit. Vielfach werden solche Warnungen als Gefahren abgetan, die nur in einer Laborumgebung funktionieren. Die technische Prüforganisation, TÜV-Süd, zeigte mit einem fiktiven Wasserwerk, das als *Honeynet* im Internet exponiert wurde, dass auch auf scheinbar unbedeutende Systeme Angriffe aller Art stattfinden[31]. Ende Juli 2015 wurden die Resultate publiziert.

Fast zeitgleich mit der Inbetriebnahme dieses Lockvogel-Systems fand der erste Zugriff auf das fiktive Wasserwerk statt. Während den acht Monaten Laufzeit des Experiments registrierten die TÜV-Süd-Experten über 60‘000 Zugriffe aus mehr als 150 Ländern. Die *IP-Adressen* der meisten Versuche stammten aus China, den USA und Südkorea, wobei IP-Adressen allerdings keine Rückschlüsse über den tatsächlichen Standort des Zugreifenden erlauben. Zugriffe erfolgen in solchen Fällen erfahrungsgemäss in der Regel über verdeckte bzw. verschleierte IP-Adressen.

Zugriffsversuche auf Standardprotokolle sind weit verbreitet. Im beschriebenen Versuchsaufbau wurden jedoch auch Anfragen über Industrieprotokolle wie Modbus/TCP oder S7Comm beobachtet. Dieser Versuch zeigt den Betreibern solcher Anlagen, dass Lücken in der Konfiguration gesucht, gefunden und auch ausgenutzt werden.

Dass das Interesse nicht nur fiktiven Systemen gilt, zeigt das nachfolgende Beispiel in Kapitel 5.3.1. Es beschreibt den ersten massiven Stromausfall, der hauptsächlich auf einen Cyber-Angriff zurückzuführen ist. Aber auch andere Bereiche wie beispielsweise medizinische Geräte (Kapitel 5.3.3) oder Autos (Kapitel 5.3.4) dürfen nicht vergessen werden und werden in Zukunft mehr in den Fokus von Angreifern rücken.

5.3.1 Stromausfall in der Ukraine – Schadsoftware im Spiel

80’000 Personen waren kurz von Weihnachten, am 23. Dezember 2015, in der ukrainischen Region «Ivano-Frankivsk Oblast» ohne Strom. Mehrere regionale Stromversorger meldeten, dass ihre Systeme Opfer einer Cyber-Attacke geworden seien. Diese hatte zur Folge, dass sieben 110-Kilovolt- und 23 35-Kilovolt-Unterwerke vom Netz getrennt wurden[32].

---

31 http://www.tuev-sued.de/tuev-sued-konzern/presse/pressearchiv/potenzielle-angreifer-sind-ueberall (Stand: 29. Februar 2016).

32 http://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid (Stand: 29. Februar 2016).

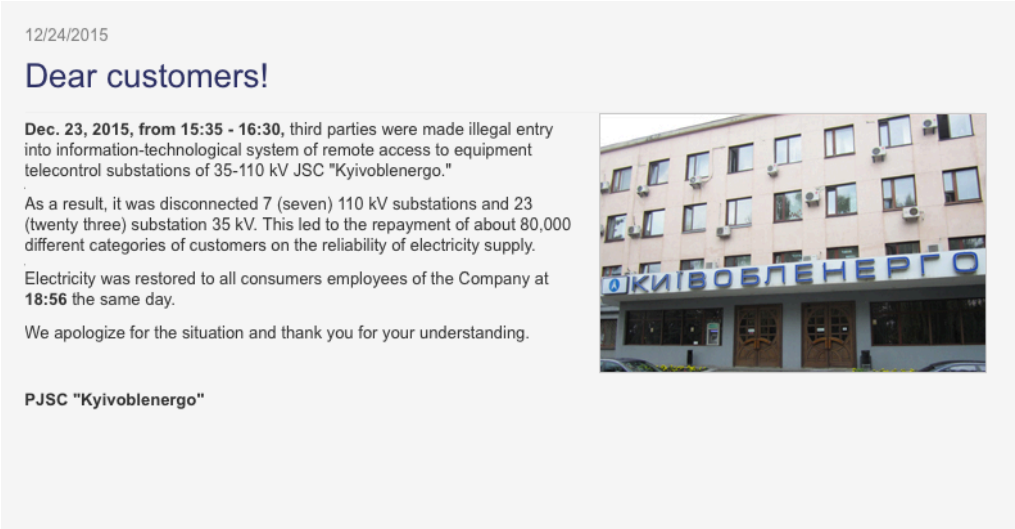

Abbildung 9: Kundeninformation eines lokalen ukrainischen Stromversorgers

Der Angriff auf die Stromversorger erfolgte mehrstufig. Das ukrainische CERT (CERT-UA) konnte auf Computern der betroffenen Energiefirmen mit internationaler Unterstützung die Schadsoftware «BlackEnergy» (BE) in mehreren Ausprägungen (BE2 und BE3) identifizieren. Die Malware selbst konnte jedoch bislang nicht als primäre Ursache des Stromausfalls bestätigt werden[33].

Nach heutigem Kenntnisstand ist der folgende Ablauf am wahrscheinlichsten: Mittels *Spearphishing* und präparierten Office-Anhängen wurden Computer im Netzwerk der betroffenen Energiefirmen infiziert. Mit Hilfe der Malware BlackEnergy kundschafteten die Angreifer das Netzwerk aus und verschafften sich so Zugriff auf weitere Geräte, inklusive solcher von Operatoren, auf denen sie SCADA-Konsolen zur Steuerung der Unterwerke fanden. Der Stromausfall selbst wurde dann mutmasslich durch die Auslösung von Trennschaltern in solchen Konsolen verursacht, wie es auch ein legitimer Operator vor Ort zu Wartungszwecken durchführen würde. Um die Wiederherstellung der Stromversorgung zu behindern und um Spuren zu verwischen, setzten die Angreifer zusätzlich die Malware «*KillDisk*» ein, welche die Festplatten der betroffenen Computer unbrauchbar machte. Gleichzeitig überlasteten sie die Website und das Call-Center des Unternehmens mit *DDoS-Angriffen,* um die Meldung der Ausfälle und die Kommunikation mit den Kunden zu erschweren.[34]

Ukrainische Regierungsvertreter beschuldigten kurz nach den Vorfällen Russland, für den Angriff verantwortlich zu sein. Dieselbe Anschuldigung folgte auch im Januar 2016, als BlackEnergy im Netzwerk des Kiewer Flughafens «Boryspil» entdeckt wurde, dort aber keinen Schaden anrichtete. Beweise für die Anschuldigungen gab es jedoch keine. Die Sicherheitsfirma «iSight Partners» vermutet das «Sandworm»-Team hinter dem Angriff, das bei früheren Angriffen auffällig deckungsgleich im Interesse der russischen Regierung

[33] https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B (Stand: 29. Februar 2016).

[34] http://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/ (Stand: 29. Februar 2016).

handelte. Jedoch wird BlackEnergy breit eingesetzt und ist teilweise auch auf dem Schwarzmarkt verfügbar, was die Zuordnung der Täterschaft zusätzlich erschwert.

Schlussfolgerung/ Empfehlung:

Das beschriebene Ereignis ist der erste massive Stromausfall, der hauptsächlich auf einen Cyber-Angriff zurückzuführen ist. Betreiber von solchen Infrastrukturen können die Erkenntnisse aus diesem Beispiel nutzen, um ihre eigenen Netzwerke und Installationen besser gegen ähnliche Angriffsmuster zu wappnen.

MELANI stellt eine Checkliste mit Massnahmen zum Schutz von Industriellen Kontrollsystemen zur Verfügung. Die aufgeführten Massnahmen sollten in einen übergeordneten Sicherheitsprozess eingebettet sein, welcher gewährleistet, dass die Massnahmen angewendet, regelmässig geprüft und kontinuierlich verbessert werden. Weiter ist es wichtig, dass der Betreiber einer Anlage seine aktuelle Bedrohungslage kennt, diese regelmässig überprüft und die Erkenntnisse in die Implementierung und Verbesserung der Sicherheitsmassnahmen einfliessen lässt. Dazu ist eine enge Zusammenarbeit zwischen Risikomanagement, Engineering und Betrieb von grosser Bedeutung.

DOKU

Checkliste mit Massnahmen zum Schutz industrieller Kontrollsysteme

https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/massnahmen-zum-schutz-von-industriellen-kontrollsystemen--ics-.html

5.3.2 Manipulationen durch datenbasierte Automation in der Erdöl- und Gasversorgung

Nicht erst seit «Stuxnet» fürchtet man sich vor Angriffen auf Steuerungssysteme kritischer Prozesse. Wie bereits im vorangehenden Kapitel zu BlackEnergy vermutet, muss nicht zwingend das Steuerungssystem direkt gestört, sondern die Prozesse können auch über Datenmanipulation in angrenzenden Systemen beeinflusst werden. Im November 2015 präsentierten Alexander Polyakov und Mathieu Geli des Sicherheitsspezialisten «ERPScan» an der Konferenz «Black Hat Europe», wie durch Manipulation von *ERP-Systemen* Ventile von Pipelines in der Öl- und Gasindustrie beeinflusst werden können.[35] Die komplexe und in vielen Bereichen automatisierte Systemlandschaft (siehe hierzu Abbildung 10) kann laut den ERP-Experten auf drei Arten attackiert werden:

Bei einer dieser Angriffsarten werden Messwerte wie Temperatur und Druck in einer Ressourcen-Verwaltunganwendung gefälscht. Dies bewirkt ein kostenintensives Aussenden von Wartungsteams, im schlimmsten Fall zu einer Ölplattform inmitten des Ozeans. Werden zusätzlich Füllstände und Fassvermögen von Öltanks gezielt verändert, kann das im schlimmsten Fall zu Explosionen führen. Zur Effizienzsteigerung sind gewisse Befehle von

[35] https://www.blackhat.com/docs/eu-15/materials/eu-15-Polyakov-Cybersecurity-For-Oil-And-Gas-Industries-How-Hackers-Can-Manipulate-Oil-Stocks-wp.pdf (Stand: 29. Februar 2016).

Drittsystemen an die Leitebene teilweise erlaubt. Dadurch ist für einen Sabotage-Angriff nicht einmal das Vorhandensein von Schwachstellen im Kontrollsystem selbst notwendig.

