GovCERT AUSTRIA

CERT.at

BERICHT INTERNET-SICHERHEIT ÖSTERREICH 2015

GESAMTAUSGABE

Wien, Februar 2016

INHALTSVERZEICHNIS

Impressum:

Medieninhaber und Verleger: nic.at GmbH, Computer Emergency Response Team Austria, Karlsplatz 1/3, 1010 Wien. Diese Publikation wurde in Kooperation mit dem Bundeskanzleramt erstellt. **Projektleitung**: Mag. Robert Schischka, CERT.at und Ing. Roland Ledinger, BKA. **Konzeption und Redaktion**: pantarhei corporate advisors (Mag. Markus Gruber, Patrick Radinger, Bakk.), **Herstellungsort**: Wien. Februar 2016.

1. VORWORT: STAATSEKRETÄRIN MAG.A SONJA STEßL


© BKA

Mag.a Sonja Steßl
Staatssekretärin für Digitales,
Verwaltung und Öffentlichen Dienst im Bundeskanzleramt

Das vergangene Jahr war gekennzeichnet von zahlreichen Cyber Angriffen, Datendiebstählen und Bedrohungen, die nicht nur weltweit für Schlagzeilen und Besorgnis sorgten, sondern auch in Österreich. Vor dem Hintergrund einer weiter steigenden Komplexität und der zunehmenden Vernetzung unseres Alltags wird die Frage der Sicherheit im Cyber Raum immer wichtiger. Die österreichische Bundesregierung hat bereits vor Jahren das Thema Cyber Sicherheit und die nationale wie auch internationale Absicherung des Cyber Raums zu einer der obersten Prioritäten erklärt.

In einer globalisierten Welt kann größtmögliche Sicherheit nur durch Vernetzung und Zusammenarbeit der einzelnen Institutionen und Unternehmen erreicht werden. Mit der Österreichischen Strategie für Cyber Sicherheit (ÖSCS) wurde 2013 ein umfassendes und proaktives Konzept zum Schutz des österreichischen Cyber Raums sowie der Menschen im virtuellen Raum beschlossen. Diese Strategie bildet seither das Fundament der gesamtstaatlichen Zusammenarbeit in diesem Bereich, die kontinuierlich ausgebaut und gestärkt wird.

Gerade in jüngster Vergangenheit hat sich diesbezüglich sehr viel in Österreich getan: Mit der Konstituierung der Cyber Sicherheit Plattform (CSP) im Bundeskanzleramt wurde eine zentrale, im Rahmen der ÖSCS beschlossene Maßnahme umgesetzt, die die Kooperation untereinander und insbesondere auch zwischen Wirtschaft und öffentlicher Verwaltung weiter intensiviert sowie bestehende Initiativen und Arbeitsgruppen zusammenführt. Durch die Einbindung von Wissenschaft und Forschung wird diese Zusammenarbeit vor dem Ziel der Erhöhung der Cyber Sicherheit Österreichs zusätzlich gestärkt. Ebenso zu einer Stärkung beitragen wird das Cyber Sicherheitsgesetz, an dessen Erstellung bereits gearbeitet wird. Dieses neue Gesetz soll die Österreichische Strategie für Cyber Sicherheit mit der Europäischen Richtlinie für Netzwerk- und Informationssicherheit (NIS) zusammenführen und den künftigen Rahmen für IKT Sicherheit in Österreich vorgeben.

Um gemeinsam die Chancen der digitalen Welt nutzen zu können, müssen gute und sichere Rahmenbedingungen geschaffen werden – Cyber Sicherheit ist hierzu eine wesentliche Säule. Nur durch eine gemeinsame Anstrengung der öffentlichen Verwaltung, der Wirtschaft und der Wissenschaft wird es uns gelingen, den Cyber Raum sicher und vertrauenswürdig zu gestalten, damit alle Österreicherinnen und Österreicher in größtem Ausmaß von den Vorteilen der digitalen Welt profitieren.

2. VORWORT: ING. ROLAND LEDINGER UND MAG. ROBERT SCHISCHKA

© HBF

Ing. Roland Ledinger
Leiter des Bereichs IKT-Strategie des Bundes im Bundeskanzleramt

© CERT.at

Mag. Robert Schischka
Leiter des Computer Emergency Response Teams (CERT.at)

Cyber Bedrohungen durch Angriffe über das Internet fanden auch 2015 in hoher Zahl statt und bekamen zunehmend Beachtung im gesellschaftlichen und medialen Diskurs. Das tägliche Leben verlagert sich immer stärker in Richtung Cyber Welt. Die damit einhergehenden Risiken kamen im Internetjahr 2015 deutlich zum Vorschein. Sowohl private NutzerInnen als auch Unternehmen waren Zielscheibe zahlreicher Cyber Angriffe, was die Relevanz sicherheitspolitischer Maßnahmen aufzeigt.

Im Internet-Sicherheitsbericht 2015 von CERT.at und GovCERT Austria machen die SicherheitsexpertInnen auf die steigende Bedeutung von Cyber Sicherheit aufmerksam. Der digitale Wandel vereinnahmt Menschen und Organisationen im täglichen Leben und Handeln zusehends. Zahlreiche Cyber Angreifer wollten daher 2015 den digitalen Fortschritt zu schadhaften Zwecken nutzen. So wurden beispielsweise sogenannte Distributed Denial-of-Service Attacken (DDoS) 2015 in zunehmend professionellem Ausmaß durchgeführt. Diese Angriffe legen Server im Internet durch eine gezielte Überlastung lahm. Die Angreifer versuchen in der Folge Erpressungen mittels E-Mails durchzuführen. Diese und andere derartige Entwicklungen in den letzten Monaten zeigen somit, dass die Strategien und Maßnahmen für Internetsicherheit in den nächsten Jahren in hohem Maß auf die neuen digitalen Gegebenheiten abgestimmt sein müssen.

Die Bedeutung der Arbeit von CERT.at sowie GovCERT und seinen ExpertInnen zur Prävention und Beratung bei Sicherheitslücken und -risiken gewinnt durch diese Vorgänge weiter an Bedeutung. Kontinuierliches Monitoring von sicherheitsrelevanten IT-Vorkommnissen in Österreich und die Kommunikation an die Öffentlichkeit sowie an alle relevanten Beteiligten sind eine wichtige Voraussetzung dafür, um notwendige Maßnahmen rechtzeitig treffen zu können. Dazu gehört auch die Vernetzung auf internationaler Ebene. Durch aktive Zusammenarbeit sind CERT.at und GovCERT Austria in wichtigen Partnerschaften mit CERTs auf der ganzen Welt vernetzt.

Auf Basis der Österreichischen Strategie für Cyber Sicherheit (ÖSCS) ist CERT.at aktiver Player einer sektor-übergreifenden Zusammenarbeit mit öffentlichen und privaten Kooperationspartnern. Durch die Cyber Sicherheit Plattform wurden erst kürzlich der Schutz von kritischen IKT-Infrastrukturen und die Ergreifung rascher Maßnahmen bei akuten Notfällen, gemeinsam mit der öffentlichen Verwaltung und der Privatwirtschaft, auf ein neues Level gehoben. Die Gemeinschaftsarbeit für Österreichs IT-Sicherheit kann daher als wichtiges Best-Practice Beispiel für den künftigen Umgang mit Cyber Sicherheitsbedrohungen angesehen werden und ist in dieser Form beispielgebend für ganz Europa.

Für eine verlässliche IT-Sicherheit in Österreich und in Europa braucht es einen gemeinsamen Schulterschluss von Gesellschaft, Wirtschaft und Staat. Denn ein kollektives Verständnis über die notwendigen Sicherheitsaspekte im Internetjahr 2016 – und darüber hinaus – sind Voraussetzung dafür, um die Vorteile und Chancen der Digitalisierung in Österreich bestmöglich nutzen zu können.

3. CYBER SICHERHEIT GLOBAL: DIE WELT IST IM WANDEL

Das Internetjahr 2015 war von langfristigen und globalen Megatrends gezeichnet. Sie sind Treiber des digitalen Wandels und nehmen auch großen Einfluss auf Entwicklungen der Cyber Sicherheit auf globaler Ebene. Die Digitalisierung und damit einhergehende Begriffe wie Industrie 4.0, Cloud Dienste oder das Internet der Dinge werden in den nächsten Jahren das Leben und damit einhergehende Sicherheitsfragen maßgeblich prägen. Egal ob in der Arbeitswelt, in der Art und Weise wie wir wohnen und leben oder beim täglichen Umgang mit Devices – jeder dieser Megatrends eröffnet Möglichkeiten in Richtung einer höheren Flexibilität und erleichtert damit unser tägliches Handeln.

Neue und innovative Technologien bergen aber auch Gefahrenpotenziale und steigern die Notwendigkeit von Investitionen in IT-Sicherheit. 2015 wurde der Wert des Cyber Sicherheits Marktes auf über 10 Milliarden US-Dollar geschätzt – Tendenz steigend (Quelle: Strategic Defence Intelligence[1]). Der Internet-Sicherheitsbericht 2015 von CERT.at und GovCERT Austria zeigt daher bekannte Gefahrenfelder auf und gibt einen Rückblick auf die relevantesten, weltweiten IT-Sicherheitsvorfälle im Allgemeinen und auf das österreichische Internetjahr 2015 im Besonderen.

Megatrends bestimmen die Entwicklung des Internets

Das „Mehr" an Komplexität im Umgang mit Daten erreicht vor dem Hintergrund der großen Trends nicht nur große Konzerne sondern mittlerweile auch kleine und mittlere Unternehmen sowie PrivatanwenderInnen. Auch deren Daten werden durch die Vernetzung automatisch sensibler und müssen besser geschützt werden.

Industrie 4.0

Die Deutsche Telekom sieht die Sicherheit als eines der größten Fragezeichen für die Industrie 4.0 in ihrem Cyber Security Report 2015[2]. In dem Bericht führt die Deutsche Telekom beispielhaft an, dass sich bereits mehr als die Hälfte der Industrieunternehmen Deutschlands mit IT-Sicherheitsfragen auseinandergesetzt haben. Dies ist inzwischen ein „Muss" für Unternehmen, denn alleine in Deutschland gaben 36% der Unternehmen an, mehrmals pro Woche Opfer von IT-Angriffen zu werden. Eine hohe Dunkelziffer wird angenommen. Für die Industrie besteht somit laufend die Gefahr einer möglichen Cyber Attacke. Durch die Verschmelzung der IT mit Fertigungstechnik werden Industrieanlagen attraktiver für organisierte Cyber Attacken. Im Rahmen ihres Honeynet-Projektes[3] analysierte die deutsche TÜV SÜD acht Monate lang Spähangriffe auf ein kleines Wasserwerk. Dabei konnten Attacken aus über 150 Ländern registriert werden, was ein deutliches Warnsignal darstellt.

[1] Quelle: http://www.reportlinker.com/p03420462-summary/The-Global-Cyber-Security-Market.html
[2] Quelle: https://www.telekom.com/medien/konzern/293674
[3] Quelle: http://www.tuev-sued.de/tuev-sued-konzern/presse/pressearchiv/potenzielle-angreifer-sind-ueberall

Immer mehr mit dem Internet verbundene Geräte und Gegenstände werden künftig miteinander Daten austauschen. Ganz gleich, ob der Kühlschrank in der Wohnung oder das vernetzte Auto – das Internet der Dinge ist eine Entwicklung, die sowohl von privaten AnwenderInnen als auch von Unternehmen stark begrüßt wird, allerdings noch nach einer Anpassung verlangt. Mit mehreren Geräten und Gegenständen vernetzt zu sein bedeutet nämlich auch eine Vervielfachung der Angriffsfläche. Der Fall eines Angriffs auf einen Jeep Cherokee[4] in den USA ist ein Beispiel für die große Sicherheitsfrage im Internet der Dinge. Angreifer verschafften sich dabei über das Entertainment System, durch einen ausgenutzten Zero-Day-Exploit, Zugang zum Auto. Bei einem Zero-Day-Exploit handelt es sich um das Ausnutzen einer Sicherheitslücke, für die es noch keinen Patch als Gegenmaßnahme gibt. Von einer solchen Sicherheitslücke geht demnach eine hohe Gefahr aus, da zumeist nach ihrer Entdeckung und Veröffentlichung sogleich von Kriminellen versucht wird, diese in Form eines Exploits auszunutzen, bevor der entsprechender Hersteller mit einem Patch darauf reagieren kann. Im Fall des Jeep Cherokee waren sogar die Fahrzeuglenkung und die Bremsen von der Sicherheitslücke betroffen. In Folge dieser Attacke wurden 1,4 Millionen Fahrzeuge vom Hersteller zurückgerufen. Was bleibt, sind viele offene Sicherheitsfragen in Bezug auf Authentifikation, Verschlüsselung von Daten und deren Speicherung, sowie natürlich auch wie man sich künftig gegen ähnliche Angriffe besser schützen kann.

Cloud Dienste

Auch die permanente Verfügbarkeit von Daten über Cloud Dienste erfreute sich 2015 wachsender Beliebtheit. Laut dem amerikanischen Cloud Anbieter Salesforce nutzen weltweit bereits ein Drittel der Privatpersonen und 60% der Unternehmen Cloud Dienste. Mit geschätzten Cloud-basierten Umsätzen bei Salesforce von 272 Milliarden US-Dollar bis 2018 sind Cloud Anwendungen mittlerweile auch ein bedeutender weltweiter Wirtschaftsfaktor. Gleichsam steigen auch die Anforderungen in puncto Sicherheit der gespeicherten Daten. Zu den größten Risiken in der Cloud[5] gehören unter anderem der Schutz auf der Infrastrukturebene, die Erfüllung von gesetzlichen Anforderungen in den verschiedenen Ländern oder die Gefahr von Datendiebstahl durch nicht autorisierte Zugriffe.

Ende des Safe-Harbor-Abkommens

Anfang Oktober 2015 erklärte der Europäische Gerichtshof (EuGH) das Safe-Harbor-Abkommen der EU-Kommission mit den Vereinigten Staaten aus dem Jahr 2000 für ungültig.[6] Das Abkommen erlaubte den Transfer von personenbezogenen Daten aus der EU in die USA, sofern dies mit der europäischen Datenschutzrichtlinie übereinstimmte. Mit dem EuGH-Urteil wurde jedoch die Übertragung persönlicher Daten in die USA auf Basis des Abkommens verboten, da die Datenspeicherung in den USA als nicht sicher eingestuft wurde. Der EU-Kommission und den USA wurde eine Übergangsfrist bis Ende Januar 2016 eingeräumt – ab diesem Zeitpunkt sollen die notwendigen Maßnahmen des Urteils

[4] Quelle: http://www.computerwoche.de/a/iot-die-sicherheit-der-dinge,3213672
[5] Quelle: http://www.computerwoche.de/a/ratgeber-it-sicherheit,2363872,2
[6] Quelle: http://futurezone.at/netzpolitik/safe-harbor-aus-schwere-folgen-fuer-usa/158.145.921

umgesetzt werden. Für internationale und in Europa tätige Unternehmen, die Daten beispielsweise in den USA gespeichert haben, ist dieses Urteil mit Folgen verbunden. Sie müssen ihre Daten künftig in der EU speichern oder die explizite Zustimmung ihrer Nutzer einholen.

Mobile Internetnutzung steigt

Die mobile Internetnutzung nimmt ebenfalls stetig zu. Zu Beginn des Jahres 2015 wurden 31% aller weltweiten Internetaufrufe durch mobile Endgeräte getätigt (Quelle: Statcounter).[7] Zum Vergleich: Im Jahr 2014 waren dies noch 22%. Mobile Devices werden vorwiegend für Online Einkäufe und soziale Netzwerke genutzt. Der hohe Anteil an persönlichen Daten in den Geräten steigert gleichzeitig deren Attraktivität für Cyber Attacken. So wurde laut dem Analyseunternehmen Forensiq zufolge 2015 durch sogenannten In-App-Betrug mit Werbung eine Schadenshöhe von über einer Milliarde US-Dollar verursacht.[8] Dabei wurde bei manipulierten Apps die NutzerInnenaktivität simuliert und damit eine Vielzahl an Aufrufen erzeugt. Sowohl Betriebssysteme, als auch Apps und die Hardware selbst müssen daher Teil des Sicherheits- und Datenschutzes für Mobile Devices sein.

Der Mensch ist und bleibt die kritischste Schwachstelle

Durch zunehmende technische Sicherheitsmaßnahmen wie Firewalls, Virenschutz oder Verschlüsselung rückt eine bestimmte Schwachstelle beim Thema Internetsicherheit immer mehr in den Mittelpunkt – der Mensch. Immer wieder wird beispielsweise versucht, durch Beeinflussung von Personen an sensible Daten oder Passwörter zu gelangen. Sobald sie die Daten bekommen haben versuchen Angreifer diese auch schadhaft und zu ihrem eigenen Vorteil zu nutzen. Der Angriff kann über soziale Netzwerke, über Phishing-E-Mails, bis hin zu einfachen Telefonanrufen erfolgen – der Kreativität der Angreifer sind hier wenige Grenzen gesetzt. Denn gegenüber vielerorts gut ausgebauten, technischen Schutzsystemen scheint der Mensch oftmals leichter zu „hacken" zu sein. Allein bei drei durch Social Engineering erfolgten Angriffen Anfang des Jahrs 2015 in der Schweiz entstand ein Schaden von rund 313.000 Schweizer Franken (rd. 287.000 Euro) bei Unternehmen und Privatpersonen[9], um nur ein internationales Beispiel von vielen wiederzugeben.

Mehr User und mehr Devices führen zu mehr Datendiebstahl

Mit der Zahl der Internet User steigen auch die Datenmengen, die Netzwerkgrößen und auch die Vielfalt an verwendeten Geräten. Im Jahr 2010 ging McAfee davon aus, dass bis 2020 rund 31 Milliarden Geräte mit dem Internet verbunden sein werden. Bereits heute scheint diese Schätzung deutlich zu gering zu sein. Mussten ursprünglich eher Behörden und Finanzinstitute Cyber Bedrohungen erwarten, sind heute auch Unternehmen und

[7] Quelle: http://www.haufe.de/marketing-vertrieb/online-marketing/mobile-internetnutzung-steigt-weltweit-weiter-an_132_291656.html
[8] Quelle: http://winfuture.de/news,88168.html
[9] Quelle: http://www.polizeiticker.ch/news/artikel/kanton-bern-vorsicht-vor-social-engineering-betrug-51395/?cHash=b3a839b16a39e6bf26bbfe76691c2e06

PrivatanwenderInnen bei Angriffen längst nicht mehr nur ein sekundäres Ziel, sondern stehen im Fokus der Angreifer.

Zu einem ähnlichen Schluss kommt auch Microsoft im Rahmen seines 19. Security Intelligence Reports.[10] Die wirtschaftliche Verwertung von gestohlenen Daten zur Profitgenerierung steht heute im Vordergrund vieler Angreifer. Die häufigsten Methoden sind dabei Social Engineering, das Hacken schwacher Passwörter oder schlecht konfigurierter Systeme und Schwachstellen aufgrund von nicht durchgeführten Updates der darauf betriebenen Software.

Cyber Bedrohung beschränkt sich aber nicht mehr auf einfache kriminelle Motive. Heute reichen die Absichten der Angreifer von Aktivismus im Internet (sog. „Hacktivismus") über organisierte Verbrechen mit dem Ziel eines finanziellen Profits bis hin zu staatlichen Spionage-Aktionen.

Ökosystem des Bösen: Cyber Angriffe als florierender „Wirtschaftszweig"

Diese Vielfalt an Angriffsmotiven führte zu einem regelrechten Untergrundmarkt, auf dem millionenfach Daten zum Verkauf angeboten werden. Dies zeigt der aktuelle McAfee Bericht „Das heimliche Geschäft mit Daten" auf.[11] Von Anmeldedaten über Finanzdaten, Zugriffsdaten für abonnierte Online Dienste oder ganze Datensammlungen und somit gesamte Online Identitäten von Opfern – der Bericht legt die schockierenden Möglichkeiten der Cyber Bedrohungen offen und zeigt: Cyber Angriffe sind ein finanziell höchst erträgliches Geschäft und haben sich längst zu einem weltweit stark wachsenden „Wirtschaftszweig" entwickelt. Wie genau Angreifer dabei vorgehen, was hinter diesem „Ökosystem des Bösen" steckt und wie weltweite Angriffe ablaufen können, beschreibt unter anderem ein Paper[12] von renommierten IT-Sicherheitsexperten des International Computer Science Institutes sowie führender US-amerikanischer Universitäten.

Prominente Opfer im Internetjahr 2015

Obwohl die Investitionen in Cyber Sicherheit kontinuierlich stiegen, finden Hacker immer wieder Möglichkeiten sich unerlaubten Zugriff auf Netzwerke zu verschaffen. So geschehen auch im Cyber Jahr 2015: Bei Anthem Inc., einer der größten Krankenversicherungen in den USA, stahlen Hacker im Februar 2015 Daten von rund 80 Millionen Kunden.[13] Dazu gehörten auch äußerst sensible Daten, wie Gehaltsinformationen. Als äußerst brisant erwies sich die Tatsache, dass die Daten unverschlüsselt abgespeichert waren, was ein Auslesen dieser Daten

[10] Quelle: http://download.microsoft.com/download/4/4/C/44CDEF0E-7924-4787-A56A-16261691ACE3/Microsoft_Security_Intelligence_Report_Volume_19_English.pdf
[11] Quelle: http://www.mcafee.com/de/resources/reports/rp-hidden-data-economy.pdf
[12] Quelle: http://research.google.com/pubs/pub43798.html
[13] Quelle: http://www.zdnet.de/88220154/nicht-nur-kunden-von-datendiebstahl-bei-anthem-betroffen/

durch die Angreifer leicht ermöglichte. Eine Schadenssumme ist schwer zu beziffern, sie dürfte jedoch über 100 Millionen US-Dollar liegen.
Die polnische Fluglinie LOT musste aufgrund eines Hackangriffs ihren Flugbetrieb im Juni 2015 für rund fünf Stunden einstellen.[14] Dies bedeutete Verspätungen für 1.400 Passagiere der Fluglinie. Beim Partnerunternehmen der Deutschen Lufthansa wurde gezielt das System der Flugplanung angegriffen und lahmgelegt. In Folge mussten insgesamt zehn Flugverbindungen gestrichen werden.

Im Frühjahr 2015 wurde auch der Deutsche Bundestag Opfer eines Hackangriffs.[15] Dabei wurden E-Mails, getarnt als Nachrichten von der UNO, gezielt an mehrere Abgeordnete versendet. Durch die sich im Anhang dieser E-Mails befundenen Schadsoftware erhielten die Angreifer Zugang auf das interne Netz des Bundestags. Bis zum heutigen Tag ist der Fall nicht komplett aufgeklärt, sodass der Datenverkehr des Bundestags seitdem über das sichere Netz der Deutschen Regierung erfolgt.

Android Smartphones als bevorzugte Angriffsziele – aber kein mobiles System ist sicher
Einer der größten globalen Begriffe des Cyber Sicherheit Jahres stellt „Stagefright" dar. Stagefright ist eine Sicherheitslücke im Android-Betriebssystem[16] und betraf zwischenzeitlich fast 95% aller Android-NutzerInnen. Angreifer konnten darin eine „Buffer-Overflow-Schwachstelle" ausnutzen, bei der sie Speicherbereiche mit neuen Code-Anweisungen überschreiben konnten. Werden Multimediadaten, beispielsweise via MMS, an die EmpfängerIn gesendet, führt das Smartphone dann einen manipulierten Programmcode aus. Vor allem in der Android-Welt, die durch unterschiedliche Versionen auf Geräten unterschiedlicher Hersteller gekennzeichnet ist, gestaltet sich die Bereitstellung von Updates, welche diese Sicherheitslücke beheben, schwierig. Einige Versionen sind daher noch bis heute betroffen.

Neben Android war 2015 auch Apple betroffen. Durch die Software XcodeGhost haben Hacker im September 2015 Apps im Apple Store infiziert und versucht, dadurch an iCloud-Passwörter von Usern zu gelangen.[17] Die Malware diente zu gezielten Phishing Angriffen. Dies wurde den Angreifern erst dadurch ermöglicht, da App EntwicklerInnen nicht das von Apple bereitgestellte Entwickler-Tool Xcode verwendeten, sondern auf private Installationsdateien zurückgriffen. Über 300 Apps mussten in der Folge aus dem App Store gelöscht werden.

[14] Quelle: http://www.heise.de/security/meldung/LOT-Polish-Airlines-Flugverkehr-nach-Hackerangriff-wieder-normal-2718810.html
[15] Quelle: http://www.spiegel.de/netzwelt/web/die-hacks-des-jahres-von-ashley-madison-bis-zum-bundestag-a-1069558.html
[16] Quelle: http://diepresse.com/home/techscience/mobil/4794130/Stagefright-Die-Mutter-aller-AndroidLucken
[17] Quelle: http://futurezone.at/digital-life/app-store-malware-in-populaere-ios-apps-eingeschleust/153.665.498

Daten als leichte Beute

Die Ausnutzung einer Sicherheitslücke in der Datenbank mittels SQL-Injection in Kombination mit einer Denial-of-Service-Attacke (DoS) erfolgte im Herbst beim britischen Telekomkonzern TalkTalk.[18] Ein DoS Angriff verfolgt das Ziel der Überlastung eines Systems. Während das Sicherheitsteam von TalkTalk mit der verursachten Überlastung beschäftigt war, konnten die Angreifer unbemerkt das System von TalkTalk durchsuchen. Vom Datenklau waren 400.000 Datensätze der rund vier Millionen KundInnen betroffen. Gerade dieses Beispiel zeigt, wie wichtig eine grundlegende Basis Sicherheitsinfrastruktur sein kann, welche die in diesem Fall durch die Angreifer ausgenutzte Sicherheitslücke schnell beseitigen hätte können.

Unternehmen werden verstärkt zur Zielscheibe

Angreifer sind sich in der Regel bewusst, dass gestohlene Daten von Unternehmen zu größerem finanziellen Profit führen können, als gestohlene Daten von PrivatanwenderInnen. Demnach waren 2015 die gegen Unternehmen gerichteten Angriffe deutlich anders ausgeprägt als jene gegen PrivatanwenderInnen. Kaspersky analysierte im Rahmen des Security Bulletin 2015/2016[19] die verwendeten Angriffsarten und kam zu dem Ergebnis, dass Software-Schwachstellen, mit gültigen Zertifikaten signierte Schädlinge sowie Verschlüsselungstrojaner (Ransomware) am häufigsten ausgenutzt bzw. verwendet wurden. Laut Kaspersky hatte über die Hälfte der weltweiten Rechner in Unternehmensnetzwerken (58%) mindestens eine Malware Attacke im Jahr 2015 zu überstehen gehabt. An Rechnern in Unternehmen werden auch drei Mal häufiger Exploits (Schadprogramme, die Sicherheitslücken ausnutzen) zu Office Anwendungen eingesetzt als bei Angriffen auf private Computer. Dabei ist die Verteilung weltweit unterschiedlich, wie die Geografie der Angriffe über Web-Ressourcen im Jahr 2015 (Abbildung 1) zeigt.

[18] Quelle: http://derstandard.at/2000024455697/Hacker-stehlen-Daten-von-vier-Millionen-Briten-fordern-Loesegeld

[19] Quelle: https://de.securelist.com/analysis/kaspersky-security-bulletin/70692/kaspersky-security-bulletin-20152016-entwicklung-der-it-bedrohungen-im-unternehmensbereich/

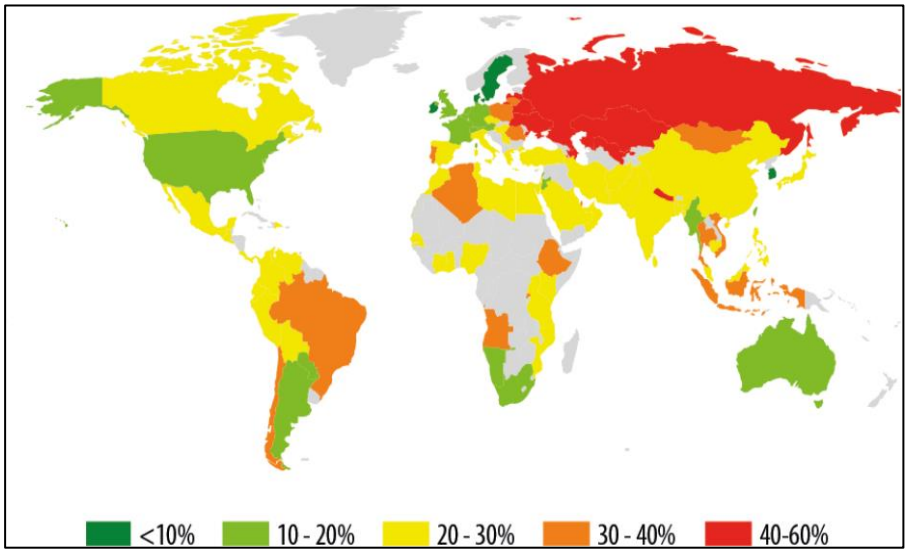


Abbildung 1: Geografie der Attacken über Web-Ressourcen im Jahr 2015 (prozentualer Anteil der angegriffenen UnternehmensanwenderInnen im Land), Quelle: Kaspersky Lab[20]

Der 2015 Internet Security Threat Report von Symantec[21] greift auf Daten aus über 157 Ländern zurück. Laut dem Report konnten weltweit im Jahr 2014 um 23% mehr Sicherheitslücken identifiziert werden als im Vorjahr. Das Bild zeigt deutlich, dass sich Angreifer Sicherheitslücken schneller zunutze machen, als Unternehmen entsprechende Patches bereitstellen können. Während Angriffe immer gezielter werden, verabsäumen es Unternehmen nach wie vor den Basisschutz, beispielsweise für unbekannte und verdächte E-Mail-Anhänge, zu aktualisieren.

Angriffe besonders gerne auch über Social Media

Der Betrug via Social Media steigt auch rasant an und wird in den nächsten Jahren weiter zunehmen. Hier schienen NutzerInnen besonders leichtsinnig zu agieren, da ein geteilter Link von einem/r Bekannten eher angeklickt wird, als ein unbekannter E-Mail-Anhang. Diese Sorglosigkeit drückt sich auch im Umgang mit Datenschutzrichtlinien aus, denen NutzerInnen für das Verwenden von Apps zustimmen müssen. Ein Beispiel: Bei 20% aller gesundheitsbezogenen Apps werden persönliche Informationen wie Passwörter als Klartext gespeichert, was den Usern in dieser Form oftmals nicht bewusst sein dürfte.

Sicherheitsbewusstsein in Europa muss geschärft werden

Mit der im Februar 2015 veröffentlichten Eurobarometer-Umfrage zum Thema Cyber Sicherheit[22] fing die EU-Kommission das Thema „Sicherheit im Internet" aus der Perspektive der Bevölkerung ein. Mit über 150.000 Viren und über einer Million Opfern von Cyber Attacken pro Tag spielen Cyber Bedrohungen in der EU eine wesentliche Rolle. Die häufigsten

[20] Quelle: https://de.securelist.com/analysis/kaspersky-security-bulletin/70692/kaspersky-security-bulletin-20152016-entwicklung-der-it-bedrohungen-im-unternehmensbereich/
[21] Quelle: https://know.elq.symantec.com/LP=1542
[22] Quelle: http://ec.europa.eu/COMMFrontOffice/PublicOpinion/index.cfm/Survey/getSurveyDetail/search/cyber%20security/surveyKy/2019

Aktivitäten der NutzerInnen im Netz sind das Abrufen von E-Mails (86%), das Lesen von Online Zeitungen (63%), soziale Netzwerke (60%) und Online Einkäufe (57%). Es ist alarmierend, dass nur 61% aller InternetnutzerInnen in Europa eine Anti-Virus Software installiert haben. In Österreich gaben 73% der BenutzerInnen an, eine Anti-Virus Software installiert zu haben. Beachtlich ist, dass heute bereits 61% der User in Europa mit dem Smartphone ins Internet einsteigen. Zum Vergleich: 2013 waren dies noch 35% der Befragten. Die Verhaltensweisen der User bei der Internetnutzung zeigt die Eurobarometerumfrage wie folgt:

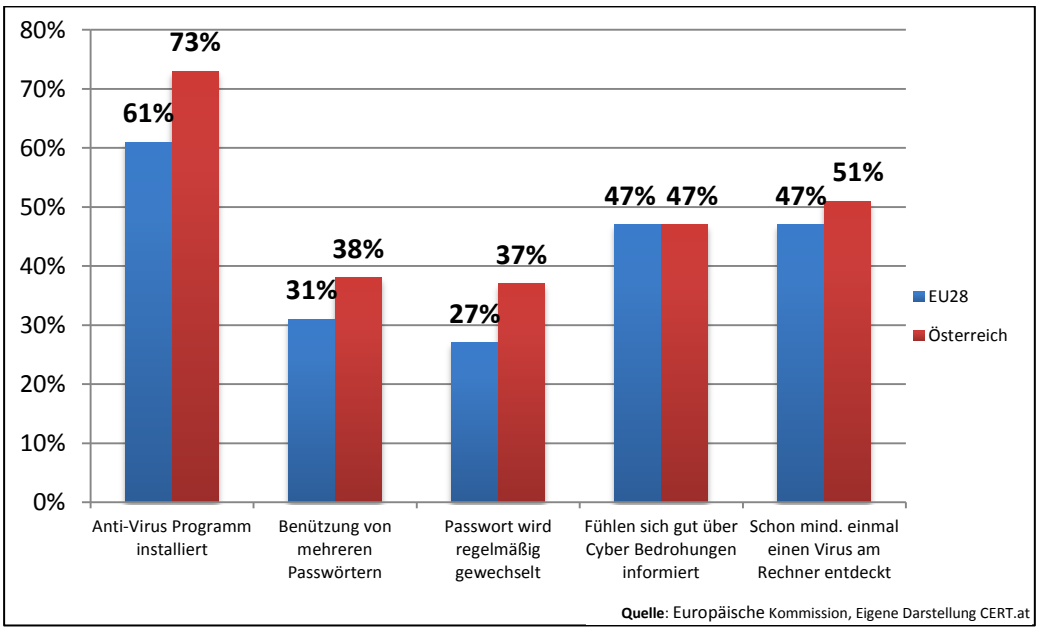


Abbildung 2: Ausgewählte Cyber Sicherheit Eurobarometer Umfrageergebnisse (EU28 & Österreich)

85% der EuropäerInnen glauben, dass gegenwärtig das Risiko steigt, ein Opfer von Cyber Angriffen werden zu können. Umso wichtiger wird es sein, das Bewusstsein gegenüber Sicherheitsmaßnahmen im Internet zu stärken. Anti-Virus Software, der sichere Umgang mit persönlichen Daten und Passwörtern bilden die Basis für die sichere Fahrt über die Datenautobahn. Sicherheitsbewusstsein und der verantwortungsvolle Umgang mit Daten ist gerade im grenzenlosen Raum des Internets sehr wichtig für höchstmögliche Sicherheit und die beste Vorsorge gegen Cyber Bedrohungen.

4. CYBER SICHERHEIT NATIONAL: DAS IT-SICHERHEITSJAHR 2015 AUS ÖSTERREICHISCHER SICHT

Angriffe und Bedrohungen aus dem Netz sind auch in Österreich ein akutes Thema. Der Cyber Raum wurde 2015 auch hierzulande zum Schauplatz zahlreicher Diebstähle, Missbräuche und Angriffe. Der CERT-Jahresbericht 2015 legt den Fokus auf ausgewählte Sicherheitsvorfälle, die speziell für Österreich relevant waren. Dies soll neben der Information auch die Aktualität der täglichen Gefahren im „www" unterstreichen. Die Bandbreite ist dabei enorm, denn von einfachen „just-for-fun"-Hackern, über Wirtschaftsspionage bis hin zu staatlicher Überwachung, sind die Akteure und ihre Ziele mittlerweile nur noch schwer überschaubar.

Die Internet-Sicherheitslage Österreichs 2015

CERT.at und GovCERT Austria führen umfangreiche Statistiken[23], mit denen sich ein Bild über die aktuelle Internet-Sicherheitslage Österreichs machen lässt. Ein Blickwinkel auf diese Lage ist die Zahl der vom CERT behandelten Vorfälle. Wichtige Kennzahlen dafür sind Reports, Incidents und Investigations.

„Reports" bezeichnen eingehende Meldungen an CERT.at. Nicht alle davon beschreiben einen Sachverhalt, der von CERT.at als relevanter Vorfall (Incident) eingestuft wird und eine aktive Behandlung erfordert. Typische Gründe für eine Beurteilung als irrelevanter Vorfall sind etwa:

- Meldungen zu Problemen, die bereits bereinigt wurden
- Falschmeldungen von einfachen Suchalgorithmen
- mangelnde Zuständigkeit von CERT.at
- generische Anfragen
- andere E-Mail-Irrläufer/Spam

Als „Incidents" werden jene Fälle eingestuft, die tatsächlich ein Sicherheitsrisiko darstellen. Bei diesen schreitet CERT.at ein und informiert beispielsweise betroffene Unternehmen, Organisationen oder PrivatanwenderInnen über IT-Sicherheitsbedrohungen und unterstützt bei Bedarf bei der Problemlösung. Diese Kontaktaufnahme wird im CERT.at Ticketsystem als „Investigation" bezeichnet.

Wichtig: Bei der Interpretation der Grafiken und Statistiken ist zu beachten:

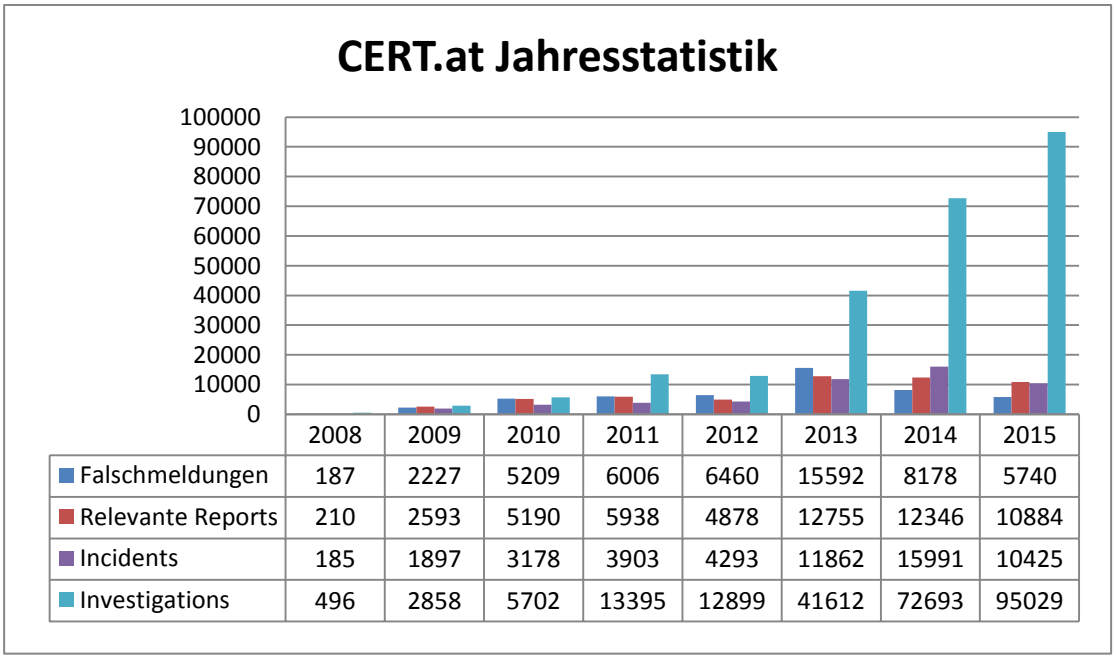
1. Eine Verbesserung in der Sensorik besitzt oft viel mehr Einfluss auf die Kurve, als eine Veränderung der dahinterliegenden Vorfälle. Wenn etwa durch eine Polizeiaktion in den USA plötzlich Daten zu einem Botnetz verfügbar werden, dann bedeutet dies einen plötzlichen und großen Sprung in den CERT.at Statistiken. In Wirklichkeit wurde das Botnetz aber über einen längeren Zeitraum hinweg aufgebaut.

[23] Quelle: http://cert.at/services/statistics/statistics.html

2. Nicht alle Vorfälle sind gleichwertig relevant. So kann ein Incident sowohl ein fehlkonfigurierter Surf-PC in einer Jugendherberge sein, als auch ein Einbruch in einen Webshop mit dem Verlust tausender KundInnendaten.