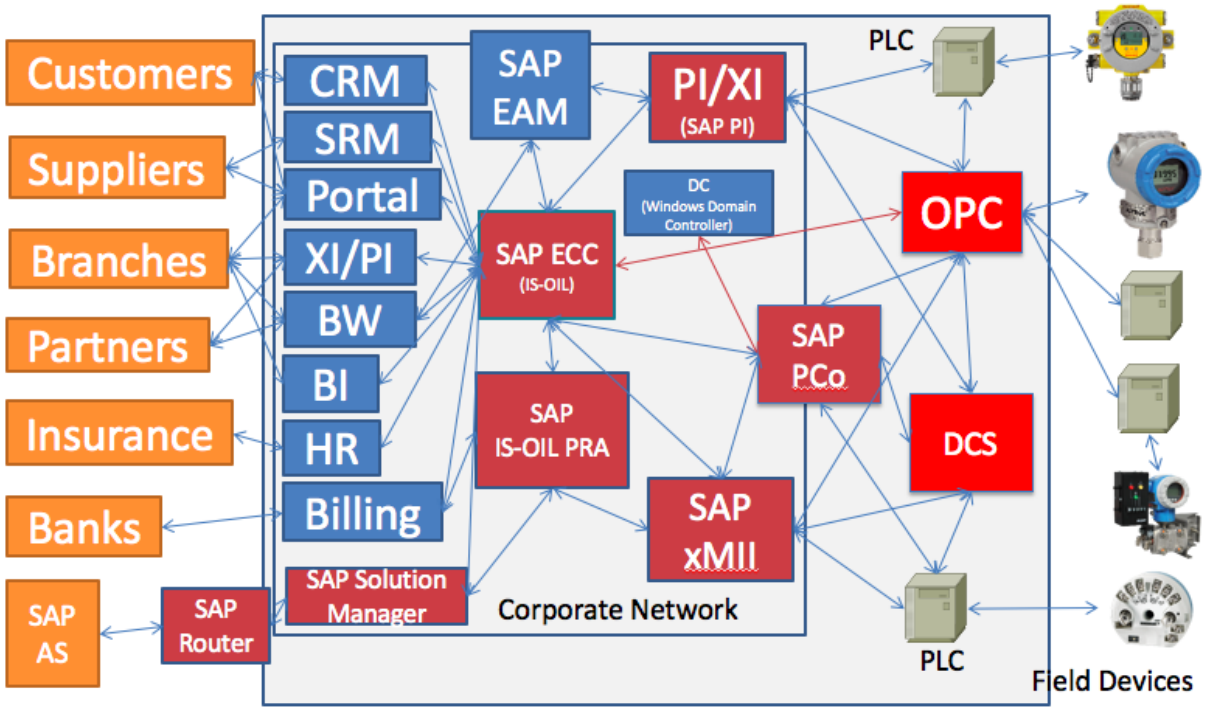

Abbildung 10: Beispiel einer Systemlandschaft Öl- und Gasindustrie. Quelle: Alexander Polyakov und Mathieu Geli

Schlussfolgerung:

Das Beispiel zeigt die Problematik auf, die mit datengestützter Automation in die Prozesse eingebracht wird. Die immer grossflächigere Verbreitung von intelligenten «Smart Meters» eröffnet deshalb nicht nur effizientere Geschäftsprozesse, sondern auch effizientere Angriffsvektoren bei einem Missbrauch.

5.3.3 Tausende medizinische Geräte aus dem Internet angreifbar

Im Spital ist oft schnelles Handeln gefragt. Leben hängen von Entscheidungen, basierend auf Labor- und Diagnosedaten ab. Diese müssen dem behandelnden Personal sofort zur Verfügung stehen. Dabei scheint bei der Konfiguration von medizinischen Geräten und ihrer Schnittstellen zur Patientendatenverwaltung teilweise der Benutzerfreundlichkeit und der Geschwindigkeit mehr Bedeutung zugemessen zu werden als für sicherheitstechnische Aspekte.

An der Sicherheitskonferenz «Derbycon 2015»[36] präsentierten die beiden Forscher Scott Even und Mark Collao Ergebnisse einer Studie, wonach bei nur einer Gesundheitsfirma über 68‘000 medizinische Geräte direkt aus dem Internet erreich- und angreifbar gewesen sein sollen. Dass solche Angriffe durchaus vorkommen, untermauerten sie mit den Ergebnissen

[36] http://www.irongeek.com/i.php?page=videos%2Fderbycon5%2Fbreak-me14-medical-devices-pwnage-and-honeypots-scott-erven-mark-collao (Stand: 29. Februar 2016).

von zehn *Honeypot*-Systemen, die vorspiegelten, ein Defibrillator oder MRI-System zu sein. Die Lockvogel-Geräte wurden 299 Mal mit Malware angegriffen, wobei 24 dieser Angriffe erfolgreich waren.

Das Risiko im Gesundheitsbereich beschränkt sich jedoch nicht nur auf unerlaubte Zugriffe auf medizintechnische Geräte. Auch Zugriffe auf besonders schützenswerte Gesundheitsdaten stehen in letzter Zeit immer wieder in den Schlagzeilen[37]. Durch die Verwendung von unsicheren Apps exponieren zudem einzelne Patienten ihre Daten gleich selbst. Obwohl vom britischen Gesundheitsbehörde NHS freigegeben, verfügen 23 von 79 durch das «Imperial College»[38] getestete Apps nicht über grundlegende Verschlüsselungsmechanismen[39]. Bei vier Anwendungen wurden die Gesundheitsangaben sogar im Klartext übermittelt.

5.3.4 Das intelligente Auto – die Verantwortung der Autoindustrie

Die Szene könnte einem Horrorfilm entstammen: Bei einer Autofahrt im Sommer beginnt plötzlich die Heizung unter Volllast zu laufen, das Radio wechselt willkürlich auf den verhassten Spartensender, die Scheibenwischer machen sich selbstständig und auf dem Navigationsdisplay erscheint ein fremdes Gesicht, das meldet, das Fahrzeug unter Kontrolle gebracht zu haben. Kurz darauf scheitern auch die Beschleunigung- oder noch schlimmer die Bremsversuche.

Auch wenn solche Angriffe in der Realität noch nicht gelungen sind, erfunden sind sie nicht: Eine Lücke im Infotainmentsystem «Uconnect» erlaubte den beiden Sicherheitsforschern Miller und Valasek, dieses aus der Ferne zu übernehmen[40]. Dazu reichte ihnen die Kenntnis der *IP-Adresse* des Systems. Einmal übernommen, erlaubte ihnen das Einspielen von eigenem Code in der Uconnect-*Firmware* den Zugriff auf die benachbarten Prozessoren der Steuerungselektronik. Über das interne Kommunikationsnetzwerk, dem sogenannten Controller Area Network-*Bus,* konnten Sie so Befehle an Motor und Bremsen absetzen und aus der Ferne dem Fahrer die Kontrolle über das Fahrzeug entziehen.

Die Forscher präsentierten ihre Erkenntnisse an der «Black Hat Konferenz 2015» inklusive dem *Patch*[41], den sie zusammen mit dem «Fiat-Chrysler»-Konzern sowie dem beteiligten Telekommunikationsanbieter «Sprint» ausgearbeitet hatten. Das anschauliche Szenario provozierte grosse Aufmerksamkeit in der Autoindustrie und auch in der Öffentlichkeit. Diese flaute jedoch bald wieder ab, denn der Konsument schätzt weiterhin die komfortable Bedienung gewisser Fahrzeugfunktionen aus der zugehörigen Smartphone-App.

Es bleibt zu hoffen, dass sich der Sicherheitsgedanke bei der Trennung von Unterhaltungs- und Steuerungselektronik durchsetzt, da laufend neue mögliche Angriffsvektoren bekannt

---

37 http://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720 (Stand: 29. Februar 2016). http://www.huffingtonpost.com/2015/03/17/premera-blue-cross-cybera_n_6890194.html (Stand: 29. Februar 2016).

38 https://www.imperial.ac.uk (Stand: 29. Februar 2016).

39 http://www.theguardian.com/society/2015/sep/25/nhs-accredited-health-apps-putting-users-privacy-at-risk-study-finds (Stand: 29. Februar 2016).

40 http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (Stand: 29. Februar 2016)

41 https://ics-cert.us-cert.gov/advisories/ICSA-15-260-01 (Stand: 29. Februar 2016).

werden. So konnten bereits Wegfahrsperren von Funkschlüsseln überwunden werden[42] oder über die Manipulation von Radiosignalen Befehle durch die Entertainmentsysteme geschleust werden[43].

Schlussfolgerung:

Wenn immer mehr Verantwortung dem intelligenten Auto abgetreten wird, entstehen notgedrungen neue Problemfelder. Angesichts von autonomen Fahrzeugen und intelligenten, sich selbst regulierenden Car2X-Systemen, verschwimmen die Grenzen von physischer Sicherheit und Informationssicherheit immer mehr, was bestenfalls zu derselben Testintensität der IKT-Systeme wie bei den Crashtests führen wird.

5.3.5 Staudamm mutmasslich als Vergeltungsmassnahme gehackt

Im Jahre 2013 soll es mutmasslich iranischen Hackern gelungen sein, in die Kontrollsysteme eines Staudammes in der Nähe von New York einzudringen. Dies berichtete das Wallstreet Journal[44] im Dezember 2015 bezugnehmend auf zwei Personen, die mit der Aufklärung des Falles betraut waren. Der eher kleine Staudamm soll im Rahmen der angeblichen Vergeltungsmassnahmen im Nachgang der Aufdeckung der Stuxnet-Sabotage angegriffen worden sein. Es ist wichtig, aus der Analyse solcher «Streifschüsse» zu lernen und die Sicherheitsvorkehrungen kritischer Infrastrukturen weiter zu verbessern.

5.4 Angriffe auf Websites: DDoS, Defacements

5.4.1 New World Hacking Gruppe schiesst bei Testlauf gegen BBC übers Ziel hinaus

Viele Briten, die an Silvester 2015 vor den Festlichkeiten noch schnell ihre BBC-Lieblingssendung im Nachhinein schauen oder die Vorbereitungen mit der BBC-Radio App begleiten wollten, wurden enttäuscht. Auf den Webseiten der BBC prangte einzig eine Fehlermeldung, siehe Abbildung 11.

[42] http://www.heise.de/make/meldung/Wegfahrsperre-VW-Hack-ist-offen-2778194.html (Stand: 29. Februar 2016).

[43] http://www.bbc.com/news/technology-33622298 (Stand: 29. Februar 2016).

[44] http://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559 (Stand: 29. Februar 2016).

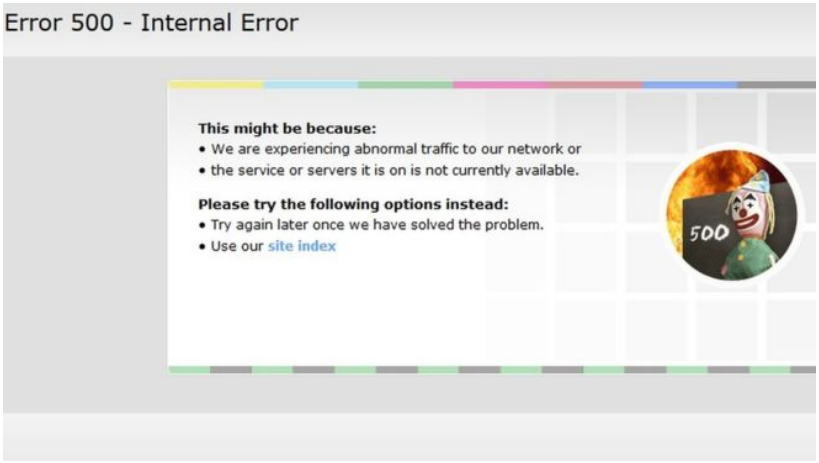

Abbildung 11: Fehlermeldung auf der BBC-Webseite an Silvester 2015[45]

Laut der Gruppe «New World Hacking» war keine technische Störung für den mehrstündigen Ausfall verantwortlich, sondern ein Test, den die Gruppe durchgeführt hatte, um ihre eigenen Fähigkeiten zu erproben. Gegenüber BBC Technologie-Korrespondent, Rory Cellan-Jones, bekannte sich einer der Angreifer, der sich selbst «Ownz» nennt, zur mutmasslichen DDoS-Attacke. Eigentlich zielt die Gruppe mit ihren Aktivitäten gegen die Online-Präsenz des Islamischen Staates. Um ihr neu entwickeltes Tool «Bangstresser» zu erproben, wählten sie jedoch die BBC als Demonstrationsziel aus. Nach Aussagen der Angreifer war es nicht ihre Absicht, einen Ausfall von solcher Dauer zu provozieren. Die Leistungsfähigkeit ihrer eigenen Angriffsinfrastruktur hatte sie selbst überrascht.

5.4.2 Anonymous vs. ISIS – Propaganda Krieg im Netz

Bereits im Umfeld der Anschläge auf die Satirezeitung «Charlie Hebdo» im Januar 2015 lancierte das Hackerkollektiv «Anonymous» ihre Kampagne «#OpISIS», in der hauptsächlich versucht wird, die Kommunikationskanäle der vermuteten Terroristen zu sabotieren und die Rekrutierung neuer Mitglieder zu erschweren. Nur einen Tag nach den erneuten Anschlägen in Paris veröffentlichte die lose Gruppierung per Video[46] eine Kriegserklärung an den Islamischen Staat.

Da Anonymous über keine klare Struktur verfügt, waren die Massnahmen im Nachgang der Anschläge nicht sehr koordiniert. Beispielsweise wurde intensiv diskutiert, ob es neben der bestehenden #OpISIS noch eine separate «#OpParis» Operation brauche. Weitere Uneinigkeit über Sinn und Unsinn einer Kriegserklärung und unterschiedlichste Ankündigungen von Subgruppierungen veranlassten das Hackerkollektiv am 18. November 2015 zur Publikation einer Pressemitteilung[47]. Darin wurden die Ziele der Gruppierung auf die laufenden Aktivitäten dargelegt, sowie die bevorzugten Kommunikationskanäle empfohlen. Die Untergruppe «Ghost Security (GhostSec)» hat es auf die Identifizierung und Sperrung von Social Media Konten abgesehen, die in Verbindung mit der Terrororganisation stehen. Die teilweise Kooperation von GhostSec mit staatlichen Behörden wird nicht von allen Mitgliedern goutiert.

---

45 http://www.bbc.com/news/technology-35213415 (Stand: 29. Februar 2016).

46 https://www.youtube.com/watch?v=RwGGcZoRs-k (Stand: 29. Februar 2016).

47 https://www.docdroid.net/hUQ7Ez2/anonymous-operations-isis-11-2015.pdf.html (Stand: 29. Februar 2016).

Neben einem Aufruf[48] zum «Trolling Day» am 11. Dezember 2015, an dem man sich über die IS-Terroristen lustig machen soll, schafften es vor allem die «*Doxing*»*-Aktivitäten* der GhostSec-Gruppe in die Presse. Bei Doxing werden die wahren Identitäten und Aufenthaltsorte von den verantwortlichen Personen hinter Social Media-Accounts und Websites öffentlich präsentiert. Ausser Anleitungen[49], wie man sich online besser schützen kann, sind von Seiten des IS jedoch kaum Reaktionen zu beobachten. In der Anleitung empfiehlt der IS neben vielen anderen Applikationen auch die Schweizer Anbieter «Swisscom IO» und «Threema» sowie die Kommunikationslösungen der in Genf beheimateten Unternehmens «Silent Circle». Es besteht die Möglichkeit, dass diese Firmen oder deren Kunden durch diese Publizität allenfalls auch ins Visier der Hacktivisten geraten.

5.4.3 Manipulierte QR-Codes

Strichcodes und in letzter Zeit vermehrt auch die zweidimensionalen *QR-Codes,* werden in den verschiedensten Anwendungsszenarien eingesetzt. Allen bekannt ist der Strichcode auf der Verpackung, der nicht nur Angaben zum Preis, sondern auch noch diverse andere Informationen enthält. Der QR-Code hat sich unter anderem in der Luftfahrt durchgesetzt, um sich beim Boarding gegenüber der Fluggesellschaft zu identifizieren.

Die Gefahr, die bisher mit diesen Strichcodes in Verbindung gebracht wurde, war vor allem die missbräuchliche Verwendung der darauf enthaltenen Informationen. Der Cyber-Sicherheitsforscher Yang Yu konnte nun aber aufzeigen, dass die gedruckten Codes auch als Angriffsvektor gegen die lesenden Computersysteme verwendet werden können[50]. Unter der Bezeichnung «Badbarcode» veröffentlichte er mehrere Videos und präsentierte seine Erkenntnisse auf der Konferenz «PacSec» 2015 in Tokyo. Yu nutzt eine Serie von Schwachstellen in den Programmen aus, die für das Scannen der Codes zuständig sind. Durch das Drucken von eigenen manipulierten Strichcodes, konnte er die Scan-Systeme dazu bewegen, nicht nur Informationen einzulesen, sondern auch Befehle auszuführen.

Bisher sind keine böswilligen Anwendungen dieser Möglichkeiten bekannt, jedoch bergen diese Schwachstellen laut Yu durchaus ein mögliches Gefahrenpotential.

5.5 Crimeware

5.5.1 Neue TLDs und Malware

Verschiedene *Top-Level-Domains* (TLD) haben unterschiedliche Sicherheitsniveaus. Deshalb ist es nicht erstaunlich, dass einige TLDs bei kriminellen Gruppen deutlich beliebter sind als andere. Mit der Einführung generischer TLDs sind für Kriminelle zudem neue Möglichkeiten entstanden, an günstige und kaum kontrollierte Domänen zu gelangen. Auf diesen betreiben sie dann ihre *Command und Control Infrastruktur*. Jedoch werden die bekanntesten Domänen (z. B. .com oder .biz) ebenfalls sehr häufig von Kriminellen missbraucht.

---

48 https://ghostbin.com/paste/ucsf3 (Stand: 29. Februar 2016).

49 http://www.wired.com/2015/11/isis-opsec-encryption-manuals-reveal-terrorist-group-security-protocols/ (Stand: 29. Februar 2016).

50 http://motherboard.vice.com/read/badbarcode-project-shows-customized-boarding-passes-can-hack-computers (Stand: 29. Februar 2016).

Laut ntldstats.com haben folgende generische TLDs einen hohen Anteil an Malware:

* .science
* .click
* .link
* .party
* .xyz

Es gibt aber auch immer wieder Länderdomänen, die gerne von kriminellen Gruppen verwendet werden. Die Gründe sind vielfältig: So bot der Registrar «freenom.com» beispielsweise die Möglichkeit, verschiedene TLDs von afrikanischen Ländern gratis zu registrieren, was zu einem starken Anstieg von Domainregistrierungen zu kriminellen Zwecken in diesen Ländern geführt hat.

Länderdomänen mit hohem Malwareanteil sind beispielsweise:

.gq (Aequatorial Guinea)
.tk (Tokelau)
.ga (Gabun)
.cf (Zentralafrikanische Republik)
.ml (Mali)

Registry und Registrare müssen über klare *Abuse*-Regeln verfügen, die festlegen, was bei einer kriminellen Verwendung einer Domain zu geschehen hat. Selbstverständlich müssen sie diese Regeln auch durchsetzen. Darüber hinaus braucht es etablierte Prozesse und Abuse Teams, welche sich um die Vorfälle kümmern und diese rasch lösen. Im Kapitel 6.2 finden Sie ausführliche Details über die Bekämpfung des Missbrauchs von Schweizer Domainnamen.

5.6 Weitere Themen

5.6.1 Lampenfieber bei Google’s Android

Am 27. Juli 2015 wurde eine von der Sicherheitsfirma «Zimperium» entdeckte Schwachstelle publiziert, die es Hackern ermöglichte, ohne Benutzerinteraktion per MMS auf die Daten von Android-Smartphones zuzugreifen. Es sollen nach Schätzungen bis zu 95 Prozent aller Android-Smartphones betroffen gewesen sein. Um die Lücke auszunutzen, musste der Angreifer seinem Opfer lediglich eine präparierte MMS-Nachricht schicken, die durch das Opfer nicht einmal geöffnet werden musste. Das Smartphone wurde bereits kompromittiert, sobald die Nachricht vom System verarbeitet wurde. Bis zur Publikation und Einspielung der entsprechenden Updates half nur das Abschalten der MMS-Empfangsfunktion. Die «Deutsche Telekom» hatte sogar die Zustellung von MMS-Nachrichten zwischenzeitlich ausgesetzt, um ihre Kunden vor potenziellen Angriffen zu schützen.