3. Viele der Incidents behandeln bereits aggregierte Informationen. So etwa generiert die Sensorik zu falsch konfigurierten Nameservern einen Report pro Tag, unabhängig wie viele einzelne IP-Adressen enthalten sind. Die ausgehenden Mails an die Netzbetreiber können ebenfalls von einem einzelnen Vorfall bis hin zu einer langen Liste an betroffenen KundInnen reichen.

Abbildung 3 gibt einen Überblick über CERT.at Jahresstatistiken seit 2008. Sie beinhaltet die Zahl der Falschmeldungen, relevanten Reports, Incidents und Investigations. Die Grafik zeigt damit die steigende Bedeutung von Cyber Sicherheit und den notwendigen Maßnahmen auf. Seit dem Jahr 2008 nahm die Zahl der relevanten Reports, Incidents und Investigations kontinuierlich zu, wobei die Incidents und Reports 2015 im Vergleich zu 2014 leicht zurückgingen. Hervorstechend ist vor allem die Zunahme der Investigations seit 2012.



	2008	2009	2010	2011	2012	2013	2014	2015
Falschmeldungen	187	2227	5209	6006	6460	15592	8178	5740
Relevante Reports	210	2593	5190	5938	4878	12755	12346	10884
Incidents	185	1897	3178	3903	4293	11862	15991	10425
Investigations	496	2858	5702	13395	12899	41612	72693	95029

Abbildung 3: CERT.at Jahresstatistik mit Übersicht über Reports, Incidents und Investigations im Zeitverlauf, Quelle: CERT.at

In Abbildung 4 werden die relevanten Reports an CERT.at im Zeitverlauf des letzten Jahres dargestellt. Dabei wird die Anzahl der relevanten Meldungen pro Monat in den Top 15 Kategorien wiedergegeben. Mit 1.205 relevanten Meldungen gingen im April 2015 die meisten Reports ein, gefolgt von den Monaten Dezember (1.074 Meldungen) und Mai (1.066 Meldungen).

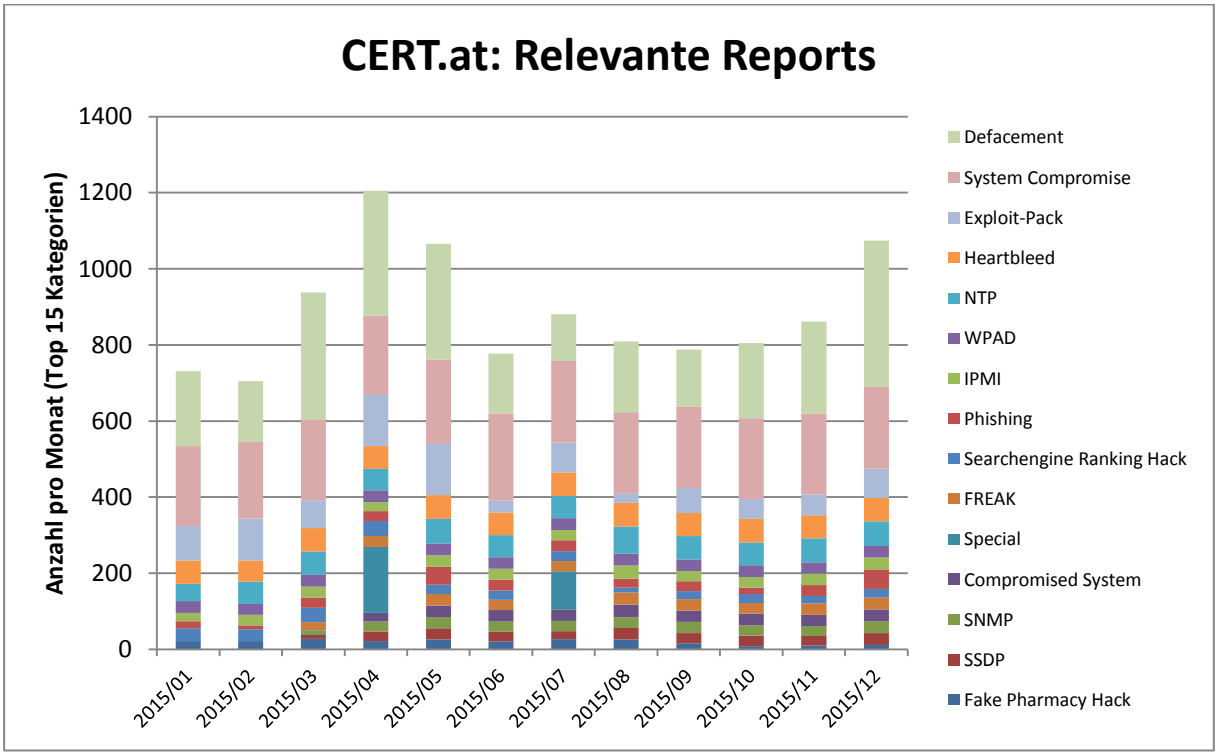


Abbildung 4: Klassifizierung der relevanten Reports nach Bedrohungsformen im Zeitverlauf, Quelle: CERT.at

Die Zahl der Fälle, die tatsächlich ein Sicherheitsrisiko darstellten, werden in Abbildung 5 abgebildet. Die meisten Incidents gab es im April 2015 mit 1.143. Viele Incidents gab es darüber hinaus in den Monaten Dezember (994), Mai (954) sowie März (908). Die geringste Zahl an Incidents wurden zu Beginn des Jahres in den Monaten Januar und Februar registriert.

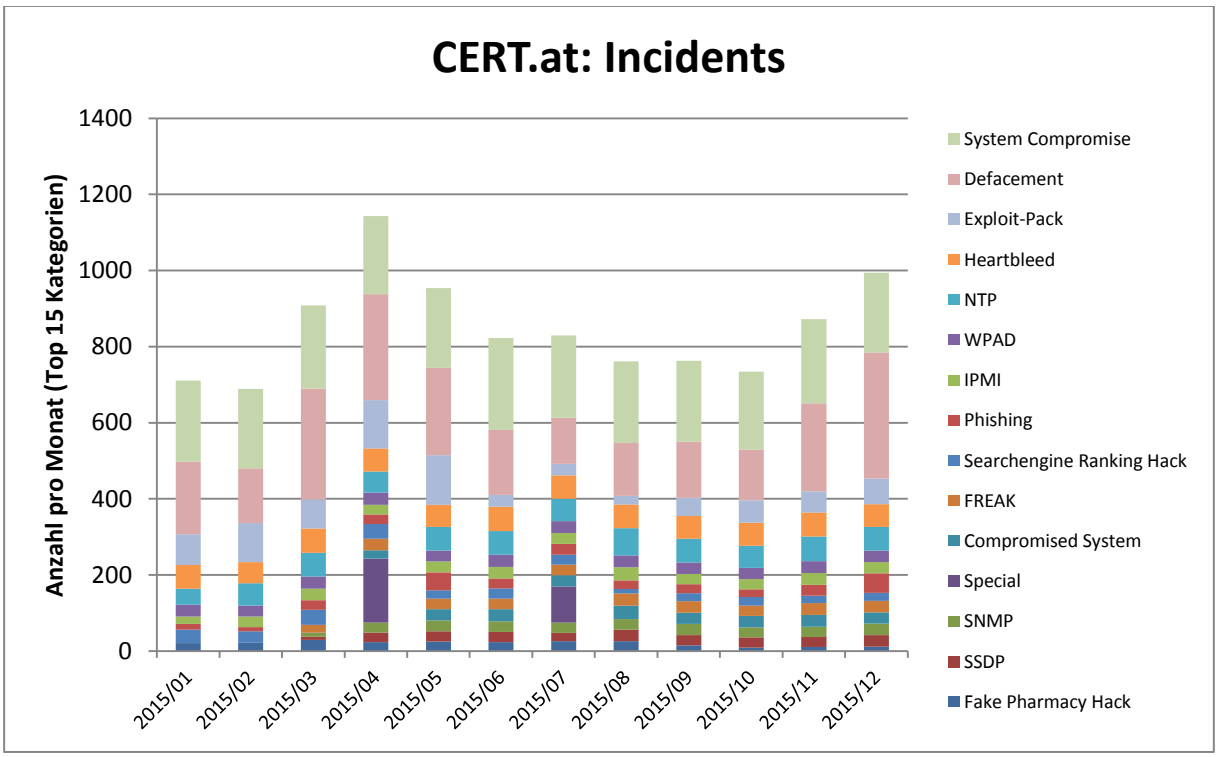


Abbildung 5: Klassifizierung von Incidents nach Bedrohungsformen im Zeitverlauf, Quelle: CERT.at

Die Zahl der Investigations, also die Kontaktaufnahmen mit betroffenen Unternehmen, Organisationen oder PrivatanwenderInnen, war wie in den vorherigen zwei Grafiken im April 2015 (1.143) am höchsten. Darauf folgten die Monate Dezember und Mai mit 994 bzw. 954 Investigations, wie Abbildung 6 zeigt.

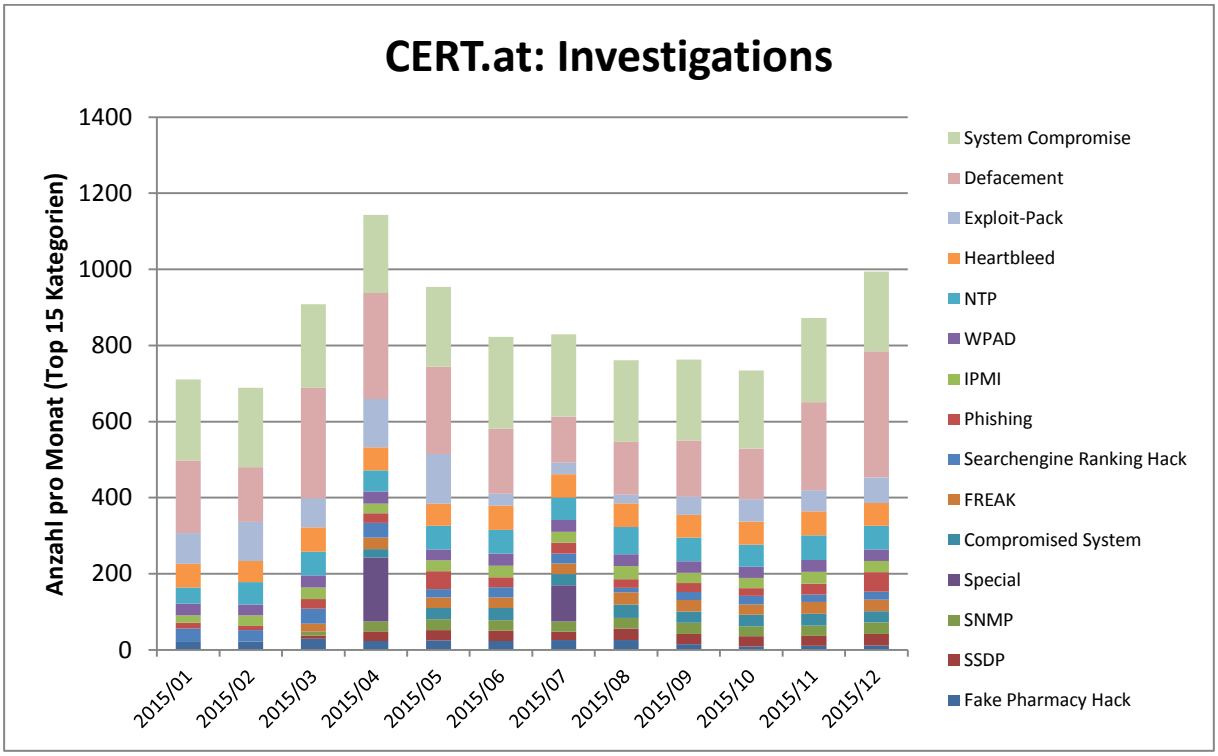


Abbildung 6: Klassifizierung der von CERT.at durchgeführten Investigations nach Bedrohungsformen im Zeitverlauf, Quelle: CERT.at

Sicherheitsprobleme im österreichischen Internet

Ein anderer Blickwinkel auf die IT Sicherheitslage in Österreich ist die Telemetrie, auf der ein Großteil der von CERT.at behandelten Fälle basiert. Diese Daten stammen aus diversen Quellen, etwa:

- Aktionen von Strafverfolgungsbehörden: Domains oder Server von Botnetzen werden beschlagnahmt. Dann werden die Steuerserver der Botnetze („Command and Control Server") durch Sensoren ersetzt, die mitprotokollieren, von wo aus infizierte PCs neue Befehle abholen wollen.
- Analyse der Malware und Registrierung der verwendeten Domains: In vielen Fällen wird für die Kommunikation zwischen infiziertem PC und dem Command and Control Server keine feste Domain benutzt, sondern diese wird aus dem aktuellen Datum abgeleitet. Analysiert man den verwendeten Algorithmus, so kann man diese Domains im Voraus – so diese noch verfügbar sind – registrieren und auch dort einen Sensor betreiben.
- Verwendet die Malware einen Peer-to-Peer Mechanismus für die Kommunikation, so lassen sich die Mitglieder des P2P-Netzes enumerieren.
- In manchen Fällen gelingt es der Polizei, Sicherheitsforschern oder CERTs Zugang zu Servern der Kriminellen zu erlangen. Die dort gefundenen Daten können sehr aufschlussreich sein.

- Aktive Suche nach Sicherheitsproblemen: Manche Themen kann man leicht von außen testen. So etwa ob ein Webserver noch für den Heartbleed-Bug anfällig ist, oder ob eine IP-Adresse auf Protokoll-Anfragen antwortet, die im offenen Internet nicht vorkommen sollten.
- Suche mittels Suchmaschinen: Will man Probleme von Webseiten suchen, so kann man Google, Bing & Co benutzen.
- Blacklisten: Es werden von mehreren Betreibern „schwarze Listen" von IP-Adressen, Domains und URLs geführt, die als bösartig oder gefährlich eingestuft werden. Der/Die einfache Internet-NutzerIn sieht den Effekt dieser Blacklists vor allem dann, wenn ihn/sie der Browser vor einer Phishingseite warnt.
- Die Täter selber: So melden etwa einige der Einbrecher in Webseiten ihre „Defacements" bei zone-h.org[24], die gestohlenen Daten aus Datenbankeinbrüchen landen oft auch auf pastebin.

Grob gesprochen fallen Meldungen zu IP-Adressen in drei Kategorien: Hinter einer solchen IP-Adresse steht ein infizierter Computer (Mitglied eines Botnetzes), ein Server der sich für Denial-of-Service Angriffe missbrauchen lässt, oder aber ein Server der Probleme (Bugs oder Fehlkonfiguration) mit verschlüsselter Kommunikation aufweist.

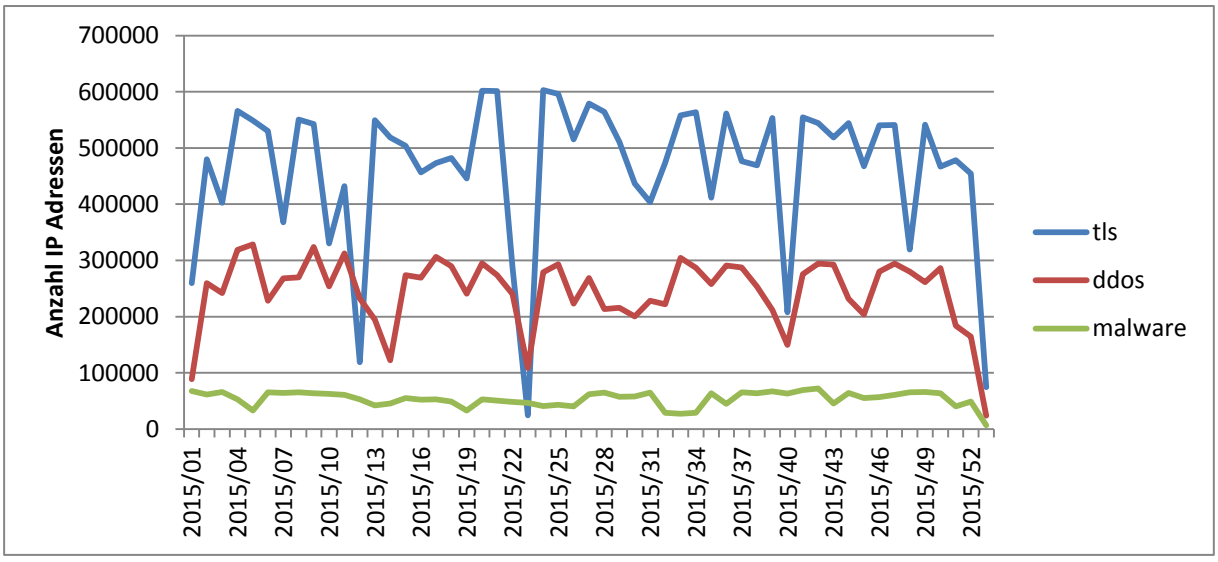


Abbildung 7: Klassifizierung der Meldungen zu IP-Adressen nach den Kategorien TLS, DDoS und Malware im Zeitverlauf, Quelle: CERT.at

Infizierte PCs

Die Datenbasis bezüglich der in Österreich verbreiteten Botnetze hängt sehr stark davon ab, zu welchen aktuell eine gute Telemetrie existiert. Die folgende Grafik zeigt, wie sehr die Zahl der gemeldeten IP-Adressen (pro Tag) für jede der Datenquellen im Jahr 2015 variiert:

[24] Quelle: https://zone-h.org/archive/special=1

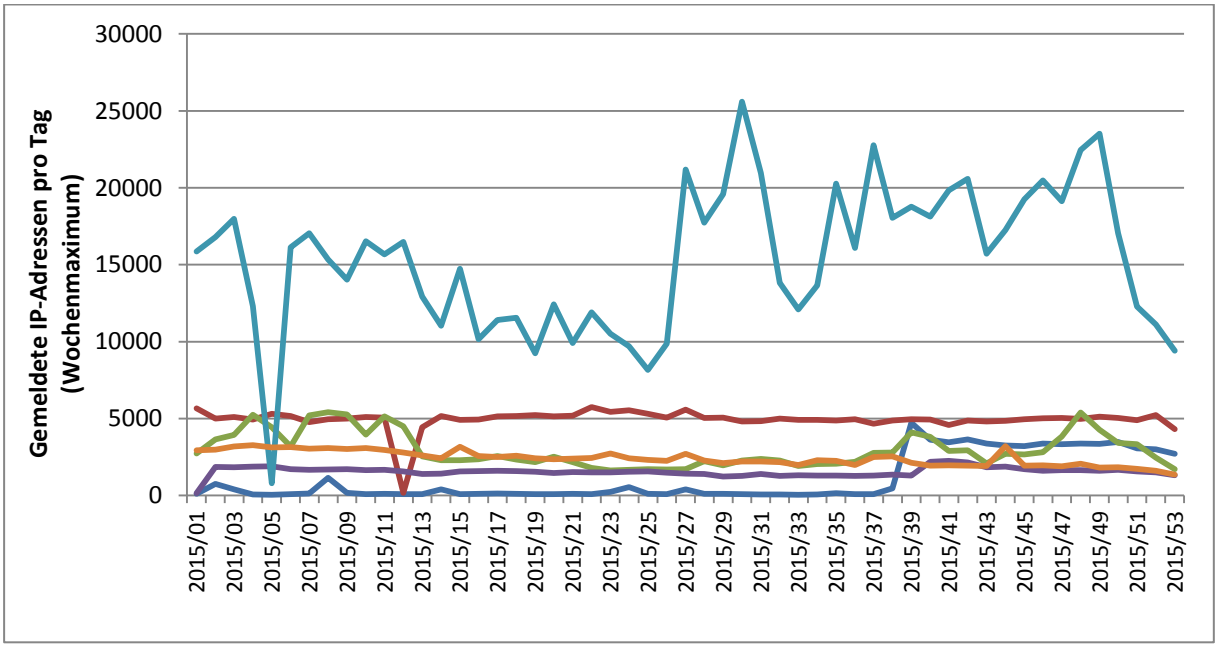


Abbildung 8: Anzahl der gemeldeten IP-Adressen (pro Tag, pro Datenquelle) in Österreich im Zeitverlauf, Quelle: CERT.at

Gute Daten existieren primär für die älteren Botnetze: Diese sind bereits gut analysiert und entsprechende Sensoren („Sinkholes") werden betrieben. Im Falle von Conficker ist beispielsweise die Malware seit Jahren konstant, was diese Messungen weiter vereinfacht. Da verschiedene Quellen auch verschiedene Namen für die gleiche Malware verwenden (so etwa wird Conficker manchmal mit Version (A, B oder C) geschrieben oder „downadup" genannt), ist die Aggregation aller Quellen in ein konsistentes Bild nicht möglich. In der folgenden Grafik sind daher Infektionen, die von mehreren Quellen gemeldet wurden, mehrfach gezählt.