6 Tendenzen und Ausblick

6.1 Mobile Payment

Schweden ist im Begriff, als erstes Land das Bargeld abzuschaffen. Noch vor zehn Jahren wäre es undenkbar gewesen, dass Kredit- und Debitkarten einmal das Bargeld ganz ablösen würden. In Skandinavien werden inzwischen aber selbst auf dem Weihnachtsmarkt fast ausschliesslich digitale Zahlungsmittel akzeptiert. Aktuelle Prognosen sagen voraus, dass das Smartphone die erwähnten Zahlkarten verdrängen und das Mobile Payment sich als Zahlmethode der Zukunft durchsetzen wird. In den USA gaben vier von zehn Käuferinnen und Käufern an, schon mindestens einmal mobil bezahlt zu haben, und gemäss Informationen der Website «The Statistic Portal» wird diese Tendenz kontinuierlich um jährlich 20 Prozent steigen. Die Schweiz, in der bargeldloses Bezahlen zwar schon seit Längerem etabliert ist, tut sich allerdings mit der Einführung von *Mobile-Payment*-Geräten schwer. Hier gibt es das Angebot seit 2011, als «Mobino» auf den Markt kam.

Stärker thematisiert wurde Mobile Payment erst vor ein paar Monaten, als die grossen Player auf dem Markt Einzug hielten. Seit Ende 2015 findet man an über 3‘000 «Coop»-Kassen im ganzen Land das grüne Sechseck von «Twint». Dieser Dienst der «Postfinance» ermöglicht an bestimmten Verkaufsstellen mit entsprechendem *Bluetooth*-Terminal die Bezahlung übers Handy. «Paymit», das Konkurrenzprodukt der Firmen «UBS», «SIX» und der «Zürcher Kantonalbank», wurde 2015 zur besten Schweizer App gekürt und ist mit über 170‘000 Downloads in der Schweiz die meistverbreitete Anwendung zum bargeldlosen Bezahlen mit dem Smartphone. Auch andere Dienstleister bringen immer neue Produkte auf den Markt: Die Kunden von «Migros», «Manor» und «Starbucks» können jetzt ihre Rechnung mit dem Handy begleichen. Seit Kurzem gibt es «Swiss One Wallet», eine digitale Plattform der Unternehmen «Aduno», «Swisscard» und «Netcetera» für die Bezahlung in Onlineshops und per Mobile Payment. Dazu kommen die Produkte von Firmen wie Apple, Facebook oder Google. Vorerst scheinen diese Dienste jedoch trotz des vielfältigen Angebots in der Schweiz nur schwer Fuss zu fassen. Abgesehen von der Tatsache, dass Menschen Ihre Gewohnheiten nur sehr langsam ändern, sind mögliche Erklärungen für die schleppende Entwicklung die Vielzahl und Unübersichtlichkeit der Anbieter, die Sorge der Kundinnen und Kunden bezüglich Datenschutz, sowie die Tatsache, dass manche Dienstleister sich für Technologien entschieden haben, die wenig verbreitet sind oder von den Mobilfunkanbietern nur begrenzt unterstützt werden. Das Scheitern der Swisscom Bezahl-App «Tapit» dürfte beispielsweise auch damit zusammenhängen, dass die damals verwendete Kommunikationsmethode «*NFC*» *(Nearfield Communication)* lange Zeit nur für Android-Nutzer verfügbar war. Apple führte diese erst mit dem iPhone 6 ein.

Jede App unterscheidet sich in ihrer Dienstleistung, in ihren Technologien und dem Zielpublikum. Die nachfolgenden Analysen beschränken sich deshalb auf die beiden Dienste Paymit und Twint, die den Schweizer Markt wohl bald beherrschen dürften.

Im Februar 2016 wurde Paymit in ersten Geschäften eingeführt und kann ab dem zweiten Quartal 2016 auch für Online-Einkäufe verwendet werden. Die App Paymit ermöglicht auch mobile Zahlungen unter Privatpersonen. Zur Anmeldung bei Paymit muss man nicht unbedingt UBS-Kunde sein, aber man braucht eine Telefonnummer und ein Bankkonto in der Schweiz sowie eine Kredit- oder Prepaidkarte. Die Transaktionen erfolgen direkt auf dem Bankkonto und werden wie bei klassischen Zahlungen von der Bank kontrolliert. Im Fall eines Diebstahls ist die Anwendung durch einen Sicherheitscode geschützt, während zur

Ausführung der Zahlvorgänge keine zusätzliche Autorisierung verlangt wird. Um die Risiken zusätzlich zu begrenzen, ist eine Bezugslimite von 500 CHF pro Tag festgelegt, die aber auch erhöht werden kann.

Mit Twint kann man nicht nur via Bluetooth in Geschäften bezahlen, sondern dank eines Peer2Peer-Systems auch Zahlungen unter Privatpersonen sowie in gewissen Online-Shops durchführen. Auch Twint setzt nicht voraus, dass man Kunde der Postfinance ist. Die direkte Anbindung eines Bankkontos funktioniert jedoch nur mit sechs Partnerbanken. Im Gegensatz zu Paymit funktioniert Twint auch ohne Kreditkarte, da die gewünschte Geldsumme von der Postfinance-Karte, per Lastschriftverfahren (LSV), mit einem Einzahlungsschein oder via Twint-Guthabencode direkt auf das «digitale Portemonnaie» der App geladen wird. Als Sicherheitsvorkehrung können maximal 3000 Franken aufgeladen werden und das Mindestalter der Benutzerinnen und Benutzer ist auf zwölf Jahre festgelegt.

Die Bluetooth-Technologie ist an und für sich eine sichere Technologie, da sie sowohl für die Authentifizierung ein Passwort als auch Verschlüsselungen verwendet, aber sie birgt trotzdem Gefahren: So verbreitete sich der erste Smartphone-Virus «Cabir» auf diesem Weg und das Spionageprogramm «Flame», das der IKT-Sicherheitsdienstleister «Kaspersky» im Mai 2012 entdeckte, konnte unter anderem über Bluetooth auf das Adressbuch zugreifen.

Zusammengefasst ist Mobile Payment ein einfacher und praktischer Dienst. Das Risiko, dass das digitale Portemonnaie in falsche Hände gerät, ist nicht höher als bei einem herkömmlichen Geldbeutel und es ist im Gegensatz zu diesem zusätzlich noch durch einen PIN-Code geschützt. Der Nachteil besteht hingegen darin, dass andere, tückischere Angriffe zu erwarten sind. Im Netz tummeln sich Cyber-Kriminelle, die ständig neue Methoden entwickeln, um sich Zugriff auf alle diejenigen Geräte zu verschaffen, die mit dem Internet verbundenen und für ihre Zwecke lukrativ sind. Bezugslimiten mögen zwar die Angreifer momentan abschrecken, aber sobald grössere Summen in Aussicht gestellt sind, ist nicht auszuschliessen, dass mithilfe von Techniken wie «*Man-in-the Middle*» oder auch durch Social Engineering Angriffe stattfinden werden, bei denen die Geldbeträge den Weg auf ein Betrügerkonto finden.

Empfehlungen:

- Bluetooth bei Nichtgebrauch deaktivieren.
- Bezugslimiten tief halten.
- Sicherheitseinstellungen am Mobiltelefon aktivieren (z.B. PIN-Code).

Grundschutz Peripherie und Geräte:

https://www.melani.admin.ch/melani/de/home/schuetzen/sekundaere-grundschutz.html

6.2 Bekämpfung des Missbrauchs von Schweizer Telefonnummern und Domainnamen

Mit dem Aufkommen des Internets wurden neue Adressierungselemente im Fernmeldeverkehr generiert: Domainnamen und IP-Adressen. Während IP-Adressen nicht

durch staatliche Behörden verwaltet werden, wurde jedem Land eine Top-Level-Domain gemäss seines zweistelligen ISO-Kürzels zugeteilt, unter welcher es Domainnamen vergeben kann. Für die Schweiz ergab sich so die Länderdomain «.ch», welche vom – respektive im Auftrag des – Bundesamt für Kommunikation (BAKOM) verwaltet wird. Die Schweiz hat sich für ein sehr liberales Vergaberegime bezüglich Domainnamen entschieden. Grundsätzlich steht es allen Personen auf der ganzen Welt frei, einen Domainnamen unter «.ch» zu registrieren und zu nutzen. Um dennoch Missbrauch effizient und effektiv bekämpfen zu können, sind flankierende Massnahmen ergriffen worden: Zum Beispiel kann eine Schweizer Behörde, die im Rahmen ihrer Zuständigkeit handelt, von einem ausländischen Registranten verlangen, dass er oder sie eine Korrespondenzadresse in der Schweiz etabliert,[51] damit behördliche Schreiben zugestellt werden können. Dies, um meist langwierige Amts- oder Rechtshilfeverfahren zu vermeiden und Streitigkeiten über Zuständigkeit und anwendbares Recht aus dem Weg gehen zu können. Auf Schweizer Domains findet Schweizer Recht Anwendung. Über den vorgenannten Mechanismus kann dieses durchgesetzt werden. Dieser Prozess nimmt jedoch Zeit in Anspruch (man muss dem Registranten eine Frist geben, um der Aufforderung nachkommen zu können). Deshalb wurde für Fälle, in denen mit Hilfe von Schweizer Domainnamen akute Bedrohungen für Internetnutzer geschaffen werden, eine Kompetenz zur unmittelbaren Blockierung von Domainnamen bei *Phishing* und *Malware* geschaffen.[52] Die konsequente Umsetzung dieser Kompetenz – insbesondere auf Stufe Registerbetreiberin – hat nachweislich zur weiteren Steigerung der guten Reputation und der Sicherheit im Schweizer Domainraum geführt.[53]

Ausserdem erfahren auch althergebrachte Adressierungselemente neue Impulse: Die *Internettelefonie* blieb nicht lange exklusiv im Internet. Mittlerweile laufen bei fast allen herkömmlichen Telefonanschlüssen die Anrufe über *IP-Netze*, sobald diese die «letzte Meile» vom Kunden ins Netz des Anbieters zurückgelegt haben. Entsprechend gibt es viele Möglichkeiten, die Schnittstellen zwischen Internet und Telefonnetz zu beanspruchen: Zum Beispiel können via Internettelefonie Gespräche auf Telefonanschlüsse in fernen Ländern zum dortigen Lokaltarif getätigt werden, weil der Anbieter einen Anschluss im Land unterhält. Oder ein internationaler Anbieter kann eine Kunden-Hotline zum Ortstarif anbieten, weil er in jedem Land eine Nummer gelöst hat.

Um ausgehende Anrufe tätigen zu können, braucht man in technischer Hinsicht jedoch keine eigene Rufnummer mehr. Die Nummer, welche bei einem Anruf angezeigt wird, ist entsprechend frei bestimmbar und ermöglicht Nummern-*Spoofing*. Das Staatssekretariat für Wirtschaft (SECO) verzeichnete in den letzten Jahren einen starken Anstieg von Beschwerden wegen unerbetenen Werbeanrufen.[54] Gegen diese Anrufe kann durch behördliche Massnahmen auf Rufnummernebene jedoch nichts unternommen werden. Um

---

[51] Art. 23 Abs. 3 VID: https://www.admin.ch/opc/de/classified-compilation/20141744/index.html#a23 (Stand: 29. Februar 2016).

[52] Art. 15 VID: https://www.admin.ch/opc/de/classified-compilation/20141744/index.html#a15 (Stand: 29. Februar 2016).

[53] https://www.switch.ch/de/news/cybercrime/ (Stand: 29. Februar 2016).

[54] http://www.seco.admin.ch/themen/00645/00653/05456/index.html?lang=de; siehe auch die Broschüre «Ruhe vor unerbetenen Werbeanrufen»: https://www.seco.admin.ch/seco/de/home/Publikationen_Dienstleistungen/Publikationen_und_Formulare/Werbe_und_Geschaeftsmethoden/Unlauterer_Wettweberb/ruhe-vor-unerbetenen-werbeanrufen_seco.html (Stand: 29. Februar 2016).

gegen diese Anrufer vorgehen zu können, bedarf es eines meist langwierigen internationalen Verfahrens – typischerweise gegen die Anbieter der Produkte und Dienstleistungen, die telefonisch beworben werden. Bei betrügerischen Anrufern wie denjenigen, die sich als Microsoft Support ausgeben[55] ist die Bekämpfung und Verfolgung der Täter kaum praktikabel. Die Inanspruchnahme internationaler Rechtshilfe stellt eine hohe Hürde dar.

Oft wird auch nach einmaligem Klingeln wieder aufgelegt. So werden die Angerufenen zu einem Rückruf verleitet. Hierzu benötigen die Anrufer eine gültige Telefonnummer. Wenn es sich dabei um eine Schweizer Nummer handelt, ist die Chance ungemein grösser, dass jemand zurückruft, als wenn es sich um ausländische Nummern handelt. Oft geben Betrüger auf Webseiten, die sie für die Abwicklung ihrer Taten verwenden, funktionierende Schweizer Telefonnummern an, um bei potenziellen Opfern Vertrauen zu erwecken.

Das Staatssekretariat für Wirtschaft (SECO) bekämpft unlautere Werbeanrufe durch Strafklagen (oft gegen unbekannt) und im Zusammenhang mit Preselection-Anbietern mit Zivilklagen.[56] Im Übrigen hat es in mehreren Fällen unter Androhung von rechtlichen Massnahmen erreicht, dass missbräuchlich verwendete Rufnummern von Fernmeldedienstunternehmen entzogen wurden.

Telefonnummern werden auf der obersten Ebene vom BAKOM verwaltet. Es vergibt diese in 10‘000er-Blöcken an Fernmeldedienstunternehmen (auch ausländische, die lediglich eine Korrespondenzadresse in der Schweiz haben müssen), die sie dann in kleineren Blöcken oder einzeln an ihre (End-)Kunden im In- und Ausland weitervermitteln. In Anbetracht von erhöhten Meldungen bezüglich Missbrauch von Schweizer Telefonnummern wurden die Möglichkeiten des BAKOM zum Widerruf der Zuteilung letztes Jahr erweitert.[57]

Der Bundesrat hat am 11. Dezember 2015 zudem die Vernehmlassung zu einer Änderung des Fernmeldegesetzes und des Bundesgesetztes über den unlauteren Wettbewerb (UWG) eröffnet. Gegenstand der Änderung ist u.a. das technische und rechtliche Instrumentarium gegen unerbetene Werbeanrufe zu verbessern. So sollen die Fernmeldedienstanbieterinnen wie bei der Spam-Bekämpfung zur Filterung von Werbeanrufen verpflichtet werden.

---

55 Siehe MELANI-Newsletter https://www.melani.admin.ch/melani/de/home/themen/fake_support.html (Stand: 29. Februar 2016).

56 http://www.seco.admin.ch (Stand: 29. Februar 2016).

57 Siehe Artikel 11 der Verordnung über die Adressierungselemente im Fernmeldebereich (AEFV): https://www.admin.ch/opc/de/classified-compilation/19970410/index.html#a11 (Stand: 29. Februar 2016).

Schlussfolgerung:

Je liberaler die Vergabe von Adressierungselementen, desto einfacher müssen auch die Kompetenzen und Massnahmen zu ihrem Widerruf bei Missbrauch ausgestaltet sein, damit das Vertrauen in die Adressierungselemente einer Vergabestelle gewahrt werden kann. Dieses Prinzip haben auch einige Anbieter von neuen Domainnamenräumen (New gTLDs) erkannt: Bei Domainnamen, die günstig und einfach bezogen werden können und deshalb auch kriminelle Akteure anziehen, gehen Registrierungsstellen beim Widerruf teilweise ziemlich aggressiv vor. Würden sie das nicht tun, könnte die Reputation ihrer TLD sinken. Die Internetnutzer könnten Adressen mit der entsprechenden Endung prinzipiell meiden oder sogar bereits auf technischer Ebene filtern. Dies könnte in der Folge auch seriöse Akteure von der Registrierung solcher Adressen abhalten.

Diese Problematik mag auf Telefonnummern nicht im gleichen Masse zutreffen – es ist jedoch zu bedenken, dass Schweizer Telefonnummern (zumindest innerhalb der Schweiz) traditionell ein hohes Vertrauen entgegengebracht wird. Um dieses Vertrauen zu bewahren muss Missbrauch möglichst verhindert und im Ereignisfall effektiv bekämpft werden.

6.3 Wenn Hacker im Kinderzimmer spielen

Das Angebot an Spielsachen, mit denen Kinder die Welt der Erwachsenen nachahmen können, war schon immer vielfältig: Die Kleinen konnten Babypuppen wiegen und füttern, mit batteriebetriebenen Spielautos herumflitzen, Miniaturhäuser einrichten und in ihrer eigenen Küche Leckereien aus Plastik backen. Heutzutage hat auch die Digitalisierung ihren Einfluss auf die Vorlieben der Kinder: Verbringen die Eltern viel Zeit am Computer und am Smartphone, eifern ihnen die Kinder bald auch hier nach, und die Spielzeugbranche passt sich an, indem sie Tablets und High-Tech-Puppen für die Kleinsten auf den Markt bringt. Das Internet der Dinge ist mitsamt seinen Vorzügen und Gefahren im Kinderzimmer angekommen.

Das in Hongkong ansässige Unternehmen «VTech Holdings Ltd.», das technologische Anwendungen für Kinder und digitale Spiele produziert, wurde im November 2015 Opfer eines der grössten Hackerangriffe aller Zeiten. Davon betroffen war die Datenbank des App-Stores «Learning Lodge», von welchem Apps, Spiele, Videos und E-Books heruntergeladen werden können. Ebenfalls betroffen waren die Datenbanken des sozialen Netzwerks «Kid Connect», mit dem Eltern und Kinder über Tablets und Smartphones miteinander kommunizieren können, sowie die Datenbank «PlanetVTeach».

Nachdem ein Hacker sich mittels *SQL-Injektion* die Root-Rechte und dadurch Zugriff auf 5 Millionen Konten von Erwachsenen und 6,3 Millionen Konten von Minderjährigen verschafft hatte, kontaktierte er die Online Media Website «Motherboard», informierte diese über seine Tat und hielt fest, dass er mit dem Angriff auf die mangelhaften Sicherheitsvorkehrungen der Firma aufmerksam machen wollte. VTech gab zu, sein Netzwerk nicht optimal gesichert zu haben und bestätigte, dass Namen, Wohn-, E Mail- und IP-Adressen, Passwörter und geheime Antworten auf Sicherheitsfragen von Eltern sowie Namen, Geschlecht und Geburtsdatum von Kindern vom Datenklau betroffen waren. Sozialversicherungs-, Fahrausweis- oder Kreditkartennummern seien hingegen keine gestohlen worden. Das

Unternehmen äusserte sich nicht zu den Anschuldigungen, dass Fotos und Videochats von Kindern in falsche Hände geraten seien.

Die japanische Firma «Sanrio», der die berühmte Marke «Hello Kitty» gehört, war ebenfalls von einem Vorfall betroffen. Ende November wurden von ihrer Datenbank persönliche Daten von 3,3 Millionen Benutzern gestohlen. Auch in diesem Fall waren offenbar ungenügende Sicherheitsvorkehrungen implementiert.

VTech und Kittyleaks sind keine Einzelfälle. Auch «Mattel» und das Startup-Unternehmen «Toy-Talk» schlossen Sicherheitslücken, die es laut IKT-Sicherheitsexperten ermöglicht hätten, die interaktive Puppe «Hello Barbie» als Spionagemittel zu verwenden. Die Puppe, die via WLAN mit dem Internet verbunden ist, kann interaktive Gespräche führen, besitzt hierzu ein Mikrofon und gleicht diese Daten via WLAN mit einem Server bei einer Drittfirma ab. Durch das Ausnützen dieser Sicherheitslücke wäre es beispielsweise möglich gewesen, die Kontrolle über das Mikrofon zu übernehmen.

Diese Beispiele zeigen, dass in der heutigen Gesellschaft das Bewusstsein darüber, welche Daten besonders schützenswert sind, noch nicht überall gleich stark entwickelt ist. Gerade Daten von Kindern sind besonders sensibel und müssen auch besonders gut geschützt werden. Spielsachen, die direkt ans Internet angeschlossen werden, sind ein relativ neues Phänomen und werden sich in den kommenden Jahren stark entwickeln. Es ist zu hoffen, dass nicht nur in neue Features investiert wird, sondern auch in deren Sicherheit.

Empfehlungen:

- Passwörter häufig wechseln.
- Bedenken, dass jedes mit dem Internet verbundene Gerät ein Risiko darstellen kann.
- Kinder zum Thema Sicherheit aufklären.
- Für die Bestellung und Bezahlung von Produkten für Kinder nicht die Angaben des Kindes verwenden.