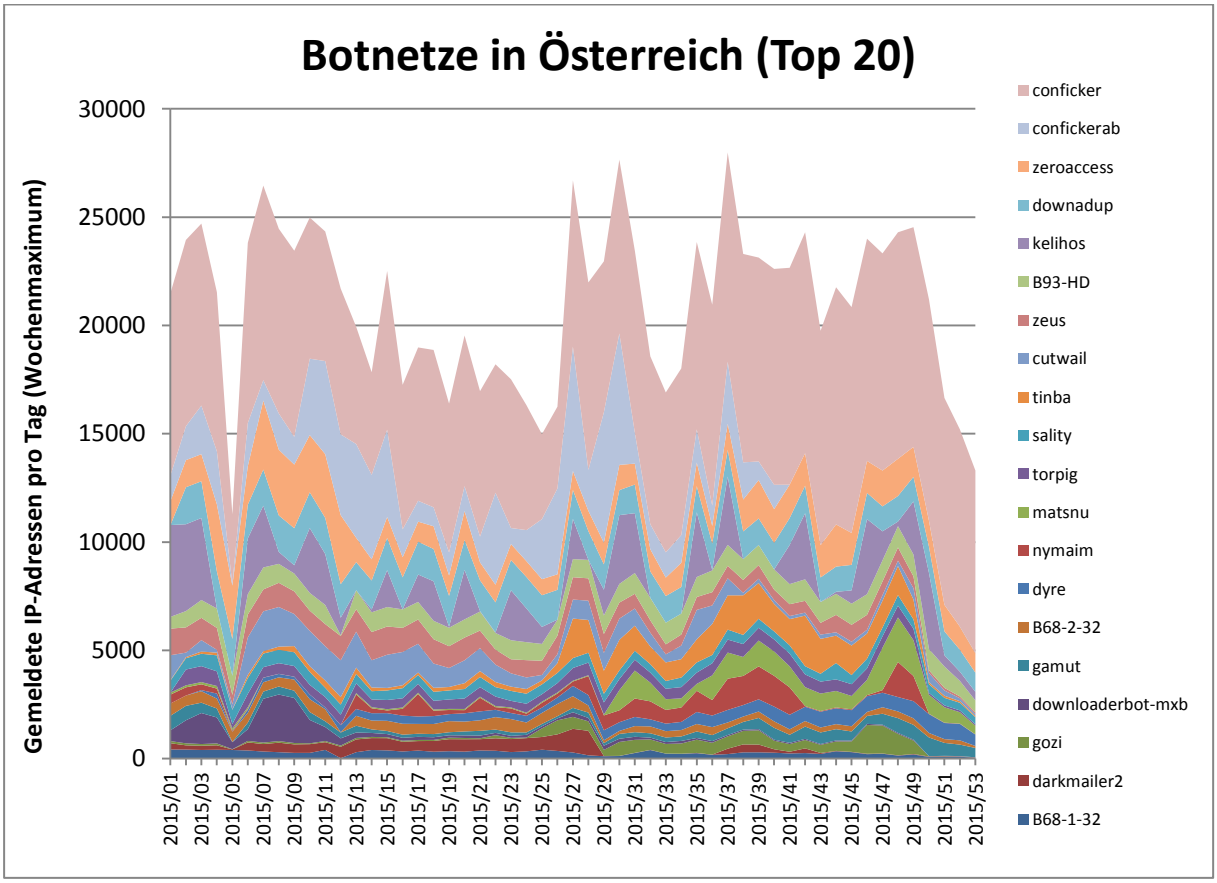


Abbildung 9: Klassifizierung der Meldungen nach Botnetzen im Zeitverlauf, Quelle: CERT.at

Mitwirkung bei Denial of Service

Denial of Service Angriffe verwendeten auch 2015 oft den Trick, Pakete von schlecht konfigurierten Servern reflektieren und verstärken zu lassen.

Dabei schickt der Angreifer eine – an sich legitime – Anfrage an ein UDP (User Datagram Protocol)-basiertes Service (etwa DNS: Domain Name Service, NTP: Network Time Protocol, SNMP: Simple Network Management Protocol, SSDP: Simple Service Discovery Protocol, …), setzt dabei aber die Absender-IP-Adresse im Datenpaket auf die des Opfers. In Folge schickt der angesprochene Server die Antwort an das Opfer, in der Annahme, dass von dort die Anfrage ausging. Die Anfragen werden so gewählt, dass sie möglichst große Antworten (hinsichtlich der übermittelten Datenmenge) zur Folge haben. Mit diesem Trick kann aus einem Strom von einem Gigabit/s an „spoofed" Paketen ein Paketsturm von dutzenden Gigabit/s beim Ziel des Angriffs werden.

CERT.at hat daher 2015 die Netzbetreiber in Österreich informiert, welche IP-Adressen in den jeweiligen Netzen für so eine Angriffsverstärkung verwendet werden können. Die Entwicklung sieht wie folgt aus:

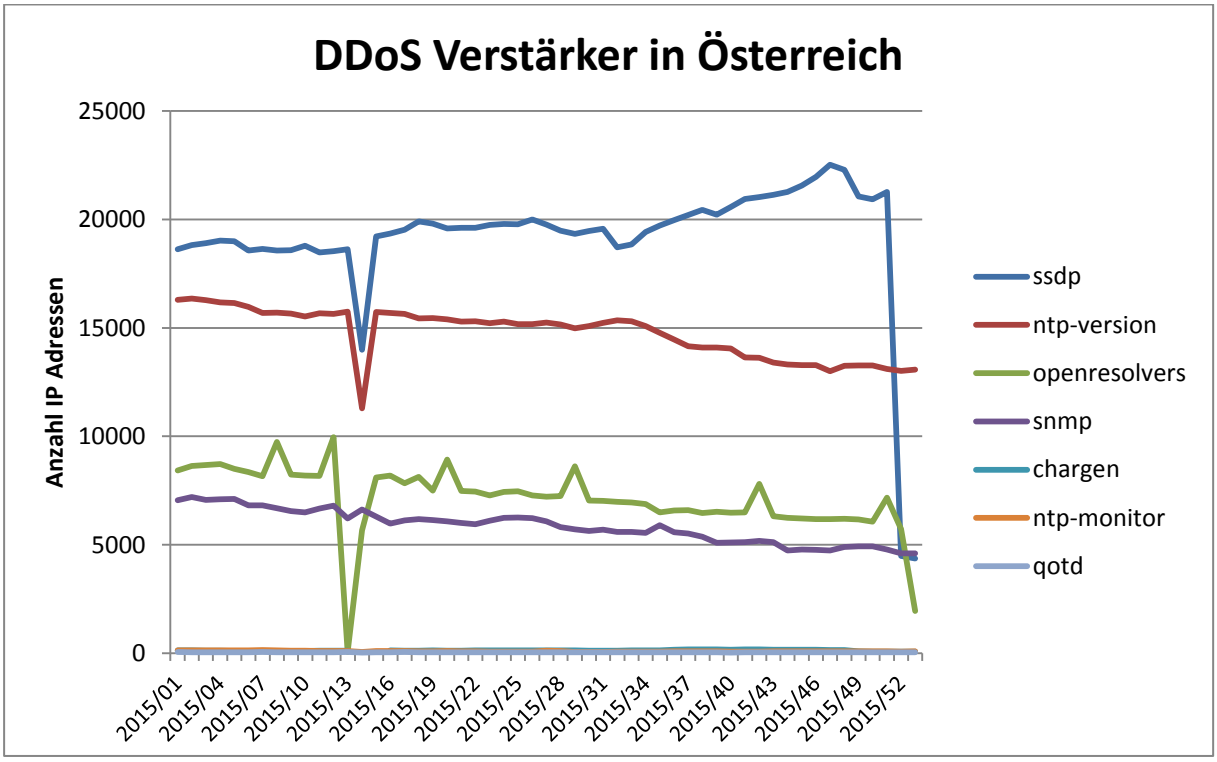


Abbildung 10: Zahl der IP-Adressen als potentielle Angriffsverstärker nach den jeweiligen Netzen im Zeitverlauf: Quelle: CERT.at

Bemerkenswert ist hier, dass die Zahl der per SSDP (Simple Service Discovery Protocol) ausnutzbaren IP Adressen bis Mitte Dezember noch angestiegen ist. Schuld daran ist ein Bug in der Firmware eines Modems, das ein einzelner ISP (Internet Service Provider) an seine Kunden liefert. CERT.at hat das Gespräch mit diesem Provider gesucht und so konnte erreicht werden, dass dieser ISP SSDP-Reflection in seinem Netz unterbunden hat.

Transport Layer Security (TLS)

Der bei weitem größte Anteil der TLS-Probleme ist die Verwendung des obsoleten Standards SSLv3: Dieses Protokoll hat ein inhärentes Problem, das sich mit der „POODLE" Attacke ausnutzen lässt. Da manch alte Webbrowser den modernen Verschlüsselungsstandard TLS1.2 noch nicht beherrschen, kann man das zögerliche Deaktivieren von SSLv3 teilweise nachvollziehen. Daher hat CERT.at 2015 die Betreiber von solchen Webservern noch nicht informiert. Wir hoffen aber doch, dass 2016 die Rücksichtnahme auf den Internet Explorer unter Windows XP – beides wird von Microsoft schon länger nicht mehr gewartet – dem Ende zugeht. CERT.at wird damit beginnen, künftig Warnmails bezüglich SSLv3 zu versenden.

Neben „POODLE" wurde auch unter dem Namen „FREAK" ein Angriff gegen manche TLS Server bekannt. Den Zahlen nach, die CERT.at vorliegen, läuft noch auf rund 600 IP-Adressen ein Webserver, der für diesen Angriff verwundbar ist.

Der Heartbleed-Bug in der openssl Library, die in vielen Mail- und Webservern benutzt wird, sorgte im April 2014 für viel Aufsehen und für Überstunden bei den Systembetreuern, die

ihre Server auf eine bereinigte openssl-Version aktualisierten. CERT.at misst seit Mai 2015, wie sehr auf Web- und Mailservern, die für .at-Domains zuständig sind, der Heartbleed-Bug noch präsent ist.

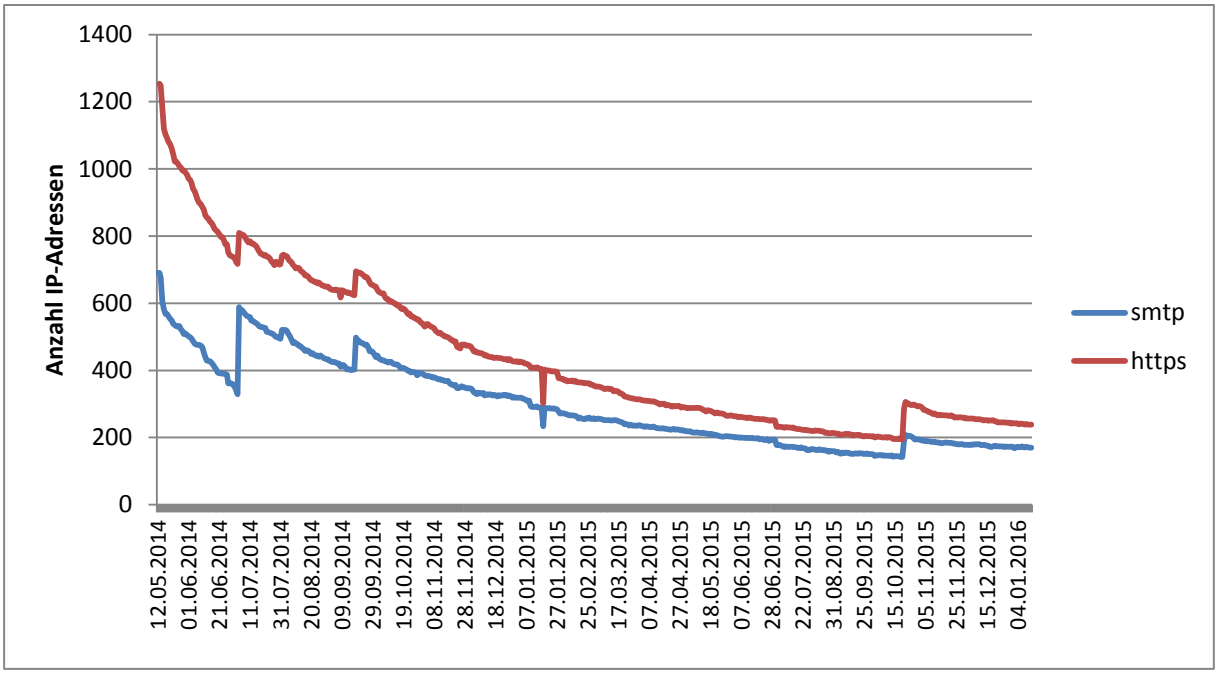


Abbildung 11: Zahl der von Heartbleed befallenen IP-Adressen nach Servern im Zeitverlauf: Quelle: CERT.at

Die Spitzen nach oben ergeben sich aus den unregelmäßig vorgenommenen Aktualisierungen der Domainliste bzw. der Zuordnung zu IP-Adressen. Stichproben bei den noch verbleibenden, verwundbaren Servern ergaben, dass dort keine relevanten oder sensitiven Services mehr betrieben werden.

Immer mehr Unternehmen auch in Österreich von Angriffen betroffen

Wie es um die IT-Sicherheit in österreichischen Unternehmen bestellt ist, hat SORA im Auftrag von A1 unter die Lupe genommen.[25] Ein Drittel der befragten Unternehmen musste bereits auf Schadensfälle reagieren. Sogar 80% hatten mit Beeinträchtigungen ihrer Systeme zu kämpfen. Den häufigsten Bedrohungen – Schadsoftware aus dem Internet, technische Probleme wie Netzwerkausfälle und Angriffe von Hackern – wird mit laufender Wartung, Updates und Schulungen entgegen getreten. 95% der Unternehmen setzen demzufolge zwar auf Anti-Virus und Anti-Malware Software, jedoch verwenden nur 86% eine Firewall. Mobile Endgeräte werden nur von 38% der Befragten geschützt. Es bleibt eine wichtige Erkenntnis zurück: IT-Sicherheit ist ein ganzheitlicher Prozess, der sich nicht nur auf Anti-Virus Software beschränkt, sondern viele weitere Bereiche wie u.a. die Gebäude-Infrastruktur oder die MitarbeiterInnenschulung umfassen sollte.

[25] Quelle: http://www.a1.net/newsroom/2015/06/a1-praesentiert-studie-zur-it-sicherheit-in-oesterreichischen-unternehmen/

Gefahr durch Ransomware

Auch Ransomware hielt österreichische InternetnutzerInnen 2015 in Atem. Diese Malware befällt den Rechner und verschlüsselt Dateien, sowohl auf der lokalen Festplatte als auch auf Netzwerklaufwerken. Bezahlt man das Lösegeld (= Ransom), so versprechen die Täter ein Werkzeug zur Wiederherstellung der Dateien. Der tatsächliche Schaden durch diese Programme kann nur geschätzt werden, da viele der Betroffenen den Fall nicht zur Anzeige bringen. Ransomware gehört mittlerweile auch in Österreich zu den gefährlichsten Angriffsformen. Der Ransomware-Trojaner **„CryptoLocker"** war im Frühjahr 2015 sehr präsent. Über E-Mail-Anhänge, gefälschte Paketdienst-Links und Webseiten verbreitet, befiel CryptoLocker zahlreiche Rechner, hauptsächlich von kleinen und mittelgroßen Unternehmen (KMU). Im Durchschnitt wurden 500 Euro – meist in Bitcoins (eine Art Internetwährung) – für den Entschlüsselungscode gefordert.

Auch Kaspersky warnt verstärkt vor Ransomware[26] und sieht künftig vor allem Smartphones, Gamer und Cloud Speicher im Visier. Alleine die Schadsoftware „Teslacrypt 2.0" greift gezielt mehr als 185 Dateiformate an. Eine Backup-Strategie für als wertvoll eingestufte Daten ist daher unerlässlich. Gerade für KMU können solche Angriffe existenzbedrohend sein. Schließlich geht es oft um KundInnendaten, was auch eine zivilrechtliche Komponente nach sich ziehen kann. Ransomware Attacken stiegen laut Kaspersky 2014 weltweit um mehr als das doppelte an – in der gleichen Zeit vermehrte sich sogar die Zahl der „CryptoLocker"-Opfer um das 45-fache.

Erpressungen mittels DDoS Angriffen

Bei Ransomware droht ein Angreifer/Erpresser mit dem Verlust der eigenen Daten, bei DDoS (Distributed Denial of Service) richten sich Angriffe auf die Verfügbarkeit der Netzwerkanbindung seiner Opfer. Wenn so eine Attacke die Netzwerkanbindung oder die Server des Opfers überlasten, dann können legitime Kunden des Opfers dessen Online-Dienstleitungen nicht mehr nutzen. Im Bereich von Wettanbietern und im Rotlicht-Milieu wurden diese Methoden schon länger zur Verdrängung des Wettbewerbs benutzt, auch im Bereich des Hacktivismus wurden in der Vergangenheit gerne DDoS-Angriffe benutzt.

In den letzten zwei Jahren hat sich der Kreis der DDoS-Opfer stark erweitert, vor allem durch das Aufkommen von Erpressungen. Im Juli 2014 tauchte die Gruppe DD4BC (DDoS for Bitcoins) zum ersten Mal auf. Initial richteten DD4BC ihre Attacken auf Bitcoin-Webseiten, dann auf Finanzdienstleister, E-Commerce Webseiten und ISPs. 2015 gerieten auch österreichische Firmen ins Blickfeld von DD4BC.[27] Ohne Schutz sind Unternehmen anfällig für diese Art von Attacken. Auch in Österreich wurden so Systeme überlastet und in der Folge Erpressungs-E-Mails versendet. Die Erpressungssummen bewegten sich oft im fünfstelligen Bereich und wurden in Form von Bitcoins verlangt. Bei ausbleibender Zahlung wurden

[26] Quelle: http://futurezone.at/produkte/kaspersky-ransomware-auf-dem-vormarsch/151.780.063
[27] Quelle: https://www.link11.de/share/public/Link11_DD4BC_Erpressermail_180915.pdf

weitere DDoS Angriffe angedroht. Neben Österreich und Deutschland war die Gruppe vor allem in Skandinavien, Australien und den Vereinigten Staaten aktiv.

Im Fall von DD4BC sieht ein typischer Erpressungsversuch wie folgt aus: Zunächst erfolgt eine Überlastung des Systems eines Unternehmens. Danach versendet DD4BC eine Erpressungs-E-Mail. Bei Nichtzahlung werden weitere Angriffe in höherem Datenausmaß angedroht. Neben immer höher werdenden Geldforderungen kann sich die Dauer der Angriffe von ein paar Stunden bis zu ein paar Tagen hinziehen. In manchen vereitelten Fällen kam es auch vor, dass DD4BC den Angriff zu einem späteren Zeitpunkt wiederholte.

Im Dezember 2015 konnten im Zuge einer Aktion von Europol – unter Federführung des österreichischen Cybercrime-Competence-Centers (C4) im Bundeskriminalamt – die Täter gefasst werden.[28]

Nachahmungstäter

Neben DD4BC hat seit Oktober 2015 auch eine zweite Gruppe, nämlich „Armada Collective" DDoS Attacken gestartet. Die Vorgehensweise ist fast ident zu jener von DD4BC. „Armada Collective" versendet unzählige Anfragen mit dem Ziel der Überlastung eines Systems und gibt dem Opfer nach der Erpressungsnachricht vier Tage Zeit bis zur Zahlung von Lösegeld.