INFO

Grundschutz Verhaltensregeln:

https://www.melani.admin.ch/melani/de/home/schuetzen/verhaltensregeln.html

7 Politik, Forschung, Policy

7.1 Parlamentarische Vorstösse

Geschäft	Nummer	Titel	Eingereicht von	Datum Einreichung	Rat	Amt	Stand Beratung & Link
Ip	15.4073	Ist die Armee wirklich in der Lage, den Schweizer Cyberspace zu schützen?	Derder Fathi	25.09.2015	NR	VBS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20154073

Po	15.5064	Service-public-Debatte. Auf die Herausforderungen der Informationsgesellschaft antworten, ohne innovative Medienkanäle zu diskriminieren	Balthasar Glättli	25.09.2015	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20154064
Po	15.3980	Industrie 4.0. Beurteilung der Chancen und Risiken	Grüne Fraktion	24.09.2015	NR	WBF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153980
Mo	15.3979	Industrie 4.0. Beurteilung der Chancen und Risiken	Adèle Thorens Goumaz	24.09.2015	NR	WBF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153979
Po	15.3957	Massnahmen gegen den illegalen Internethandel mit bedrohten Arten	Guillaume Barrazone	24.09.2015	NR	EDI	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153957
Ip	15.3917	Crowdfunding. Im Spannungsfeld von wirtschaftlichen Innovationen und Anlegerschutz	Konrad Graber	23.09.2015	SR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153917
Mo	15.3903	Keine weiteren Verzögerungen für Online-Casinos	Peter Schilliger	23.09.2015	NR		https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153903
Pl	15.482	Gleichbehandlung von privaten Rundfunkanbietern und privaten Online-Anbietern	Thomas Matter	22.09.2015	NR	KVF-NR	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20150482
Ip	15.3959	Zeitlich begrenzte Weiterführung von E-Mail-Dienstleistungen nach Vertragskündigung	Anita Fetz	24.09.2015	SR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153959
Ip	15.3882	Gesundheitliche Risiken des Einsatzes von IKT in der Informationsgesellschaft	Thomas Böhni	22.09.2015	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153882
Fr	15.5466	Engagement der Post bei der Entwicklung einer E-Voting Plattform	Cédric Wermuth	15.09.2015	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20155466
DA	15.1059	Dringende Finanzhilfe des Bundes infolge des Cyberangriffs auf TV5 Monde	Didier Berberat	10.09.2015	SR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20151059
Ip	15.3822	Kinderkrankheiten des neuen Abonnements des öffentlichen Verkehrs «Swiss Pass» schnell kurieren	Jean Christophe Schwaab	09.09.2015	NR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153822
Mo	15.3799	Netzbeschluss und E-Vignette	Kommission für Verkehr und Fernmeldewesen SR	18.08.2015	SR	UVEK	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153799
Ip	15.4062	Projekte zum Bürokratieabbau zügig umsetzen	Hans Grunder, Fraktion BD	25.09.2015	NR	WBF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20154062

Ip	15.3994	Massnahmen zur Sicherung des Erfolgs von IKT-Projekten der Bundesverwaltung. Überbordende Personalstellungen	Thomas Maier, Martin Bäumle	24.09.2015	NR	EFD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153994
Po	15.4045	Recht auf Nutzung der persönlichen Daten. Recht auf Kopie	Derder Fathi	25.09.2015	NR	EJPD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20154045

7.2 Deutsches IT-Sicherheitsgesetz

Am 25 Juli 2015 ist das breit diskutierte «Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)» in Deutschland in Kraft getreten. Es hat zum Ziel, das IKT-Sicherheitsniveau stark anzuheben und damit einen Beitrag zur Sicherheit der Wirtschaft und der Privatanwender zu leisten.[58] Adressaten des Gesetzes sind hauptsächlich die Betreiber Kritischer Infrastrukturen sowie die Betreiber von nicht rein privaten Webseiten. Das Gesetz führt für Betreiber Kritischer Infrastrukturen Pflichten zur Absicherung ihrer IKT nach dem Stand der Technik und zur Meldung erheblicher IKT-Sicherheitsvorfälle ein. Mit der «Zentralen Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen» wird beim Bundesamt für Sicherheit in der Informationstechnik (BSI) das kontrollierende Organ dazu geschaffen. Verstösse gegen die neu statuierten Pflichten (z. B. nicht erfolgte, nicht richtige, nicht vollständige oder nicht rechtzeitige Meldungen) werden künftig mit Bussgeld bis zu 100‘000 Euro geahndet.

Während der allgemeine Zweck des IT-Sicherheitsgesetzes mit der signifikanten Verbesserung der Sicherheit informationstechnischer Systeme in Deutschland und dem Schutz kritischer Infrastrukturen umschrieben wird, sind die konkreten Ziele des stark nebenstrafrechtlich geprägten Erlasses nicht auf Anhieb ersichtlich. Ob der Fokus der Durchsetzung auf der Überprüfung der Rechtsunterworfenen bezüglich Erfüllung der Vorgaben zum Schutz verschiedener Kategorien von schützenswerten (personenbezogenen) Daten oder eher auf die Einhaltung der Meldepflicht von IKT-Vorfällen (oder auf beides) gelegt wird, ist noch nicht absehbar. Die zuständigen Stellen werden insbesondere zur Verhältnismässigkeit und dem unbestimmten Rechtsgriff «Stand der Technik» erst eine Anwendungspraxis und entsprechende Beurteilungskriterien erarbeiten müssen.

Für die Schweiz hat das IT-Sicherheitsgesetz keine direkte Auswirkung, da es sich um deutsches Recht handelt. Allerdings sind mit der Erarbeitung einer EU-Richtlinie über Netz- und Informationssicherheit (NIS Richtlinie) ähnliche Bestrebungen im Gange (z. B. Einführung einer Meldepflicht), was schliesslich im Rahmen des autonomen Nachvollzugs von EU-Recht durch die Schweiz auch zu einer hiesigen Übernahme von solchen Vorschlägen führen kann. Schweizer Unternehmen, die Tochtergesellschaften in Deutschland führen, welche neu dem IT-Sicherheitsgesetz unterstellt sind, müssen sich allerdings bereits früher mit der Thematik auseinandersetzen. Es ist nicht auszuschliessen, dass Ermittlungen gegen Tochterunternehmen bei möglichen Verstössen gegen das Gesetz Kreise bis ins schweizerische Mutterhaus ziehen können.

[58] http://dipbt.bundestag.de/extrakt/ba/WP18/643/64396.html (Stand: 29. Februar 2016).

7.3 NCS-Tagung

Am 2. November 2015 fand im «Stade de Suisse» in Bern die zweite Tagung zur «Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (Nationale Cyber-Strategie; NCS)» statt. Über 250 Teilnehmerinnen und Teilnehmer aus Wirtschaft, Politik, Verwaltung und Gesellschaft informierten sich zum Stand der NCS und erhielten einen Eindruck über die Massnahmen, welche die Schweiz zum Schutz gegen Cyber-Risiken ergriffen hat. Nationale und internationale Referenten erörterten die verschiedenen Aspekte der Cyber-Risiken. Unter anderem zeigte das GovCERT.ch auf, wie eine Vorfallanalyse konkret abläuft. MELANI stellte den Prototypen des Lagebildes vor, welches im Rahmen der NCS entwickelt wird. Ein Schwerpunkt der Tagung lag zudem auf der Bekämpfung von Cyberkriminalität. Die Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK) präsentierte den Stand der Arbeiten bei der Erstellung einer nationalen Fallübersicht, und die Staatsanwaltschaft Zürich lieferte Beispiele aus der täglichen Praxis von Strafverfolgungsbehörden. Auf grosses Interesse stiess auch die Live-Demonstration eines Hackers, der aufzeigte, wie er systematisch Steuerungsanlagen für industrielle Systeme und deren Schwachstellen identifizieren kann.

Die Tagung hat deutlich gemacht, dass der Schutz der Schweiz vor Cyber-Risiken eine grosse Herausforderung bleibt. Sie hat aber auch aufgezeigt, dass in den letzten Jahren Fortschritte erzielt werden konnten. Der Schlüssel für den Erfolg liegt in einer guten Koordination der zahlreichen involvierten Akteure. Die Stärkung dieser Zusammenarbeit wird auch im nächsten Jahr das zentrale Anliegen der NCS sein.

8 Publizierte MELANI Produkte

MELANI stellt neben den Halbjahresberichten für die breite Öffentlichkeit eine Anzahl verschiedenster Produkte zur Verfügung. Die folgenden Unterkapitel bieten eine Übersicht über die im Berichtszeitraum erstellten Blogs, Newsletter, Checklisten, Anleitungen und Merkblätter.

8.1 GovCERT.ch Blog

8.1.1 TorrentLocker Ransomware targeting Swiss Internet Users

21.01.2016 - On Wednesday, Jan 20 2016, we have noticed a major spam campaign hitting the Swiss cyberspace, distributing a ransomware called TorrentLocker. We have already warned about similar TorrentLocker attacks against Swiss internet users last year via Twitter. TorrentLocker is one of many ransomware families that encrypts any local file on a victim's computer and demands that the victim pays a ransom to have his files decrypted again. Since some ransomware families do not only encrypt files stored locally on the infected machine but also on any mapped network share, ransomware also represent a serious threat to corporate networks. To make sure that the malicious email goes through spam filters and gets opened by the recipient swiftly, the TorrentLocker gang is using a handful of tricks.

➔ http://www.govcert.admin.ch/blog/17/torrentlocker-ransomware-targeting-swiss-internet-users

8.1.2 Ads on popular Search Engine are leading to Phishing Sites

23.11.2015 - GovCERT.ch and Reporting and Analysis Centre for Information Assurance (MELANI) are aware of an ongoing phishing campaign that is targeting a large credit card issuer in Switzerland. What makes this phishing campaign somehow unique is the way how the phishers are advertising their phishing sites: while traditionally phishing sites are being promoted through phishing emails that are usually being sent to a large audience, the phishers are using advertisements (Ads) on a popular search engine to promote their phishing sites.

➔ http://www.govcert.admin.ch/blog/16/ads-on-popular-search-engine-are-leading-to-phishing-sites

8.1.3 Update on Armada Collective extort Swiss Hosting Providers

08.11.2015 - During the recent days and weeks, various Hosting Providers in Switzerland have been blackmailed by a hacking group that calls themselves Armada Collective. As the Distributed Denial of Service (DDoS) attacks carried out by the Armada Collective have grown in terms of intensity and frequency, we have decided to publish an update to our previous blog post about Armada Collective, providing a short overview on the current situation in Switzerland and some additional information.