Die Opfer waren auch hier bunt gemischt: Zuerst nur E-Mail-Dienstleister, dann aber auch Internet Service Provider, Banken und E-Commerce Seiten. Auch österreichische Firmen waren betroffen. In diesen Fällen konnte sich CERT.at einbringen: So wurde erreicht, dass alle Betroffenen untereinander ihre Erfahrungen und Reaktionen teilten, und man sich auf eine gemeinsame Vorgehensweise gegen die Erpressung geeinigt hat. Aus dem internationalen Kontaktnetz von CERT.at wurden weitere Erfahrungsberichte eingeholt und an die Erpressungsopfer weitergegeben. Auch die Zusammenarbeit mit der Polizei und dem Cyber Security Center im BVT wurde koordiniert.

Nach der Festnahme der DD4BC-Tätergruppe wurde es auch um Armada Collective ruhig.

Internet Service Provider sind mehr denn je gefordert

Technisch gesehen beruht der Großteil der Angriffe von DD4BC und Armada Collective auf Reflected DDoS: Dazu braucht es für den Täter a) die Möglichkeit, IP-Pakete mit gefälschten Absenderadressen zu versenden, und b) Services, die sich vom Täter als Verstärker missbrauchen lassen. Um ersteres zu unterbinden sollten ISPs die Datenpakete in ihren Netzen nach Best Current Practice (BCP) 38[29] filtern. Bezüglich der möglichen Reflektoren/Verstärker in deren Netz ist CERT.at in laufendem Kontakt mit den ISPs. Dieser

[28] Quelle: http://www.bmi.gv.at/cms/bk/_news/pressemeldungen.aspx?id=736870697475742F454E6F3D&page=0&view=1

[29] Quelle: https://tools.ietf.org/html/bcp38

Bereinigungsprozess schreitet zwar nur langsam voran, aber der Trend – siehe Abbildung 10 – geht hier in die richtige Richtung.

Sind diese beiden Punkte behandelt, so kann der ISP nicht mehr einen Reflected DDoS verursachen. Dass er selber – oder einer seiner Kunden – ein Opfer eines solchen wird, wird dadurch aber nicht verhindert.

Was aus den Angriffen mitzunehmen ist bzw. die **Empfehlungen von CERT.at** sind im Falle einer DDoS Attacke wie folgt:

- Das verlangte Lösegeld auf keinen Fall bezahlen. Es ist durch eine Zahlung nicht garantiert, dass keine weiteren Angriffe folgen werden. Außerdem steigt auch die Wahrscheinlichkeit für Nachahmungs- und Wiederholungstäter.
- In jedem Fall sollte Kontakt mit CERT.at aufgenommen werden.
- Eine DDoS Attacke ist eine Straftat im Cyber Space. Sie sollte daher zur Anzeige gebracht werden, damit an der Ausforschung der Täter gearbeitet werden kann. Je mehr Opfer sich melden, desto mehr Ressourcen kann die Exekutive bereitstellen.
- Kontakt sollte daher auch mit dem Cyber Crime Competence Center (C4), der nationalen Koordinierungs- und Meldestelle zur Bekämpfung der Cyber Kriminalität des BM.I, aufgenommen werden.
- Kontakt zum Upstream-ISP aufnehmen. Viele der Angriffe können vom Opfer alleine nicht mehr abgewehrt werden, daher benötigt es die Mithilfe beim Upstream.
- Zu empfehlen ist auch die Kontaktaufnahme mit dem Cyber Security Center (CSC) im BVT.
- Recherchieren: Inzwischen gibt es einiges an Ressourcen im Netz bzgl. DDoS Mitigation inkl. Handlungsempfehlungen. Siehe etwa www.melani.admin.ch.

Verschlüsselung bleibt weiter ein Thema

Die durch Edward Snowden ans Licht gekommenen Enthüllungen haben dem Thema Verschlüsselung einen neuen Stellenwert gegeben. Immer mehr Mailserver verwenden daher auch Transportverschlüsselung. Von weltweit 33% im Jahr 2013 auf 61% im Jahr 2015[30] ist die Entwicklung durchaus positiv zu sehen. Die TLS-Verschlüsselung (Transport Layer Security) ermöglicht über das SSL/TLS Zertifikat (Secure Sockets Layer/Transport Layer Security) einen verschlüsselten Kommunikationsweg zu einem Server und bildet eine effektive Verschlüsselungsmethode. Leider werden jedoch weite Teile im Web noch immer im Klartext übertragen.

Gegen Ende 2014 zeichneten sich jedoch Probleme bei Verschlüsselungen ab - Stichwort POODLE (Padding Oracle On Downgraded Legacy Encryption).[31] Vor allem die SSL-Protokoll Version 3 (SSLv3) war betroffen. Durch eine darin vorhandene Schwachstelle können

[30] Quelle: http://derstandard.at/2000025672676/Gmail-warnt-kuenftig-vor-unverschluesselt-uebertragenen-Mails
[31] Quelle: http://derstandard.at/2000018234459/SSL3-Aus-fuer-altes-Verschluesselungsprotokoll

Angreifer die Daten zwischen dem Browser des Users und einer SSL-gesicherten Website abfangen und entschlüsseln. Zwar läuft mit 0,3% nur noch ein Bruchteil der verschlüsselten Kommunikation im Web über SSLv3, jedoch können neuere Verschlüsselungen (TLS 1.0 oder 1.1) insofern blockiert werden, so dass die Verbindung automatisch auf SSL 3.0 zurückfällt.

Die Internet Engineering Task Force (IETF) beschloss als eine Folge daraus das Ende von SSLv3. In der Erklärung gaben auch Google und Mozilla an, das fast 20 Jahre alte Protokoll nicht mehr zu unterstützen. Empfohlen wird, nunmehr ausschließlich TLS Protokolle zu verwenden, bestenfalls in der aktuellsten Version 1.2. SSL sollte auf allen Servern und Clients deaktiviert werden.

Logjam-Attacke hielt Server auch in Österreich in Schach

Mitte des Jahres kam auch die Verwundbarkeit des Diffie-Hellmann-Schlüsselaustauschs ans Licht, welcher beim Aufbau einer sicheren Verbindung zur Anwendung kommt. Sehr viele Server (Web-, Mail-, SSH- und VPN-Server) waren durch die sogenannte Logjam-Attacke[32] betroffen und deren verschlüsselte Verbindung somit geschwächt. Angreifern gelang es so, bei verschlüsselten Verbindungen an den Schlüssel zu kommen. Davon sind etwa vermeintlich sicher geglaubte Verbindungen, wie beispielsweise Passworteingaben oder die Verwendung von Online Banking, betroffen. Von der ersten Million der größten Websites waren zwischenzeitlich 8,4% betroffen. Die Sicherheitslücke im Protokoll ermöglichte es, die Kommunikation in Echtzeit abzufangen und damit Daten zu stehlen. NutzerInnen haben darauf zu achten, stets die aktuellste Version und alle Updates des jeweiligen Browsers installiert zu haben. Umfangreichere Sicherheitsmaßnahmen bestehen in diesem Zusammenhang für Systemadministratoren.[33]

Vergleichbar mit Logjam war auch die Sicherheitslücke FREAK[34], die eine Entschlüsselung von gesichertem Datenverkehr ermöglichte. Dabei wurde bestimmten Browsern durch eine Sicherheitslücke die Nutzung einer veralteten und daher unsicheren Verschlüsselungsform aufgezwungen. Betroffen waren davon unter anderem der Standard-Android Browser, Safari, Chrome (nur die Versionen für Android und OS X), Opera und Opera Mini, Internet Explorer und der Blackberry Browser.

[32] Quelle: http://www.heise.de/security/meldung/Logjam-Attacke-Verschluesselung-von-zehntausenden-Servern-gefaehrdet-2657502.html
[33] Quelle: https://weakdh.org/
[34] Quelle: http://www.spiegel.de/netzwelt/web/freak-sicherheitsluecke-betrifft-weitere-browser-und-windows-a-1022091.html

Ablöse vom SHA 1 Signier-Standard

SHA 1 (Secure Hash Algorithm) wurde lange Zeit als Signier-Standard für SSL/TLS Zertifikate verwendet. Solche Zertifikate werden beispielsweise eingesetzt, wenn Daten von Webseiten verschlüsselt zum Browser übertragen werden sollen. Da dieser Standard mittlerweile als nicht mehr sicher gilt, gaben bereits Ende 2014 die Browserhersteller ihre Pläne zur schrittweisen Ablehnung von SHA-1-Zertifikaten bekannt („gradually sunsetting SHA-1").[35]

Seit dem Bekanntwerden dieser Pläne werden neue SSL/TLS Zertifikate vermehrt mit dem Nachfolge-Standard SHA 2 ausgestellt und eingesetzt.

Für NutzerInnen älterer Smartphones oder Rechner entsteht hier das Problem, dass ihre Browser die SHA 2 Methode nicht unterstützen. CloudFlare rechnet damit, dass mehr als 37 Millionen Menschen weltweit betroffen sind und bietet wie auch Facebook seinen Nutzern eine Art automatischen SHA-1 Fallback-Mechanismus an.

Lücke im TLS-Protokoll

Das österreichische Technologieunternehmen Rise hat im Herbst 2015 eine Lücke im TLS-Protokoll entdeckt.[36] Den betroffenen Unternehmen, dazu gehörten u.a. Apple und Facebook, blieben dadurch viele „Man-in-the-Middle Attacken" durch die Schließung der Lücke erspart. Bei dieser Form von Angriffen schleusen sich Hacker in den Kommunikationsweg zwischen Opfer und Zielserver ein, geben sich als Zielserver aus und können so die übermittelten Daten mitlesen. Es ist sehr erfreulich, dass gerade ein österreichisches Unternehmen dazu beitragen konnte, diese gefährliche Sicherheitslücke zu schließen.

Vorsicht vor gefälschten Rechnungen

Eine weitere Entwicklung, die auch zahlreiche ÖsterreicherInnen konfrontiert, ist die Verlagerung von Betrugsmaschen in das Internet. Das reicht von Vorschussbetrug[37], über den Neffentrick[38] bis hin zum Versuch, mit gefälschten Rechnungen an Geld zu gelangen. Selbst mit gefälschten Rechnungen für Partezettel gehen Online Angreifer mittlerweile vor.[39] Regelmäßig sind große Online Unternehmen wie Amazon & Co. von in Umlauf gebrachten gefälschten Rechnungen betroffen.[40] Hierbei ergeht eine E-Mail von einem angeblichen Anwalt an die KundInnen. Die Anwalt-Variante ist zwar neu, die Ziele bleiben jedoch die alten. Nämlich das Erspähen von Kontodaten oder das Drängen zur Überweisung. Diese Variante ist jedoch nur eine von vielen gegenwärtig im Umlauf befindenden Online-Betrugsmaschen.

[35] Quelle: https://googleonlinesecurity.blogspot.co.at/2014/09/gradually-sunsetting-sha-1.html
[36] Quelle: http://derstandard.at/2000022197161/Oesterreichische-Forscher-entdecken-TLS-Schwachstelle
[37] Quelle: https://de.wikipedia.org/wiki/Vorschussbetrug
[38] Quelle: https://de.wikipedia.org/wiki/Enkeltrick
[39] Quelle: http://www.kleinezeitung.at/k/kaernten/chronik/4668805/SpittalDrau_Betruger-verrechnen-Kosten-fur-Partezettel
[40] Quelle: http://salzburg.orf.at/news/stories/2743367/

Außerdem sind u.a. auch E-Mails von Paketdienstleistern, Mobilfunkanbietern oder Banken im Umlauf. Über die E-Mails wird versucht, die User auf Websiten zu locken, die diverse Schadsoftware („Geodo", „Dridex", „Dyre", ...) verbreiten. Nach Klick auf den Link im E-Mail wird man auf eine kompromittierte Webseite weitergeleitet, die eine .zip oder .exe Datei zum Download bereitstellt. Nach deren Ausführung wird der Schadcode installiert. Es ist für den Laien oft schwierig, diese gefälschten Mails von Originalmails zu unterscheiden.

Seitensprung mit Folgen: Datendiebstahl und vieles mehr

Zahlreiche ÖsterreicherInnen waren auch betroffen, als im August 2015 das Seitensprung-Portal ashleymadison.com durch die Hackergruppe „Impact Team" angegriffen wurde.[41] Die gestohlenen Daten von 32 Millionen Usern weltweit beinhalteten unter anderem Namen, Adressen und Telefonnummern. Neben US-Regierungs- und Militäradressen wurden auch rund 80.000 Datensätze aus Österreich publik. Mittlerweile ist bei Ashley Madison eine Vielzahl an Schadenersatzklagen anhängig. Die Höhe der bevorstehenden Zahlungen ist kaum abzusehen, wobei alleine in Kanada über 400 Millionen Euro eingeklagt werden.

Österreichische Unternehmen sind Angreifern oft ausgeliefert

Bei unzureichenden Sicherheitsvorkehrungen sind österreichische Firmen anfällig für Datendiebstähle. In den beiden folgenden Gastbeiträgen wird anhand von Beispielen die aktuelle Bedrohungslage beschrieben.

[41] Quelle: http://futurezone.at/digital-life/80-000-oesterreicher-von-seitensprung-datenleck-betroffen/148.120.829

5. GASTBEITRAG: CYBER CRIME – EINE REALE BEDROHUNG FÜR KLASSISCHE GESCHÄFTSMODELLE (DR. THOMAS STUBBINGS)

27. Februar 2015. Sergey (Name geändert, Anm.), Händler einer großen russischen Bank kommt aus der Mittagspause zurück. Als er seinen Bildschirm mit dem Handelssystem aufdreht, traut er seinen Augen nicht. Auf seinem Handelsaccount wurden in der letzten Viertelstunde Devisengeschäfte in der Größenordnung mehrerer Hundert Millionen Dollar durchgeführt – während er Mittagessen war! Als Sergey den Verlauf dieser Geschäfte genauer prüft wird er schlagartig blass und ruft sofort seinen Vorgesetzten an: durch die massiven Verkäufe und Käufe innerhalb kürzester Zeit war eine Rubel-Dollar-Volatilität in einer Bandbreite von 55 bis 66 entstanden, das ist das Zehnfache des Normalen – und das auf Kosten seiner Bank. Gesamtschaden: über 5 Millionen US-Dollar.

Bei genauer forensischer Untersuchung des Vorfalls stellt sich heraus, dass das System des Händlers mit einem neuartigen Trojaner befallen war, dem Corkow-Trojaner russischer Herkunft, der genau für diesen Angriff entwickelt worden war. Es stellt sich weiters heraus, dass die Infektion bereits fünf Monate früher stattgefunden hatte und seit über zwei Monaten eine intensive Überwachung jeglicher Tätigkeit des Händlers auf seinem PC stattgefunden hatte. Jede Mausbewegung, jeder Tastenanschlag war mitgeloggt und an die Cyber Angreifer übermittelt worden. Diese hatten sich dabei komplett ruhig verhalten, da sie keinesfalls auffallen oder entdeckt werden wollten.

Um die Sicherheitsvorkehrungen der Bank zu umgehen, wurde der Trojaner in dieser Zeit ständig aktualisiert und verändert, um nicht von Anti-Viren Programmen entdeckt zu werden. Dies war so erfolgreich, dass niemand etwas von der Infektion merkte. Am 27.2. schlugen die Täter dann schließlich zu: Punkt 12:30 Uhr, während der Mittagspause des Händlers übernahmen sie mit dem Fernzugriffsmodul des Trojaners die Steuerung des Handelssystems, das ihnen die vollständige Kontrolle ermöglichte. Sie konnten nach Belieben Kaufen, Verkaufen, ja sogar Limits des Händlers erhöhen. So war es ihnen möglich, in nur 14 Minuten Kauforders in der Höhe von 437 Mio. US-Dollar und Verkauforders in der Höhe von 97 Mio. US-Dollar zu platzieren. Von den Kauforders wurde zwar nur etwa ein Drittel tatsächlich ausgeführt, vermutlich aufgrund der begrenzten Zeit, aber dennoch reichte dies für einen Millionenschaden für die Bank. Es wird vermutet, dass die Täter bei einer anderen Bank gegenläufig spekuliert haben und somit einen Teil des Verlustes der Bank als Gewinn für sich verbuchen konnten.

Der zielgerichtete Angriff auf ein Handelssystem war tatsächlich ein Novum im Jahr 2015. Die gezielte Attacke auf IT-Kernsysteme ist hingegen schon länger traurige Realität. Im Jahr 2013 haben Mitglieder der russischen Carperb-Gruppe eine neuartige Malware namens Carbanak in Umlauf gebracht, mit welcher mehr als 50 russische Banken und fünf Zahlungsverkehrssysteme angegriffen wurden, was insgesamt zu einem Schaden in Höhe von

einer Milliarde US-Dollar geführt hat und für zwei Banken den Verlust ihrer Banklizenz zur Folge hatte.

Dies war der erste Fall, bei dem ein Cyberangriff zu einem vollständigen Verlust der Geschäftsbasis einer Bank geführt hat. Die Vorgehensweise ist dabei immer dieselbe: Der Angriff beginnt mit gezieltem Inverkehrbringen der Schadsoftware durch sogenanntes „Spear-Phishing", dabei werden E-Mails mit interessant klingenden Anhängen wie „Planung2015.xls" oder „Gehaltsliste.xls" an ausgewählte MitarbeiterInnen geschickt. Nach einer Studie von Verizon öffnen 23% der MitarbeiterInnen Phishing E-Mails und 11% klicken auf Anhänge; die Schadsoftware findet somit fast immer ihren Weg ins Unternehmen. Sobald der Schadcode die Unternehmensgrenze überwunden und sich auf einem PC festgesetzt hat, sucht er nach einem privilegierten User, üblicherweise einen PC-Administrator, und versucht dessen Passwort zu knacken. Nachdem dies geschafft ist, identifiziert der Angreifer einen Server, auf den der privilegierte User Zugriff hat. Auf diesem Server versucht der Angreifer nun das Passwort des Domänenadministrators zu überwinden; damit hat er Kontrolle über die gesamte Domäne. Nun werden noch E-Mail und Workflow-Server übernommen sowie Workstations, die Zugriff auf das Kernbank- und Zahlungsverkehrssystem haben.

Auf diesen werden dann Überwachungstools installiert, Keyboard-Logger sowie Kameraüberwachung. Die BenutzerInnen werden dann über die nächsten Wochen und Monate regelrecht ausspioniert, die Tätigkeiten und Gewohnheiten werden studiert und protokolliert, Prozesse und Freigabemechanismen werden analysiert. Zuletzt werden Fernzugriffsmodule installiert, mit denen der Angreifer Zugriff auf die Steuerung der Banksoftware erhält und über die er zu gegebener Zeit in einer konzertierten Aktion zuschlägt. Dabei werden verschiedene Betrugsmethoden angewendet: von der Manipulation von Zahlungsverkehrsströmen, Veränderung von Kontobilanzen bis hin zur Fernsteuerung von Bankomaten, die auf Knopfdruck Geld ausgeben, reicht dabei das Portfolio der Angreifer. Das Ganze dauert meist nur wenige Minuten oder Stunden, danach wird der Code per Fernsteuerung wieder gelöscht, um alle Spuren zu verwischen.

Auch wenn Banken oft Ziel von Cybercrime Angriffen sind, so sind es keineswegs nur Finanzdienstleister, die im Fokus der Cyberkriminellen stehen. Ganz im Gegenteil: Cyber Angreifer haben keine besonderen „Präferenzen" bei ihren Opfern, sondern sie schlagen dort zu, wo sie Beute vermuten. Und das sind in zunehmendem Ausmaß auch mittlere und kleinere Unternehmen aller Branchen. Nach dem Symantec Internet Security Report 2015 richten sich ein Drittel aller Angriffe bereits gegen Unternehmen bis 250 MitarbeiterInnen und damit dem klassischen KMU.

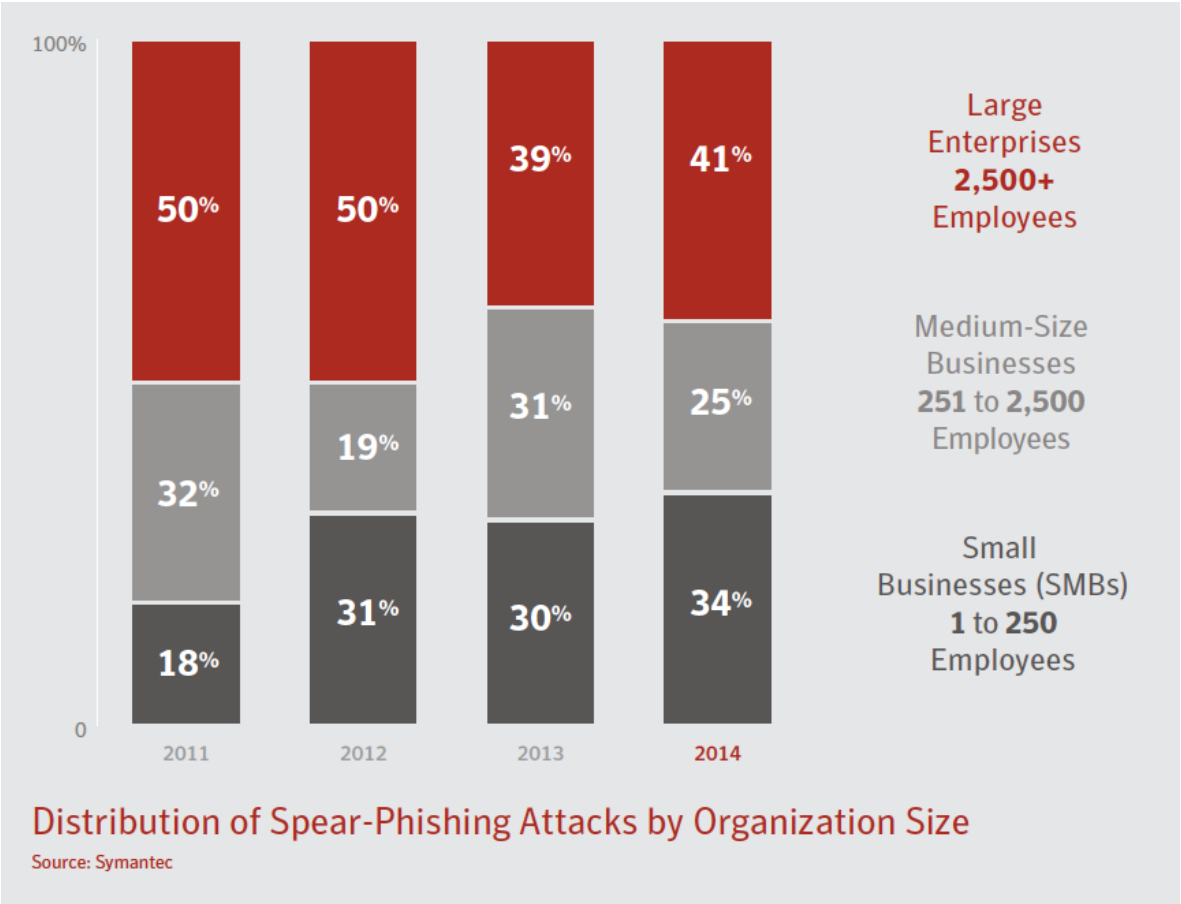


Abbildung 12: Distribution of Spear-Phishing Attacks by Organization Size (Quelle: Symantec)

Die Tendenz ist weiter steigend, was nicht verwundert, haben doch gerade KMUs oft nur unzureichende Sicherheitsstrategien entwickelt. Sie sind im Vergleich zu Banken sicherheitstechnisch deutlich schlechter aufgestellt und somit leichte Beute. Ein gutes Beispiel hierfür sind sogenannte „digitale Erpressungsversuche", welche im letzten Jahr um mehrere hundert Prozent zugenommen haben. Dazu gibt es verschiedene Vorgehensmuster: eines bedient sich **Distributed Denial of Service Attacken (DDoS)**, bei welchen von weltweit verteilten Systemen, oft mehrere zehntausend, Datenpakete an das Opfer geschickt werden, bis dessen Rechner hoffnungslos überfordert sind und nicht mehr reagieren.

Der Cyber Angreifer startet nun einen solchen DDoS Angriff gegen ein Opfer, um zu demonstrieren wozu er in der Lage ist. Danach bietet er dem Opfer an - ganz im Stil der klassischen Schutzgelderpressung - von weiteren Angriffen gegen die Zahlung einer gewissen Summe Abstand zu nehmen. Die Summe ist meistens in einem Bereich, der für KMU noch verkraftbar ist, wohingegen professionelle DDoS Abwehrmaßnahmen oft das Zehnfache davon kosten, was dazu führt, dass manche KMU der Zahlungsaufforderung Folge leisten.

Ein zweites Vorgehensmuster ist noch perfider und beruht auf einer sogenannten **Cryptolocker-Attacke**. Dabei sorgt eine über E-Mails eingebrachte Schadsoftware dafür, dass sämtliche Daten im Netzwerk mit starker Kryptographie verschlüsselt werden. Der Cyber

Angreifer bietet dem Opfer nunmehr an, für die Zahlung einer bestimmten Summe den Schlüssel bekannt zu geben, mit dem das Opfer wieder an seine Daten kommt. Für viele Betroffene stellt dies ein existenzielles Problem dar, besonders wenn sie nicht mit einer geeigneten Backup Strategie vorgesorgt haben. In diesen Fällen wird oft bezahlt, in der Praxis erhält das Opfer aber in einer Vielzahl der Fälle den Schlüssel dennoch nicht. Es hat bereits Fälle gegeben, wo Firmen aufgrund von Cyber Angriffen ihrer Geschäftsgrundlage beraubt wurden.

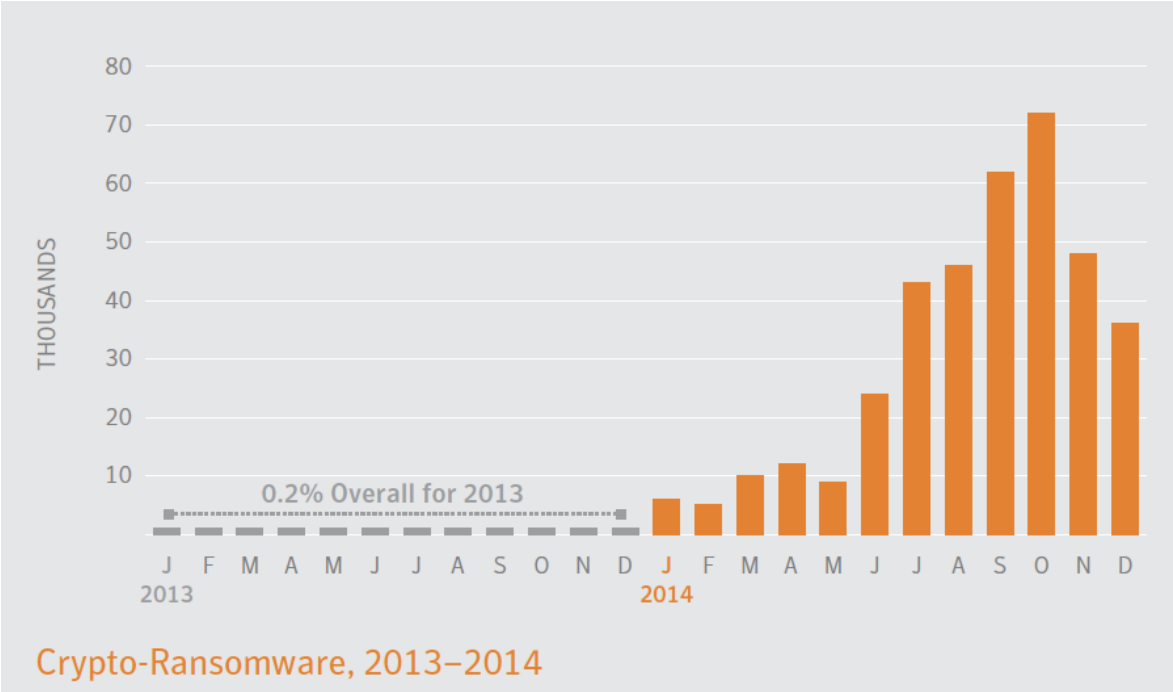


Abbildung 13: Crypto-Ransomware, 2013-2014 (Quelle: Symantec)

Das Fazit aus diesen Entwicklungen ist einfach

Kein Unternehmen, egal wie groß oder klein, egal in welcher Branche, kommt heute noch um das Thema Cyber Sicherheit herum. Jedes Unternehmen ist gut beraten, sich zeitgerecht mit dem Thema zu beschäftigen und eine für seine Größe und sein Geschäftsmodell ausgerichtete Cyber Sicherheits Strategie zu erstellen, um sich auf Angriffe vorzubereiten. Nur so können die Auswirkungen solcher Angriffe so gering wie möglich gehalten werden. Eine geeignete Strategie muss nicht immer kostspielig sein, oft sind es kleine Anpassungen, die schon weiterhelfen. Wichtig ist jedenfalls die Auseinandersetzung mit dem Thema auf Geschäftsführungsebene.

Cyber Sicherheit ist dabei keineswegs ein Thema nur für IT-Abteilungen. Es geht um das Geschäftsmodell und die Existenz des ganzen Unternehmens – und damit muss es Chefsache sein. Die Bedeutung des Themas hat inzwischen auch der Gesetzgeber erkannt. Im Jahr 2013 wurde von der EU-Kommission im Rahmen ihrer „Digital Single Market Strategy" und auf Basis der Cyber Security Strategie der EU die Entwicklung der sogenannten NIS Directive beauftragt, welche ein Regelwerk zur Herstellung eines „hohen Niveaus von Netzwerk- und Informationssicherheit" in Europa darstellt. Diese NIS Directive ist gerade in Fertigstellung, ihr

formaler Beschluss durch den EU-Ministerrat wird für Mai 2016 erwartet. Spätestens zwei Jahre später ist diese Direktive in nationales Recht umzusetzen.

Das bereits im Juli 2015 in Kraft getretene deutsche IT-Sicherheitsgesetz zeigt, wohin es gehen wird: verpflichtende Mindeststandards, umfassende Prüfrechte durch zu schaffende NIS-Behörden sowie eine Meldepflicht für schwerwiegende IT-Sicherheitsvorfälle. Spätestens 2018 wird es somit auch in Österreich ein entsprechendes IT-Sicherheitsgesetz geben und Unternehmen werden sich mit diesen Herausforderungen befassen müssen. Es ist jedoch empfehlenswert, mit dem Handeln bezüglich Cyber Sicherheit nicht erst auf das Gesetz zu warten, sondern bereits jetzt tätig zu werden. Denn die Angreifer sind schon jetzt höchst aktiv und werden mit Sicherheit nicht bis 2018 warten.

© TS MC

Gastbeitrag von: Dr. Thomas C. Stubbings

Dr. Thomas C. Stubbings ist selbstständiger Unternehmensberater und berät unter anderem die Raiffeisenbank International Gruppe zum Thema Cyber Sicherheit. Des Weiteren ist er Vorsitzender der Cyber Security Plattform der österreichischen Bundesregierung und in zahlreichen nationalen und internationalen Gremien vertreten.

6. GASTBEITRAG: SPOOFED INVOICE FRAUD – CYBER VORFÄLLE TREFFEN ÖSTERREICHS INDUSTRIE (DIPL.-ING. MAG. ANDREAS TOMEK)

Österreich – Land des Mittelstandes, der Familienbetriebe und der Branchenkaiser. Ende 2014 und 2015 wurden vor allem diverse Industriebetriebe Opfer des Spoofed Invoice Frauds. Im Rahmen der Aufklärung und bei der Maßnahmenberatung vor Ort hat SBA Research gemeinsam mit CERT.at Lessons Learned aus diesen Vorfällen abgeleitet, die nachfolgend vorgestellt werden.

Rückblickend auf das Internetjahr 2015 wissen wir von mehr als einem halben Duzend dieser Angriffe. Manche davon waren erfolgreich, manche davon wurden durch Sicherheitsbewusstsein abgewehrt. Es entstanden dadurch teilweise direkte und indirekte finanzielle Schäden im sechs- und siebenstelligen Euro Bereich.

Dabei bedienen sich Angreifer der Methode eines so genannten „**Business E-Mail Compromises**" und folgen dabei zumeist einem ähnlichen Schema:

- Unternehmen A stellt per E-Mail eine Rechnung an Unternehmen B, über einen langjährigen Sales-Agent oder direkt.
- Einige Stunden später folgt ein zweites E-Mail von einer neu registrierten (mit Hilfe eines WebHoster Trial Accounts mit gefälschten Daten) und ähnlich klingenden/aussehenden Domain-Namen (der sich zum Beispiel dadurch unterscheidet, dass anstatt des Großbuchstaben „L" nun der Kleinbuchstabe „l" verwendet wird).
- Der gesamte Inhalt der E-Mail ist mit der vorigen ident, inklusive Adressaten, Anhängen und CC-Empfängern. Die Adressen der letzteren beinhalten aber nun alle die gefälschte Domain.
- In der neuen E-Mail gibt es nun einen neuen Passus, der eine Änderung des Empfängerkontos verlangt. Mögliche angegebene Gründe dafür: Die Finanz sperrte ein Konto wegen Audit o.ä.
- Kommt es zu Rückfragen durch das Unternehmen B, wird vom Angreifer geantwortet, das wiederum teils mit gefälschten Dokumenten.
- Erkennt Unternehmen B diesen Angriffsversuch nicht, überweist es das Geld somit auf ein falsches Konto, nämlich jenes des Angreifers.

Das Federal Bureau of Investigation (FBI) warnt in einem Public Service Announcement vor dieser Bedrohung und nennt auch konkrete Zahlen: So gab es alleine 2013 über 2.100 bekannte Opfer weltweit mit einem Schaden von insgesamt rd. 215 Millionen US-Dollar, der nur auf diese bestimmte Betrugsform zurückzuführen ist.[42] Aber auch hier dürfte die Dunkelziffer deutlich höher liegen und das FBI geht davon aus, dass die Opferzahlen und Schadenshöhen weiter steigen werden.

[42] Quelle: https://www.ic3.gov/media/2015/150122.aspx

Das Gefährliche am Rechnungsbetrug

Glaubhaft waren die Angriffe vor allem dadurch, dass die Angreifer dabei zum entscheidenden Zeitpunkt in eine bestehende Kommunikation eingegriffen haben. Häufig wird dieses Vorgehen beim gleichen Opfer öfters wiederholt (2-3 mal pro Zielunternehmen), bis es zum Erfolg führt oder auffliegt. Typischerweise glauben Unternehmen erst beim zweiten Mal an interne Probleme. Dabei war zu beobachten, dass es sich bei fast allen betroffenen Unternehmen um produzierende Industrieunternehmen mit globalen Märkten bzw. Niederlassungen handelte. Auch dürften auf Angreiferseite mehrere Gruppen arbeitsteilig tätig sein, da z.B. die Domainanlage nicht mit dem Versandzeitpunkt der E-Mails abgestimmt war und so Angriffe aufflogen.

Die Kernfrage für Unternehmen lautet: Woher kommen meine E-Mails?

Unternehmen sollten sich daher jedenfalls immer wieder folgende Fragen stellen, um womöglich nicht selbst Opfer von Spoofed Invoice Fraud zu werden: Woher kommen die Original-E-Mails? Woher die Anhänge und teilweise die Unterschriften? Denn das sind Fragen, die Forensiker in jedem der Fälle beschäftigen. Hintergrund ist, dass es nämlich ein breites Spektrum an Optionen gibt, wo und wie ein Angreifer zuschlagen kann.

Potenzielle menschliche Täter können sein: Insider, das Management, Administratoren, Zwischenhändler, MitarbeiterInnen von TelKo-Anbietern oder Mailprovidern – sowohl auf Seite des Unternehmens, wie auch beim Kunden.

Auch die technischen Optionen sind vielfältig und reichen vom Client PC (User, Admin, Management), lokalem Mail-Server, LAN und Corporate WAN, Mail Provider, Internet, der IT-Infrastruktur beim Kunden bis hin zu Malware.

Forensische Untersuchung & Lessons Learned

Was kann man nun aus diesen Fällen mitnehmen? Der Status des Security Managements und der Incident Response ist in den ersten Stunden und Tagen entscheidend. Kernfragen wie „an wen wendet sich das Unternehmen“ oder „wer koordiniert externe HelferInnen und Parteien“ müssen vorab geklärt und geregelt sein. Gerade zu Urlaubs- und auch Ferienzeiten stellt sich die Frage, wer überhaupt Zeit und technische Mittel zur Untersuchung verfügbar hat und wie man im Falle des Falles schnell Hilfe bekommt. Oft sind auch rechtliche Fragen offen, wie zum Beispiel, wem man einen Angriff melden muss und wie man eine erkannte Fraud Domain abschalten lässt. Und auch der Versicherungsschutz und die Schadensübernahme sind im Nachhinein oft Themen, welche die Kraft des gesamten Unternehmens binden und es somit lähmen können.

Was Unternehmen tun können

In Bezug auf die in Österreich bekannt gewordenen Fälle können folgende Punkte als Lessons Learned weitergegeben werden:

- Einrichten eines Domain Monitorings der eigenen Firmennamen, Produkte & Webseiten.
- Etablierung eines Security Managements & Prozesse, sowie Festlegung einer Incident Response & Kommunikationsstrategie.
- Etablierung technischer Voraussetzungen für eine forensische Auswertung, insbesondere: Logs, Logs, Logs! Moderne AV (Anti-Viren) und APT (Advanced Persistent Threat) Tools, Firewall und Mail Server Auswertungen sowie AD (Access Directory) Access Logs
- AnsprechpartnerInnen und Dienstleister definieren, sowie Dienstleister in die rechtliche Pflicht nehmen (z.B. Mailprovider).

Und zu guter Letzt muss natürlich auch das Sicherheitsbewusstsein beim Senior Management und den MitarbeiterInnen geschaffen werden. Auf jeden Fall braucht es mehr gut ausgebildete ErsthelferInnen und wir müssen die Kommunikation in der Sicherheits Community forcieren. Denn Vorfälle können klein anfangen und sich rasch ausdehnen. Das ist vor allem eine Gefahr für den gehobenen Unternehmensmittelstand, der oft noch nicht bereit ist, eine solche Situation alleine zu meistern.

© SBA Research

Gastbeitrag von: Dipl.-Ing. Mag. Andreas Tomek

Andreas Tomek ist Geschäftsleiter für Professional Services & Business Development bei SBA Research. Er hat über 15 Jahre IT-Erfahrung in den Bereichen System Engineering & Administration, IT Security sowie IT Audit & Training. Sein Forschungsschwerpunkt liegt bei Konzepten der Softwaresicherheit sowie IT Auditing & Governance. Dazu ist er Lektor an der Donau-Universität Krems.

7. UPDATE: ÖSTERREICHISCHE STRATEGIE FÜR CYBER SICHERHEIT

Die nationale und internationale Absicherung des Cyber Raums ist eine der obersten Prioritäten Österreichs. Mit der Österreichischen Strategie für Cyber Sicherheit (ÖSCS) wurde von der Bundesregierung am 20. März 2013 ein umfassendes und proaktives Konzept zum Schutz des Cyber Raums und der Menschen in eben diesem beschlossen. Die Strategie für Cyber Sicherheit bildet das Fundament der gesamtstaatlichen Zusammenarbeit in diesem Bereich und beruht auf den Prinzipien Rechtstaatlichkeit, Subsidiarität, Selbstregulierung und Verhältnismäßigkeit. Ein offenes und freies Internet, der Schutz personenbezogener Daten, die Unversehrtheit von miteinander verbundenen Netzwerken sind Grundlage für globalen Wohlstand, Sicherheit und Förderung der Menschenrechte.

Die Implementierung der ÖSCS ist ein permanenter Prozess, der von einer eigenen Cyber Sicherheit Steuerungsgruppe koordiniert wird. Diese Steuerungsgruppe unterstützt im Rahmen eines Implementierungsplans mit klar geregelten Verantwortlichkeiten die Umsetzung der Strategie in Österreich entlang der folgenden sieben definierten Handlungsfelder:

Handlungsfeld 1: Strukturen und Prozesse
Die Stärkung bestehender Cyber Strukturen ist ein zentrales Anliegen im Rahmen der ÖSCS. Zur Schaffung einer gesamtstaatlichen Struktur zur Koordination auf operativer Ebene wurde die ebenfalls in der ÖSCS definierte Cyber Sicherheit Steuerungsgruppe (CSS) unter Vorsitz des Bundeskanzleramtes beauftragt. Diese Struktur arbeitet und koordiniert unter Einbindung der öffentlichen Ressorts und operativen Strukturen aus Wirtschaft und Forschung. Ihre Federführung liegt beim BM.I, welches dabei vom BMLVS unterstützt wird. Im Cyber Verteidigungsfall geht die Federführung auf das BMLVS über. Zur Bewältigung von Cyber Krisen wurde außerdem ein eigenes Cyber Krisenmanagement (CKM) eingerichtet, dessen Federführung im zivilen Bereich beim BM.I bleibt und im militärischen Falle auf das BMLVS übergeht. Die Arbeitsweise des Cyber Krisenmanagements und seine Zusammensetzung orientieren sich dabei eng am staatlichen Krisen- und Katastrophenschutzmanagement. Sämtliche neu definierten Strukturen und Prozesse basieren außerdem auf bereits bestehenden, wohl etablierten und bewährt effektiven Cyber Strukturen (z.B. bestehenden CERTs).