➔ http://www.govcert.admin.ch/blog/15/update-on-armada-collective-extort-swiss-hosting-providers

8.1.4 Armada Collective blackmails Swiss Hosting Providers

22.09.2015 - Earlier this year, we warned about DD4BC, a hacker group that tried to extort money from high value targets in Switzerland and abroad. While DD4BC is still around, MELANI / GovCERT.ch as well as the Cybercrime Coordination Unit Switzerland (CYCO) did receive several independent reports from hosting Providers in Switzerland recently that they are being blackmailed by a hacker group that calls themselves Armada Collective.

➔ http://www.govcert.admin.ch/blog/14/armada-collective-blackmails-swiss-hosting-providers

8.1.5 Swiss Advertising network compromised and distributing a Trojan

22.09.2015 - On September 11, 2015, MELANI / GovCERT.ch got informed by security researcher Kafeine about a popular advertising network in Switzerland that obviously got compromised by cybercriminals, leading to an exploit kit called Niteris.

➔ http://www.govcert.admin.ch/blog/13/swiss-advertising-network-compromised-and-distributing-a-trojan

8.1.6 Analysing a new eBanking Trojan called Fobber

11.09.2015 - Some weeks ago we read an interesting blog by Malwarebytes about Fobber, a new e-banking focussed malware in the arena that seems to be a Tinba spinoff. We decided to have a closer look at it to find out whether Swiss critical infrastructures are targeted by it. We'd like to share our findings with you, because it contains some interesting advanced techniques that at the same time are implemented in a comparably simple way; we think this makes Fobber an ideal case study.

➔ http://www.govcert.admin.ch/blog/12/analysing-a-new-ebanking-trojan-called-fobber

8.2 MELANI Newsletter

Im zweiten Halbjahr 2015 hat MELANI folgende Newsletter publiziert:

8.2.1 TeslaCrypt: Angriffe, die Daten verschlüsseln und danach Lösegeld fordern reissen nicht ab

03.12.2015 - Diverse Meldungen in den letzten Tagen über die Schadsoftware TeslaCrypt an die Melde- und Analysestelle Informationssicherung MELANI zeugen von einer steigenden Verbreitung dieser Variante von Schadsoftware, welche Daten verschlüsselt und anschliessend ein Lösegeld fordert.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/teslacrypt.html

8.2.2 Lösegeldzahlungen finanzieren und stärken DDoS-Angriffsinfrastruktur

19.11.2015 - Erpressung ist derzeit eine beliebte Masche der Cyberkriminellen, die auf einen schnellen finanziellen Gewinn aus sind. Über verschiedene Angriffsarten wird versucht, von einem Opfer Geld zu erpressen. Dazu gehören auch DDoS-Angriffe, mit welchen die Verfügbarkeit von Webseiten und –diensten gestört wird. MELANI berichtete dieses Jahr bereits mehrfach über solche Attacken und damit einhergehende Erpressungen der Gruppen

Armada Collective und DD4BC, welche in der Schweiz für mediales Aufsehen gesorgt haben. MELANI rät dringend davon ab, auf die Forderungen der Erpresserbanden einzugehen.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/ddos_extortion.html

8.2.3 21. MELANI-Halbjahresbericht widmet sich dem Schwerpunktthema «Website-Sicherheit»

29.10.2015 - Der 21. Halbjahresbericht MELANI widmet sich unter Anderem Spionageangriffen, von denen auch die Schweiz betroffen war, den nach wie vor präsenten Phishing-Angriffen, sowie dem Schwerpunktthema «Website-Sicherheit». Das Schwerpunktthema ist eine von mehreren Neuerungen, die der Halbjahresbericht erfahren hat.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/21-MELANI-halbjahresbericht.html

8.2.4 Meldeportal gegen Phishing

29.07.2015 - In den vergangenen Jahren ist die Zahl der durch die Melde- und Analysestelle Informationssicherung MELANI bearbeiteten Anfragen bezüglich Phishing stark angestiegen. Bei den meisten Anfragen wurden uns Phishing E-Mails und Phishing Webseiten gemeldet, welche Kunden von Finanzinstituten in der Schweiz, aber auch international bekannte Internet-Plattformen (wie z.B. Social Networks, E-Mail Dienste oder Online Payment Service Provider) im Visier haben. Um die Vielzahl der eingehenden Meldungen betreffend Phishing effizienter bearbeiten zu können, hat die Melde- und Analysestelle Informationssicherung MELANI eine Website aufgeschaltet, auf welcher vermeintliche Phishing Seiten gemeldet werden können.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/meldeportal_gegen_phishing.html

8.3 Checklisten und Anleitungen

Im zweiten Halbjahr 2015 hat MELANI keine neuen Checklisten und Anleitungen publiziert.

9 Glossar

Begriff	Erklärung
Abuse-Stelle	Stelle an welche Beschwerden (beispielsweise der Missbrauch einer Webseite) gesendet werden können
Application Programming Interface (API)	Ein Application Programming Interface (API) (zu Deutsch eine Programmierschnittstelle) ist ein Programmteil, der von einem Softwaresystem anderen Programmen zur Anbindung an das System zur Verfügung gestellt wird.

Autonome Systeme	Ein autonomes System ist eine Ansammlung von IP-Netzen, welche als Einheit verwaltet werden und über ein gemeinsames internes Routing-Protokoll verbunden sind.
Backdoor	Backdoor (deutsch: Hintertür) bezeichnet einen Teil einer Software, der es Benutzern ermöglicht, unter Umgehung der normalen Zugriffssicherung Zugang zum Computer oder einer sonst geschützten Funktion eines Computerprogramms zu erlangen.
Backbone	Telekommunikationsnetz mit sehr hoher Übertragunsrate. Der Internet-Backbone bezeichnet den «Kern» des Internets.
Backup	Backup (deutsch Datensicherung) bezeichnet das Kopieren von Daten in der Absicht, diese im Fall eines Datenverlustes zurückkopieren zu können.
Bibliotheken	Eine Programmbibliothek bezeichnet in der Programmierung eine Sammlung von Unterprogrammen/-Routinen, die Lösungswege für thematisch zusammengehörende Problemstellungen anbieten.
Bitcoin	Bitcoin ist ein weltweit verfügbares dezentrales Zahlungssystem und der Name einer virtuellen Geldeinheit.
Bluetooth	Eine Technologie, die eine drahtlose Kommunikation zwischen zwei Endgeräten ermöglicht und vor allem bei Mobiltelefonen, Laptops, PDAs und Eingabegeräten (z. B. Computermaus) zur Anwendung gelangt.
Booter- oder Stresser-Dienste	Service mit welchem auch technisch unerfahrene Benutzer DDoS-Angriffe durchführen können.
Border Gateway Protocol (BGP)	Das Border Gateway Protocol ist das im Internet eingesetzte Routingprotokoll und verbindet autonome Systeme miteinander.
Botnet	Ursprung im slawischen Wort für Arbeit (Robota). Bezeichnet ein Programm, das bestimmte Aktionen nach dem Empfang eines Befehls selbstständig ausführt. So genannte Malicious Bots können kompromittierte Systeme fernsteuern und zur Durchführung beliebiger Aktionen veranlassen.
Bug Bounty	Ein Bug-Bounty-Programm ist eine von wahlweise Unternehmen, Interessenverbänden, Privatpersonen oder Regierungsstellen betriebene Initiative zur Identifizierung, Behebung und Bekanntmachung von Fehlern in Software unter Auslobung von Sach- und/oder

	Geldpreisen für die Entdecker.
Bus	Ein Bus ist ein System zur Datenübertragung zwischen mehreren Teilnehmern über einen gemeinsamen Übertragungsweg, bei dem die Datenübertragung durch eine von Sender und Empfänger unabhängige, vereinheitlichte Kommunikationsschicht übernommen wird.
Captcha	CAPTCHA ist die Abkürzung für Completely Automated Public Turing test to tell Computers and Humans Apart. CAPTCHAs werden verwendet, um zu entscheiden, ob das Gegenüber ein Mensch oder eine Maschine ist.
CERTs	Ein Computer Emergency Response Team (CERT), deutsch Computersicherheits-Ereignis- und Reaktionsteam ist eine Gruppe von Sicherheitsfachleuten, die bei der Lösung von konkreten IT-Sicherheitsvorfälle Lösungsansätze anbietet
USB-Stick	Kleine Datenspeichergeräte, die über die USB-Schnittstelle an einen Rechner angeschlossen werden.
Cloud	Cloud Computing (Synonym: Cloud IT, deutsch etwa Rechnen in der Wolke) ist ein Begriff aus der Informationstechnik (IT). Die IT-Landschaft wird durch den Anwender nicht mehr selbst betrieben/bereitgestellt, sondern über einen oder mehrere Anbieter bezogen. Die Anwendungen und Daten befinden sich nicht mehr auf dem lokalen Rechner oder im Firmenrechenzentrum, sondern in der Wolke (Cloud). Der Zugriff auf diese entfernten Systeme erfolgt über ein Netzwerk.
Command&Control Infrastruktur	Die meisten Botnet können von einem Botmaster über einen Kommunikationskanal überwacht werden und Befehle empfangen. Dieser wird als Command and Control-Server bezeichnet.
Contentmanagementsysteme	Ein Content-Management-System (kurz: CMS, übersetzt: Inhaltsverwaltungssystem) ist ein System, das die gemeinschaftliche Erstellung und Bearbeitung von Inhalt, bestehend aus Text- und Multimedia-Dokumenten, ermöglicht und organisiert, meist für das World Wide Web. Ein Autor kann ein solches System auch ohne Programmier- oder HTML-Kenntnisse bedienen. Der darzustellende Informationsgehalt wird in diesem Zusammenhang als Content (Inhalt) bezeichnet.
Crimeware Kit	Baukasten , der auch unerfahrenen Benutzern erlaubt, auf einfache Art und Weise eine Schadsoftware zusammenzustellen.
DDoS-Angriff	Distributed-Denial-of-Service Attacke Eine DoS Attacke, bei der das Opfer von vielen verscheiden Systemen aus