Handlungsfeld 2: Governance
Die Arbeitsgruppe Ordnungspolitischer Rahmen erarbeitet derzeit einen Bericht über die Notwendigkeit der Schaffung zusätzlicher rechtlicher Grundlagen, regulatorischer Maßnahmen und nicht-rechtlicher Selbstverpflichtungen für die Gewährleistung der Cyber Sicherheit in Österreich. Ein Zwischenbericht wurde im April 2015 vorgelegt, der Endbericht der Arbeitsgruppe, der auch die Ergebnisse der Arbeiten auf EU-Ebene zur Richtlinie für Netzwerk- und Informationssicherheit (NIS-RL) berücksichtigen wird, soll nach Abstimmung und Vorlage an die Regierung mittels eines Begleitgesetzes für Cyber Sicherheit umgesetzt

werden. Dabei werden auch Konsultationen der Wirtschaft und der Akademien berücksichtigt. Der Rahmen für die Umsetzung der in der NIS-Richtlinie vorgegebenen Maßnahmen soll ressortweit durch die Arbeitsgruppe Ordnungspolitischer Rahmen abgestimmt und festgehalten werden.

Seit 2014 wird außerdem ein jährlicher Bericht zur Cyber Sicherheit erstellt, der sich aus Informationen der verfügbaren österreichischen Cyber Sicherheitsberichte wie dem Internet-Sicherheitsbericht von CERT.at und GovCERT Austria und zusätzlichen Informationen aus den Ressorts zusammensetzt.

Handlungsfeld 3: Kooperation Staat, Wirtschaft und Gesellschaft

Im März 2015 wurde die Cyber Sicherheit Plattform (CSP) konstituiert. Sie gewährleistet einen periodischen Informationsaustausch zwischen Stakeholdern aus Wirtschaft, Wissenschaft und öffentlicher Verwaltung. Für kleine und mittlere Unternehmen besteht ein Cyber Sicherheit Schwerpunkt mit einem Fokus zur Bewusstseinsbildung für Vorsorgebedarf und Risikoprävention, welcher vom BMWFW koordiniert wird. Zur Optimierung der Kommunikation unter den Cyber Sicherheit Stakeholdern in Österreich wurde außerdem eine eigene Cyber Sicherheit Kommunikationsstrategie erarbeitet.

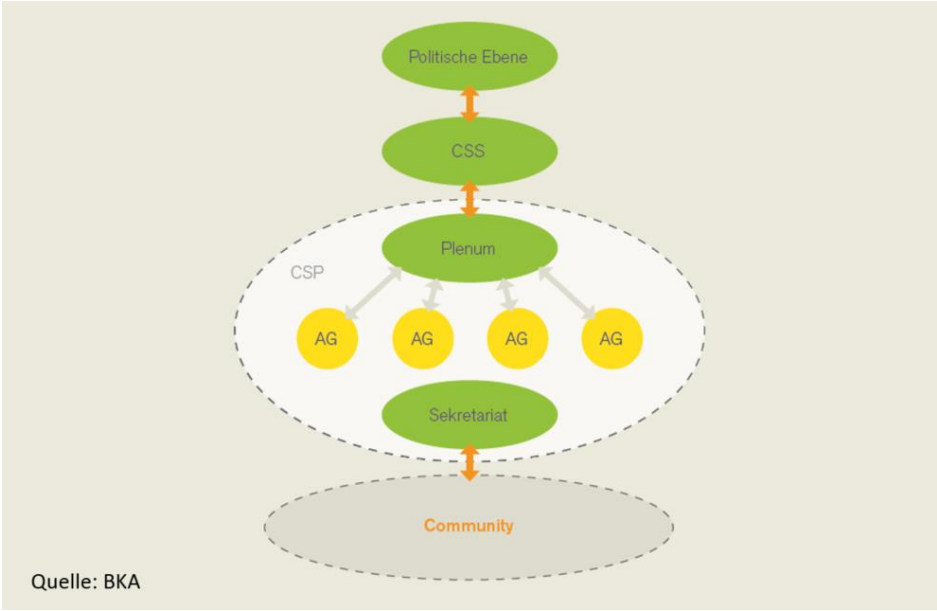


Abbildung 14: Aufbauorganisation der Cyber Security Plattform (CSP)

Handlungsfeld 4: Schutz kritischer Infrastrukturen

Die Bundesregierung hat am 4. November 2014 das Österreichische Programm zum Schutz kritischer Infrastrukturen (APCIP) beschlossen. Der Schwerpunkt der Umsetzung dieses Programms liegt im Aufbau von Sicherheitspartnerschaften mit strategischen Unternehmen, die kritische Infrastrukturen betreiben. Ein Konzept zu Cyber Sicherheits- und branchenbezogener Standards wird einerseits durch das KIRAS Projekt „Secure eGov" und andererseits durch eine Arbeitsgruppe der Cyber Sicherheit Plattform vorbereitet.

Handlungsfeld 5: Sensibilisierung und Ausbildung

Das IKT-Sicherheitsportal, erreichbar unter www.onlinesicherheit.gv.at, ist eine interministerielle Initiative in Kooperation mit der österreichischen Wirtschaft und fungiert seit Februar 2013 als zentrales Internetportal für Themen rund um die Sicherheit in der digitalen Welt. Die IT-Strategie „efit21 – digitale Bildung" des BMBF verfolgt das Ziel der Vermittlung digitaler Kompetenzen an Schülerinnen und Schüler sowie an Lehrende, die Universitäten werden vom BMWFW für die inhaltlichen Ziele der Strategie für Cyber Sicherheit sensibilisiert. Aktuelle Warnmeldungen aufgrund neuer Erkenntnisse werden von der Cyber Crime Competence Center (C4) Meldestelle an Medien weitergeleitet.

Im Rahmen dieses Handlungsfelds wurden auch einige Projekte umgesetzt, wie zum Beispiel das C4 Präventionsprojekt „Cyber.Kids", das Kinder und Jugendliche im Alter von 8 bis 12 Jahren im Umgang mit dem Cyberspace sensibilisiert und schult. Einen wichtigen Beitrag zur Cyber Prävention liefert auch das Projekt „Click & Check", in welchem in Schulen Jugendliche ab 14 Jahren über die Gefahren von Internet und Cyber Crime durch speziell ausgebildete Präventionsbeamte informiert werden. Im Bereich des BM.I/C4 wurde außerdem die Ausbildung von Forensikern und Ermittlern für die Bekämpfung von Cyber Crime weiter intensiviert. Durch die Wehrdienstreform wurde innerhalb des BMLVS mit Anfang 2014 außerdem das Wahlmodul „Cyber Sicherheit" für Präsenzdiener geschaffen.

Handlungsfeld 6: Forschung und Entwicklung

In der Forschung bildet das Thema Cyber Sicherheit auf nationaler Ebene im Sicherheitsforschungsprogramm KIRAS als auch auf europäischer Ebene in Horizont 2020 einen wichtigen Forschungsschwerpunkt. KIRAS, das Österreichische Förderprogramm für Sicherheitsforschung, unterstützt nationale Forschungsvorhaben, deren Ergebnisse dazu beitragen, die Sicherheit – als dauerhafte Gewährleistung eines hohen Niveaus an Lebensgrundlagen und Entfaltungsmöglichkeiten – für alle Mitglieder der Gesellschaft zu erhöhen.

Handlungsfeld 7: Internationale Zusammenarbeit

Fragen der Cyber Sicherheit werden im Rahmen von EU, Vereinten Nationen, OSZE, NATO, OECD und Europarat sowie in multilateralen Foren (Global Conference on Cyberspace, Central European Cyber Security Platform, Freedom Online Coalition) unter aktiver Beteiligung von Österreich verstärkt thematisiert. Die Koordination der relevanten außenpolitischen Maßnahmen erfolgt dabei über das BMEIA.

Wichtige **internationale Themen** mit intensiver Beteiligung Österreichs sind unter anderem:

- Das Einsetzen für Grund- und Menschenrechte im Internet, sowie für ein freies Internet.
- Die Strategie für einen digitalen Binnenmarkt für Europa.
- Die „EU Cyber Sicherheitsstrategie" mit der angeschlossenen „Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit" (NIS).
- Das „EU Cyber Defence Policy Framework".
- Die Schlussfolgerungen zur Cyber Diplomatie.
- Aktivitäten der „European Network and Information Security Agency" (ENISA).
- Regelmäßige bilaterale Konsultationen mit der NATO.
- Die bilateralen Konsultationen mit der „Cooperative Cyber Defence Center of Excellence (CCDCoE)" in Tallinn/Estland.
- Die Mitarbeit an vertrauensbildenden Maßnahmen im Rahmen der OSZE.

Weitere Informationen:

- Bericht Cyber Sicherheit 2015 (PDF Download)[43]
- Download der Österreichischen Strategie für Cyber Sicherheit (ÖSCS).[44]
- Mehr über die ÖSCS auf der Website des Bundeskanzleramts unter: https://www.bka.gv.at/site/7863/default.aspx

[43] Quelle: https://www.bka.gv.at/DocView.axd?CobId=58898
[44] Quelle: https://www.bka.gv.at/DocView.axd?CobId=50748

8. AUSBLICK: RICHTLINIE FÜR NETZWERK- UND INFORMATIONSSICHERHEIT UND CYBER SICHERHEITSGESETZ

Am 7. Februar 2013 veröffentlichte die Europäische Kommission eine gemeinsame Mitteilung der Kommission und der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik zur **„Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum",** sowie begleitend dazu den Vorschlag für eine **Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit (NIS-RL)** in der Union. Ziel der NIS-RL ist es, EU-weit eine hohe Sicherheit der Netzwerk- und Informationssysteme zu erreichen. Vor diesem Hintergrund soll die Zusammenarbeit zwischen den Mitgliedstaaten in strategischer und operationeller Hinsicht gestärkt sowie bestimmte, wichtige (private und öffentliche) Anbieter zu angemessenen Sicherheitsmaßnahmen und zur Meldung gröberer Störfälle verpflichtet werden. Die inhaltlichen Verhandlungen konnten Ende 2015 abgeschlossen und ein gemeinsamer Kompromisstext gefunden werden. Es ist mit einer Annahme der NIS-RL im Februar/März 2016 zu rechnen. Ab Inkrafttreten haben die Mitgliedstaaten dann 21 Monate Zeit, die NIS-RL in nationales Recht umzusetzen.

Ein Cyber Sicherheitsgesetz für Österreich

Das Cyber Sicherheitsgesetz soll künftig die Österreichische Strategie für Cyber Sicherheit (ÖSCS) mit der NIS-RL zusammenführen und im Zuge dessen den Rahmen der nationalen und zwischenstaatlichen Zusammenarbeit definieren.

In Österreich wurde zur Vorbereitung dazu bereits im Juni 2013 – kurz nach Veröffentlichung des ersten Vorschlags der NIS-Richtlinie der EU-Kommission – die Arbeitsgruppe Ordnungspolitischer Rahmen eingesetzt. Diese hat den Auftrag, den bestehenden Rechtsrahmen in Österreich zu erfassen und mit den kommenden Anforderungen in Verbindung mit der Richtlinie abzugleichen. Ferner hat das Kuratorium „Sicheres Österreich" (KSÖ) gemeinsam mit dem Bundesministerium für Inneres und dem Bundeskanzleramt Rechts- und Technologiedialoge zu diesem Thema abgehalten, mit dem Ziel einer Diskussion mit allen Stakeholdern zur Erarbeitung von Leitthemen für das geplante österreichische Cyber Sicherheitsgesetz.

Hauptpfeiler des österreichischen Cyber Sicherheitsgesetzes wird die vom BKA verhandelte NIS-RL sein, angereichert um Elemente aus den Handlungsfeldern im Rahmen der Umsetzung der Österreichischen Strategie für Cyber Sicherheit, den Endbericht der Arbeitsgruppe Ordnungspolitischer Rahmen sowie dem Endbericht des KSÖ ebenso wie Ergebnisse aus verschiedenen Arbeitstreffen mit VertreterInnen aus Wirtschaft und Wissenschaft. Zur Ausarbeitung des Cyber Sicherheitsgesetzes wird eine interministerielle, legistische Arbeitsgruppe unter Vorsitzführung des BKA eingerichtet.

Inhalte der Richtlinie für Netzwerk- und Informationssicherheit

Mit der NIS-Richtlinie soll einerseits EU-weit eine hohe Sicherheit der Netzwerk- und Informationssysteme erreicht sowie die Zusammenarbeit zwischen den Mitgliedstaaten verbessert werden, andererseits sollen bestimmte Anbieter kritischer Infrastrukturen zu angemessenen Sicherheitsmaßnahmen und zur Meldung von Störfällen verpflichtet werden.

Des Weiteren verpflichten sich die Mitgliedstaaten zur Erarbeitung einer nationalen NIS-Strategie, die strategische Ziele, Prioritäten und Maßnahmen enthält, um ein hohes Sicherheitslevel der Netzwerk- und Informationssysteme zu erreichen. Jeder Mitgliedstaat hat im Zuge dessen auf nationaler Ebene auch mindestens ein Computer Security Incident Response Team (CSIRT), ein oder mehrere NIS-Behörden, sowie einen Single Point of Contact (SPOC) einzurichten. Auf EU-Ebene werden außerdem eine Kooperationsgruppe sowie ein CSIRT-Netzwerk eingerichtet.

Die Aufgabe der Computer Security Incident Response Teams besteht vorwiegend darin, auf akute Sicherheitsbedrohungen zu reagieren, Warnungen und Informationen an betroffene Personenkreise auszugeben, Bewusstsein für IKT-Sicherheit zu schaffen und als Kontaktpunkt für sicherheitsrelevante IKT-Ereignisse aufzutreten. In Österreich betreibt das Bundeskanzleramt seit 2008 das GovCERT Austria in Kooperation mit nic.at für den öffentlichen, sowie CERT.at für den privaten Sektor. Daneben etablieren sich weitere Branchen-CERTs, wie z.B. das Austrian Energy CERT für den Energiesektor. Im österreichischen Cyber Sicherheitsgesetz soll etwa vorgesehen werden, dass Meldungen aufgrund der NIS-RL an das jeweils zuständige CERT im Sektor zu richten sind.

Österreich bei Netzwerk- und Informationssicherheit führend

Durch die hierzulande bereits seit etlichen Jahren erfolgreich umgesetzte und laufend verbesserte Zusammenarbeit im Cyber Sicherheitsbereich ist Österreich im Hinblick auf die Implementierung der NIS-Richtlinie bereits jetzt bestmöglich aufgestellt und gilt als europaweites Best-practice Beispiel in diesem Bereich. Der Ausbau weiterer Branchen-CERTs (wie dem zuvor genannten Austrian Energy CERT für den Energiesektor) sowie bereits seit mehreren Jahren erfolgreich bestehende sektorübergreifende Kooperationen wie etwa der Austrian Trust Circles (ATC) bestätigen dies.

Bei den Austrian Trust Circles handelt es sich um Cyber Security Information Exchanges in verschiedenen Sektoren der strategischen Infrastruktur. Dies erlaubt den praxisnahen Austausch führender VertreterInnen kritischer Infrastrukturen (z.B. Banken, Energie- oder Telekommunikationsbetreiber) zu aktuellen Sicherheitsthemen – und gilt dadurch auch international als angesehenes Musterbeispiel für mehr Informationsaustausch im Bereich Cyber Sicherheit.

Seine hohe Umsetzungs- und Lösungskompetenz im Fall von Cyber Sicherheitsvorfällen demonstriert Österreich außerdem regelmäßig im Rahmen von nationalen wie auch internationalen Übungen. Bei diesen werden verschiedene Ernstfälle bzw. Szenarien simuliert und vor allem die länder- und sektorenübergreifende Zusammenarbeit trainiert – wie etwa anlässlich einer von der Europäischen Verteidigungsagentur (EVA) organisierten Cyber Übung, die 2015 unter österreichischer Anleitung stattfand. Die Schwerpunkte lagen im Übungsbereich dabei verstärkt auf technischer, operationeller sowie strategisch-politischer Ebene.

Breiter Dialog zur Klärung der offenen Fragen

In Bezug auf das geplante Cyber Sicherheitsgesetz sind derzeit noch viele Fragen offen, die im Laufe der kommenden Wochen und Monate im Rahmen eines intensiven Dialogs aller betroffenen Stakeholder unter Koordination des Bundeskanzleramts geklärt werden sollen. Dies gilt insbesondere im Hinblick auf die geplanten Meldepflichten und den zugrunde liegenden Diensten bzw. Betreibern. Die Beschlussfassung des Gesetzes wird noch im Laufe der aktuellen Legislaturperiode angepeilt. Nachdem die NIS-Richtlinie viele unterschiedliche Bereiche und Materiengesetze berührt, haben ein gut funktionierender Koordinationsmechanismus und ein intensiver Dialog mit den Stakeholdern im Cyber Sicherheitsbereich im Rahmen der Erarbeitung des Gesetzes jedenfalls höchste Priorität.

9. AUSBLICK: CYBER SICHERHEITS TRENDS UND GEFAHREN VON MORGEN

Computer, Smartphone oder Tablet sind Begleiter in jedem Aspekt unseres Lebens. In Zukunft wird sich dies durch vernetzte Heimgeräte, Autos oder Wearables erweitern. Solche werden, ebenso wie das Smartphone heute, künftig allgegenwärtig sein. Bewegten sich früher Rechner von Unternehmen nur innerhalb des Unternehmensnetzwerks, so finden sie heute den Weg zur jederzeitigen Datenverfügbarkeit in die Cloud. McAfee rechnet bis 2020 mit mindestens 200 Milliarden vernetzten Geräten rund um den Globus. Die Folge daraus werden noch mehr BenutzerInnen, mehr Daten und mehr Netzverkehr sein.

Bedeutung und Menge von Daten nehmen zu

Im Informationszeitalter nehmen Daten fast schon eine rohstoffähnliche Bedeutung ein. Waren die riesigen Datenmengen – Big Data – bisher noch zu komplex und zu groß, um sie entsprechend auswerten zu können, wird künftig die Nachfrage nach Echtzeitverarbeitung steigen. Dies kann wiederum für Softwareunternehmen interessant werden, die sich auf diese Auswertungen und Visualisierungen spezialisieren. Hinzu kommen vermehrt wirtschaftliche Überlegungen von Unternehmen, aus den Daten per se Wertschöpfung generieren zu können – sei es durch Kauf, Verkauf oder dem Hinzufügen eines Added-Value. Dies setzt jedoch auch voraus, dass sich die Daten entsprechend verarbeiten lassen können. Ein Trend, den auch IBM in den nächsten Jahren sieht.[45]

Nicht nur die Menge der Daten wird zunehmen, auch das Speicherverhalten wird sich weiterentwickeln. Die Cloud als Speicherform oder „Arbeitsplatz der Zukunft" etabliert sich nach und nach. Die letzte statistische Erhebung von Eurostat im Jahr 2014 ergab, dass 19% der Unternehmen in der EU Cloud Dienste nutzen. In Österreich nutzen dies nur 12%, während Unternehmen aus Finnland mit 51% die Spitzenreiter in Europa sind.[46]

Auch PrivatanwenderInnen bedienen sich immer größerer Datenmengen, um ihr Verhalten im täglichen Leben zu überprüfen. Angefangen von den gelaufenen Kilometern beim Sport, über das Einkaufsverhalten, bis zum eigenen Schlaf- und Essverhalten, werden Daten in Zukunft eine größere Rolle spielen und in größerer Menge gespeichert werden. Sie gewinnen daher auch in der Gesellschaft an Bedeutung, da sich Daten nach und nach auch in der breiten Öffentlichkeit etablieren werden.