	gleichzeitig angegriffen wird.
Defacement	Verunstaltung von Webseiten.
Doxing	Doxing ist das internetbasierte Zusammentragen und anschließende Veröffentlichen personenbezogener Daten, zumeist mit bösartigen Absichten gegenüber den Betroffenen.
Drive-By-Infektionen	Infektion eines Computers mit Malware allein durch Besuch einer Web-Seite. Vielfach beinhalten die betroffenen Websites seriöse Angebote und sind zwecks Verteilung der Malware zuvor kompromittiert worden. Die Infektion erfolgt meistens durch das Ausprobieren von Exploits für vom Besucher noch nicht geschlossene Sicherheitslücken.
End-to-End Verschlüsselung	Methode, bei der nur an den Endpunkten ver-/entschlüsselt wird.
ERP-System	Enterprise-Resource-Planning (ERP) bezeichnet die unternehmerische Aufgabe, Ressourcen wie Kapital, Personal, Betriebsmittel, Material, Informations- und Kommunikationstechnik, IKT-Systeme im Sinne des Unternehmenszwecks rechtzeitig und bedarfsgerecht zu planen und zu steuern.
Exploit-Kit	Baukasten, mit denen Kriminelle Programme, Scripts oder Codezeilen generieren können, mit denen sich Schwachstellen in Computersystemen ausnutzen lassen.
Firmware	Befehlsdaten zur Steuerung eines Gerätes (z. B. Scanner, Grafikkarten, usw.), die in einem Chip gespeichert sind. Diese Daten können in der Regel über Upgrades geändert werden.
Flash	Adobe Flash (kurz Flash, ehemals Macromedia Flash) ist eine proprietäre integrierte Entwicklungsumgebung zur Erstellung multimedialer Inhalte. Flash findet heutzutage auf vielen Websites Anwendung, sei es als Werbebanner, als Teil einer Website z. B. als Steuerungsmenü oder in Form kompletter Flash-Seiten.
Honeypot	Als Honeypot (deutsch: Honigtopf) wird in der Computersicherheit ein Computerprogramm oder ein Server bezeichnet, das Netzwerkdienste eines Computers, eines ganzen Rechnernetzes oder das Verhalten eines Anwenders simuliert. Honeypots werden eingesetzt, um Angreifer anzulocken und dadurch Informationen über deren Angriffsmuster und Angreifverhalten zu erhalten.

IKS-Systeme	Kontroll- oder Steuerungssysteme (IKS) bestehen aus einem oder mehreren Geräten, welche das Verhalten von anderen Geräten oder Systemen steuern, regeln und/oder überwachen. In der industriellen Produktion ist der Begriff «Industrielle Kontrollsysteme» (engl. Industrial Control Systems, ICS) geläufig.
Internettelefonie	Voice over IP. Telefonie über das Internet-Protokoll (IP). Häufig verwendete Protokolle: H.323 und SIP.
IP-Adresse	Adresse, welche einen Computer im Internet (oder einem TCP/IP-Netzwerk) identifiziert (Beispiel: 172.16.54.87).
Jailbreak	Mit Jailbreaking (englisch: Gefängnisausbruch) wird das Überwinden der Nutzungseinschränkungen auf Apple-Produkten mittels geeigneter Software bezeichnet.
JavaScript	Eine objektbasierte Scriptingsprache zur Entwicklung von Applikationen. JavaScripts sind im HTML-Code integrierte Programmteile, die bestimmte Funktionen im Internet Browser ermöglichen. Ein Beispiel kann das Kontrollieren von Benutzereingaben bei einem Webformular sein. So kann überprüft werden, ob alle eingegebenen Zeichen bei geforderter Angabe einer Telefonnummer auch wirklich Zahlen sind. Wie ActiveX Controls werden JavaScripts auf dem Rechner des Webseitenbesuchers ausgeführt. Neben nützlichen, lassen sich leider auch schädliche Funktionen programmieren. Im Gegensatz zu ActiveX werden JavaScripts von allen Browsern unterstützt.
KillDisk	Low Level-Formatierung zur sicheren und unwiederbringlichen Löschung von Daten auf einer Harddisk.
Kryptosysteme	Ein Kryptosystem ist ein System, dass zur Verschlüsselung eingesetzt wird. Kryptographie bedeutet ursprünglich die Wissenschaft der Verschlüsselung von Informationen.
Makros	Ein Makro ist in der Software-Entwicklung eine zusammengefasste Folge von Anweisungen oder Deklarationen, um diese mit nur einem einfachen Aufruf ausführen zu können.
Malware	Oberbegriff für Software, die schädliche Funktionen auf einem Rechner ausführt (wie beispielsweise Viren, Würmer, Trojanische Pferde). Siehe auch Malware.
Man-in-the Middle	Man-in-the-Middle Attacke. Attacke, bei der sich der Angreifer unbemerkt in den Kommunikationskanal zweier Partner hängt und dadurch deren

	Datenaustausch mitlesen oder verändern kann.
Mobile Payment	Mobile-Payment sind Bezahlvorgänge, bei denen mindestens der Zahlungspflichtige mobile elektronische Techniken zur Initiierung, Autorisierung oder Realisierung der Zahlung einsetzt.
NFC (Near Field Communication)	Die Near Field Communication ist ein Übertragungsstandard nach internationalem Standard zum kontaktlosen Austausch von Daten über kurze Strecken.
Patch	Eine Software, die den fehlerhaften Teil eines Programms durch einen fehlerfreien ersetzt und dadurch z. B. eine Sicherheitslücke behebt.
Phishing	Mittels Phishing versuchen Betrüger, an vertrauliche Daten von ahnungslosen Internet-Benutzern zu gelangen. Dabei kann es sich beispielsweise um Kontoinformationen von Online-Auktionsanbietern (z. B. eBay) oder Zugangsdaten für das E-Banking handeln. Die Betrüger nutzen die Gutgläubigkeit und Hilfsbereitschaft ihrer Opfer aus, indem sie ihnen beispielsweise E-Mails mit gefälschten Absenderadressen zustellen.
Programmable Logic Controller (PLC bzw. SPS)	Eine speicherprogrammierbare Steuerung (SPS) ist ein Gerät, das zur Steuerung oder Regelung einer Maschine oder Anlage eingesetzt wird und auf digitaler Basis programmiert wird.
QR-Codes	Der QR-Code ist eine Methode, Informationen so aufzuschreiben, dass diese besonders schnell maschinell gefunden und eingelesen werden können.
Ransomware	Malware, mit der die Besitzer der infizierten Rechner erpresst werden sollen (ransom: englisch für Lösegeld). Typischerweise werden Daten verschlüsselt und erst nach Lösegeldzahlungen der zur Rettung nötige Schlüssel vom Angreifer zur Verfügung gestellt.
Remote Access Tool	Die Fernwartungssoftware (englisch: Remote Administration Tool) stellt eine Anwendung des Konzeptes Fernwartung für beliebige Rechner oder Rechnersysteme dar.
Routers	Geräte aus dem Bereich Computernetzwerke, Telekommunikation oder auch Internet, die mehrere Rechnernetze koppeln oder trennen. Router werden beispielsweise in Heimnetzwerken eingesetzt und machen die Verbindung zwischen internem Netz und dem Intranet.

SCADA	Supervisory Control And Data Acquisition Systeme. Werden zur Überwachung und Steuerung von technischen Prozessen eingesetzt (z. B. Energie- und Wasserversorgung).
SmartMeter	Ein SmartMeter (deutsch: intelligenter Zähler) ist ein Zähler für Energie, der dem jeweiligen An-schlussnutzer den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit anzeigt, die auch an das Energieversorgungsunternehmen übertragen werden können.
Smartphone	Ein Smartphone ist ein Mobiltelefon, das mehr Computerfunktionalität und -konnektivität als ein herkömmliches fortschrittliches Mobiltelefon zur Verfügung stellt.
SMS	Short Message Service Dienst zum Versenden von Kurzmitteilungen (maximal 160 Zeichen) an Mobiltelefonbenutzer.
Spam	Unaufgefordert und automatisiert zugesandte Massenwerbung, worunter auch Spam-E-Mails fallen. Als Spammer bezeichnet man den Absender dieser Mitteilungen, während das Versenden selbst als Spamming bezeichnet wird.
Spearphishing	Gezielte Phishing Attacke. Dem Opfer wird zum Beispiel vorgegaukelt, mit einer ihr vertrauten Person via E-Mail zu kommunizieren.
Spoofing	Spoofing nennt man in der Informationstechnik verschiedene Täuschungsversuche in Computernetzwerken zur Verschleierung der eigenen Identität.
SQL-Injection	SQL-Injection (SQL-Einschleusung) bezeichnet das Ausnutzen einer Sicherheitslücke in Zusammenhang mit SQL-Datenbanken, die durch mangelnde Überprüfung von zu übermittelnden Variablen entsteht. Der Angreifer versucht dabei eigene Datenbankbefehle einzuschleusen, um Daten in seinem Sinne zu verändern oder Kontrolle über den Server zu erhalten.
Streaming	Streaming Media bezeichnet die gleichzeitige Übertragung und Wiedergabe von Video- und Audiodaten über ein Netzwerk.
Switch	Verteiler, der Netzwerksegmente miteinander verbindet
Top Level Domain	Jeder Name einer Domain im Internet besteht aus einer Folge von durch Punkte getrennten Zeichenfolgen. Die Bezeichnung Top-Level-Domain bezeichnet dabei den

	letzten Namen dieser Folge und stellt die höchste Ebene der Namensauflösung dar. Ist der vollständige Domain-Name eines Rechners bzw. einer Website beispielsweise de.example.com, so entspricht das letzte Glied (com) der Top-Level-Domain dieses Namens.
TOR	Tor ist ein Netzwerk zur Anonymisierung von Verbindungsdaten.
Trojanern	Trojanische Pferde (häufig als Trojaner bezeichnet) sind Programme, die im Verborgenen schädliche Aktionen ausführen und sich dabei für den Benutzer als nützliche Anwendung oder Datei tarnen.
VPN	Virtual Private Network Ermöglicht durch Verschlüsselung des Datenverkehrs eine sichere Kommunikation zwischen Rechnern über öffentliche Netzwerke (z. B. das Internet).
Watering Hole Attacken	Gezielte Infektion durch Schadsoftware über Web-sites, welche bevorzugt nur von einer spezifischen Benutzergruppe besucht werden.
Zero-Day Lücke	Lücke, welche noch nicht öffentlich bekannt ist.
Zertifikat	Ein digitales Zertifikat ist gewissermassen das Cyberspaceäquivalent eines Personalausweises und dient dazu, einen bestimmten öffentlichen Schlüssel einer Person oder Organisation zuzuordnen. Diese Zuordnung wird von der Zertifizierungsstelle beglaubigt, indem sie diese mit ihrer eigenen digitalen Unterschrift versieht.