[45] Quelle: http://www.ibmbigdatahub.com/blog/big-data-trends-top-eight-analytics-lessons-business
[46] Quelle: http://ec.europa.eu/eurostat/documents/2995521/6208102/4-09122014-AP-DE.pdf/4a3fdeb8-d389-41a2-92cc-db541a45646e

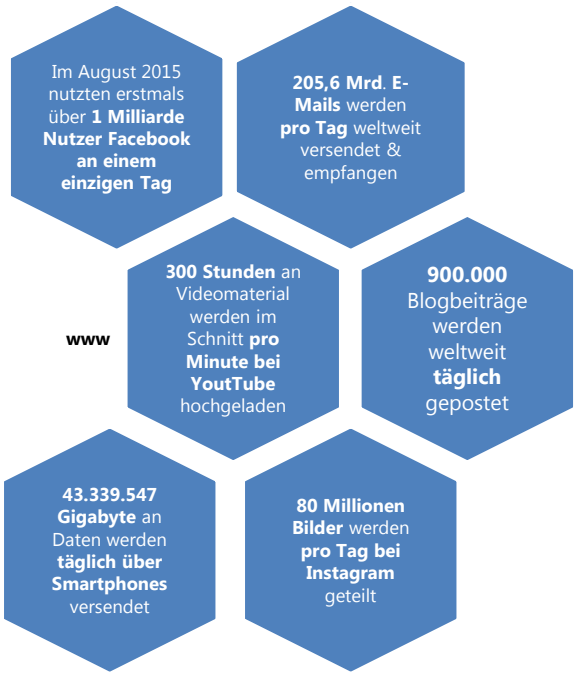


Abbildung 15: Daten und Fakten zur durchschnittlichen weltweiten Internetnutzung pro Tag im Jahr 2015; Quellen: de.statista.com[47, 48], sociallystacked.com[49], www.internetworld.de[50], instagram.com[51]

Mobilität als Treiber unserer Flexibilisierung

Nichts unterstützt uns in Richtung steigender Flexibilität mehr als die zunehmende Mobilität. Vor allem spielt es eine Rolle, Informationen auf jedem Gerät auch adäquat anzeigen lassen zu können. So verwenden laut einer Gartner Umfrage[52] beispielsweise 85% der Befragten aus den USA und 77% der Befragten aus dem Rest der Welt mehrere Geräte gleichzeitig. Der Bedarf mit jedem Gerät zu seinen Daten – und das in einer brauchbaren und in bearbeitbarer Form – zugreifen zu können, steigt.

Social Engineering ist im Kommen

Das aufkommende Social Engineering könnte auch in Zukunft eine wachsende Bedrohung darstellen. Durch die zunehmende Bedeutung von Daten wird auch deren technischer Schutz vermehrte Aufmerksamkeit geschenkt werden. Der Mensch wird immer öfter zur größten Schwachstelle im System, die als Ziel für Social Engineering Attacken dient. Dazu gehören Angriffsversuche via Telefon, Messaging, E-Mail und über Social Media.

---

[47] Quelle: http://de.statista.com/statistik/daten/studie/252278/umfrage/prognose-zur-zahl-der-taeglich-versendeter-e-mails-weltweit/

[48] Quelle: http://de.statista.com/statistik/daten/studie/207321/umfrage/upload-von-videomaterial-bei-youtube-pro-minute-zeitreihe/http:/de.statista.com/statistik/daten/studie/207321/umfrage/upload-von-videomaterial-bei-youtube-pro-minute-zeitreihe/

[49] Quelle: http://www.sociallystacked.com/2015/02/day-internet-numbers-will-blow-mind-infographic/

[50] Quelle: http://www.internetworld.de/social-media/facebook/facebook-milliarde-nutzer-am-tag-1005674.html

[51] Quelle: http://blog.instagram.com/post/129662501137/150922-400million

[52] Quelle: http://www.computerwelt.at/news/software/bi/detail/artikel/113867-2016-was-kommt-als-naechstes/

Womit in Zukunft zu rechnen sein wird:

- Mehr Daten, mehr Analysen und mehr Geräte verstärken die Sicherheitskomplexität – eine weitere, große Herausforderung für die Zukunft.
- Bei diesen Aussichten müssen sich Unternehmen, PrivatanwenderInnen und IT-Unternehmen die Frage stellen, wie bei der Menge an Daten speziell mit den privaten Daten bzw. sensiblen Daten umgegangen werden soll.
- Die Frage nach der Speicherung ist eine sehr wichtige. Viele Daten der NutzerInnen erzählen sehr viel über den Menschen hinter diesen Daten. Die Nützlichkeit dieser Daten wird sich daher künftig weiter erhöhen, diese sind daher anfällig für Cyber Attacken.
- Die Hacker Szene unterliegt einem kontinuierlichen Trend der Professionalisierung[53], der sich 2016 weiter fortsetzen wird.
- Im Bereich der Datenspeicherung sind in den nächsten Jahren hohe Investitionen zu erwarten. Es entwickelt sich dabei ein Geschäftsfeld, das sich somit zu vergrößern beginnen wird und neuen Geschäftsmodellen Raum bieten kann, beispielsweise in der Frage, wie man zu den generierten Daten einen Mehrwert hinzufügen kann.
- Neben der Speicherinfrastruktur wird bei zunehmender Datenmenge auch die Bandbreite für die zu übertragenden Daten in den nächsten Jahren herausgefordert werden. Durch das "Internet of Things" (IoT), Cloud Dienste und zunehmende Mobilität wird das Muster der Datenübertragung vor Herausforderungen gestellt. Gerade auch in Österreich mit den vielen ländlichen Regionen ist hier u.a. der Breitbandausbau Grundlage für wirtschaftliche Weiterentwicklung.
- Die Vernetzung wird immer engmaschiger und straffer angezogen. Unser Leben und die Geschäftstätigkeit vieler Firmen basieren in steigendem Maße auf dem Funktionieren und der Erreichbarkeit einer Vielfalt an IT Services.

Obwohl uns die Aussichten auf die Zukunft eine Bandbreite an neuen Möglichkeiten aufzeigt, muss vor allem der schmale Grat zwischen der Nutzbarkeit und der Sicherheit von Daten im Auge behalten werden. Es muss davon ausgegangen werden, dass nicht nur die Verwendung der Daten, sondern auch die Versuche, durch Cyber Angriffe an diese Daten heran zu kommen, zunehmen werden.

Neben dem Datenverlust ist hier die Verfügbarkeit aller Dienstleistungen, auf denen die moderne Gesellschaft basiert, ein zentraler Punkt.

In diesen Zusammenhang ist es von hoher Bedeutung, sich bereits präventiv in Form einer Sicherheitsinfrastruktur, die die Basisanforderungen erfüllt, auf diese neuen Herausforderungen vorzubereiten.

[53] Quelle: http://www.computerwoche.de/a/im-untergrund-blueht-ein-reifes-crimeware-oekosystem,3220427

10. SERVICE: TIPPS UND TRICKS FÜR DEN SICHEREN UMGANG IM NETZ

Von entscheidender Wichtigkeit bei der Nutzung des Internet ist der Schutz vor Angriffen und Bedrohungen. Dabei kann für jede/n einzelne/n InternetnutzerIn bereits ein Mindestmaß an Vorsichtsmaßnahmen, wie die Installation eines Anti-Viren Programmes, den Schutz vor Angriffen bereits um ein Vielfaches steigern. „Vorsicht ist besser als Nachsicht" gilt daher vor allem in der Online Welt – jetzt und auch in Zukunft.

Gestohlene Daten und angegriffene Rechner können bei Unternehmen und Privaten Schaden anrichten. Ein Bewusstsein für den Schutz seines eigenen Systems ist daher von hoher Bedeutung. Damit wird der Gefahr etwaiger Attacken wie Phishing, Clickjacking, Malware, Angriffen auf die Webcam, Infektionen und Überlastungsangriffen, vorgebeugt. Auch wenn ein hundertprozentiger Schutz nie gewährleistet werden kann, kann ein hoher zeitlicher und finanzieller Aufwand eingespart werden, indem man präventiv auf einfach umzusetzende Maßnahmen setzt.

Augen auf bei E-Mails

Spam E-Mails gehören mittlerweile zum täglichen Inhalt des Posteingangs. Als Schutz sollte in jedem Fall auf Spamfilter vom Provider und Spamfilter auf dem Computer (bei Verwendung von E-Mail Programmen wie Outlook) gesetzt werden. Dasselbe gilt für Phishing-E-Mails, die oft durch Tippfehler oder seltsamen Absenderadressen gekennzeichnet sind. Viele User sind mit angeblichen E-Mails von ihrer Bank konfrontiert. Man sollte jedoch beachten, dass Banken niemals Daten via E-Mail erfragen oder gar darum ersuchen, diese via E-Mail zu bestätigen. E-Mail Absender können trivial gefälscht werden. Es empfiehlt sich daher im Zweifelsfall den vermeintlichen Sender anzurufen und die tatsächliche Sendung der empfangenen E-Mail auf diese Weise zu bestätigen.

Schutz in sozialen Netzwerken

Soziale Netzwerke bieten heute einen einfachen Weg, um mit FreundInnen und Bekannten in Kontakt zu bleiben. Da man sich ausschließlich in der Umgebung seiner FreundInnen sicher wähnt, liegt auch die Hemmschwelle in puncto Sicherheit tiefer. Wichtig ist jedoch, nicht unüberlegt auf verdächtig verlockende Links zu klicken, auch wenn die Nachricht von einem/r FreundIn kommt. So sind Profile auf sozialen Medien häufig angegriffene Ziele für Hacker.

Sollte man jedoch einmal zu unachtsam, beispielsweise auf Facebook, sein und dadurch einen Wurm eingefangen haben, sollte man alle Meldungen auf der Pinnwand, die der Wurm erstellt hat, löschen. Genauso sollte man bei den sogenannten Fan-Seiten darauf achten, dass diese keine Fälschungen sind. Darüber hinaus empfiehlt es sich, auf Facebook Superlativen wie "OMG", "Unglaublich", "Spektakulär" o.ä. zu ignorieren. Als Grundvoraussetzung sollte beim Profil generell die Angabe persönlicher Daten auf ein Minimum reduziert werden. Verdächtiges ist bei sozialen Medien darüber hinaus auch dem Betreiber zu melden.

Beim Teilen heikler Daten in sozialen Netzen sollte man zwei Punkte im Auge behalten: Wie sicher kann man sich sein, dass der Empfänger seinen Computers genauso sorgsam schützt wie man selber? Und: Wer heute mein „Freund" auf Facebook ist, muss das nicht notwendigerweise morgen auch noch sein.

Mobiler Schutz wird immer wichtiger

Noch hinkt der Einsatz von Anti-Viren Programmen auf mobilen Geräten deren verbreiteter Nutzung hinterher. Und das, obwohl die Menge an Schadsoftware laufend zunimmt und der Schutz der eigenen Privatsphäre nicht zu vernachlässigen ist – beispielsweise durch PIN-Abfragen und Displaysperren. Datenverbindungen wie Bluetooth oder WLAN sollten idealerweise deaktiviert bleiben, wenn man diese gerade nicht nützt. Auch bietet ein öffentliches WLAN eine Plattform, auf der sich Angreifer Zugang zu Smartphones oder anderen Geräten verschaffen können. Aus diesem Grund sollte man bei der Nutzung eines öffentlichen WLANs entsprechende Vorsichtsmaßnahmen treffen, wie etwa VPNs verwenden und Datei- und Verzeichnisfreigaben deaktivieren.

Updates

Unabhängig ob Anwendungsprogramme, Internetbrowser oder Betriebssysteme, oder wie neu der Rechner, das Smartphone oder das Tablet ist, eine Lücke kann durch eine veraltete Software schnell bei jedem Gerät zu Problemen führen. Sicherheitslücken in Software können durch stetige Aktualisierung und Updates so gering wie möglich gehalten werden. Die automatische Einstellung für Software Updates kann hier helfen, um diese auch wirklich regelmäßig durchzuführen. Vor allem sensible Anwendungen wie Java oder Flash Player sollten immer auf dem aktuellsten Stand gehalten werden – oder erst gar deinstalliert werden.

Schutzsoftware und Schutzanwendungen

Als Schutzanwendung ist in jedem Fall eine Personal Firewall – entweder durch ein eigenes Programm, Teil einer Security Software Suite oder eines Betriebssystems bereitgestellt – zu verwenden. Die Installation eines Anti-Viren Programms gehört zur Basisausstattung, ebenso wie regelmäßige Updates zu den wichtigsten „To Do's" zählen. Denn nur wenn Schutzsoftware auch auf dem neuesten Stand ist, kann sie den höchstmöglichen Schutz gewährleisten.

Zusätzlich sollten Programme zum Schutz vor Spyware oder Adware genutzt werden.
Auch das Anlegen von BenutzerInnenkonten mit eingeschränkten Berechtigungen für Kinder, die auf den Computer Zugriff haben, kann man verhindern, dass diese versehentlich unerwünschte Programme installieren.

Deinstallation von Software, die nicht gebraucht wird

Wird ein Programm nicht mehr benötigt, sollte es idealerweise deinstalliert werden. Somit kann das Programm auch keine Angriffsfläche mehr darstellen. Benötigt man beispielsweise Java nicht, sollte es vom Rechner (bzw. aus dem Browser) entfernt werden. Geht das nicht, so sollte man zumindest "click-to-run" aktivieren: Diese Funktionalität im Browser erschwert möglichen Exploit-Packs (Software zur einfachen Erstellung von Malware, was u.a. zu deren weiter Verbreitung führt) massiv die Arbeit.

Gute Passwörter nützen & schützen

Passwörter sind der Zugangspunkt für viele Online Anwendungen, wie soziale Netzwerke und Online Banking. Sie fungieren als Schlüssel und sollten wie der eigene Haustürschlüssel gehütet werden. Bei der Erstellung ist zu beachten, dass sie immer aus Buchstaben, Sonderzeichen und Zahlen zusammengesetzt sein sollten. Es ist essentiell, für alle wichtigen Anwendungen unterschiedliche Passwörter zu verwenden. Um die Verwaltung von Passwörtern komfortabler und sicherer zu gestalten, bietet sich die Verwendung von Passwortmanagern wie etwa KeePass an.

Online Einkaufen und Bezahlen

Immer mehr Menschen kaufen Online ein. Damit sind auch wesentliche Gefahren des Internets verbunden. Es sollte ausschließlich bei seriösen Anbietern aus dem Online Handel gekauft werden. Händlern, die etwa das Euro-Label Österreichisches E-Commerce-Gütezeichen[54] verwenden, kann diesbezüglich vertraut werden. Gütesiegel sind hier ein guter Richtwert bei etwaiger Unsicherheit. Am häufigsten wird Online mittels Kreditkarte bezahlt. Beim Bezahlen ist es unerlässlich darauf zu achten, dass eine verschlüsselte Verbindung (https://) vom Service Dienstleister aufgebaut wird. Dies gilt generell für alle Webseiten, über die sensible Daten (Username, Passwort) eingegeben werden.

Nur Vertrauenswürdiges aus dem App Store installieren

Infizierte Apps nehmen zu. Diese Art von Malware speichert Informationen über das BenutzerInnenverhalten. Mit den daraus generierten Daten versuchen Angreifer in der Folge Profit zu generieren oder nutzen sie selbst für weitere Angriffe. Apps sollten daher nur aus einem offiziellen App Store bezogen werden und der jeweilige App Entwickler auf seine Seriosität überprüft werden. Bei Gratis-Apps bzw. deren Zugriffsberechtigungen gilt es, sie generell zu hinterfragen.

Gesunder Menschenverstand/Awareness

Ein/e aufmerksame/r NutzerIn im Netz ist für Angreifer noch immer das größte Hindernis für eine erfolgreiche Attacke. Allerdings wird oft zu nachlässig gehandelt, wie das häufige Vorkommen von Social Engineering zeigt. Angreifer brauchen dabei keine technischen Programme, wenn sie ein Opfer zum Deaktivieren von Sicherheitsmechanismen oder zur

[54] Quelle: https://www.guetezeichen.at/

Installation von Schadsoftware überreden können. Ein aufmerksames Surfen im Web ist daher für jede/n NutzerIn ratsam.

Sicherheit in Unternehmen

Die IT-Sicherheit ist in Unternehmen ein sehr breit angelegtes Feld. So lassen sich für ein KMU nicht exakt die gleichen Handlungsempfehlungen geben, wie für einen großen Konzern. Während KMUs eher auf eine kleine IT-Abteilung oder eine/n IT-BetreuerIn setzen (können), gibt es für größere Unternehmen eine Vielzahl weitere zu beachtende Maßnahmen. Sie lösen IT-Sicherheitsfragen meist unter Zuhilfenahme professioneller Hilfe. Zu Standards, welche sinnvolle Maßnahmen für Unternehmen bereitstellen, gehört unter anderem das A-SIT Sicherheitshandbuch[55].

Weiterführende Informationen zum Thema Sicherheit unter:

- www.onlinesicherheit.gv.at
- Öffentliche Sicherheit, ein Magazin des Innenministeriums[56]
- Computer Emergency Response Team: www.cert.at
- help.gv.at - Internet und Handy – sicher durch die digitale Welt[57]

[55] Quelle: https://www.sicherheitshandbuch.gv.at/
[56] Quelle: http://www.bmi.gv.at/cms/bmi_oeffentlichesicherheit/
[57] Quelle: https://www.help.gv.at/Portal.Node/hlpd/public/content/172/Seite.1720000.html

11. ABOUT: CERT.AT UND GOVCERT AUSTRIA

CERT.at: Die österreichische Internet-Feuerwehr

CERT.at ist das österreichische Computer Emergency Response Team (CERT) und wurde 2008 gemeinsam mit GovCERT Austria vom Bundeskanzleramt in Kooperation mit nic.at eingerichtet. Die klassischen Aufgaben eines Computer Emergency Response Teams sind mit jenen einer Feuerwehr vergleichbar: Das CERT-Team wird in erster Linie bei akuten Sicherheitsbedrohungen und Ereignissen aktiv. Dies geschieht durch Verständigung von betroffenen Stellen oder auf Basis eigener Recherchen.

Darüber hinaus ist CERT.at jedoch auch für vorbeugende Maßnahmen, wie Früherkennung, Vorbereitung für Notfälle, Öffentlichkeitsarbeit und Beratung zuständig. CERT.at versteht sich auch als Kontaktpunkt für sicherheitsrelevante IKT-Ereignisse in Österreich und dient als vertrauenswürdige und anerkannte Informationsdrehscheibe. Zusätzlich – durch die internationale Vernetzung – ist CERT.at auch der „international sichtbare Partner" für ausländische CERTs. Das Team von CERT.at besteht derzeit aus über zehn Personen und wird von Robert Schischka geleitet.

Abbildung 16: Logo von CERT.at, dem Computer Emergency Response Team

CERT.at: Wie wir arbeiten

CERT.at sammelt Informationen zu Sicherheitsproblemen im österreichischen Internet, wie etwa infizierte Windows-PCs, manipulierte Webseiten oder fehlkonfigurierte Server. Dazu stützt sich CERT.at neben der eigens entwickelten Sensorik primär auf Quellen innerhalb der internationalen Gemeinschaft der IT-Sicherheitsbranche. Mit einer eigens entwickelten Sensorik überprüft CERT.at proaktiv das österreichische Internet auf potenzielle und tatsächliche Bedrohungen. Zusätzlich bearbeitet CERT.at akribisch alle eingehenden Meldungen über sicherheitsrelevante Vorkommnisse und entscheidet anlassbezogen über die weitere Vorgehensweise. Handelt es sich tatsächlich um Bedrohungen und ist ein akutes Eingreifen notwendig, so liegt die Hauptarbeit von CERT.at in weiterer Folge darin, die jeweiligen Internet Service Provider (ISPs) bzw. Domaineigentümer darüber zu informieren. Dabei werden Handlungsanleitungen bereitgestellt und Informationen geteilt, wie Bedrohungen am besten beseitigt werden können. CERT.at hat hierbei eine vorwiegend beratende und unterstützende Rolle, denn die tatsächliche Problembeseitigung kann letztlich nur durch die Betroffenen selbst erfolgen.

Weiters führt CERT.at tägliche Quellenbeobachtungen durch und fasst diese in einer Mailingliste zusammen. Auch werden auf www.cert.at Warnungen über IT-Sicherheitsprobleme veröffentlicht, um diese möglichst rasch der interessierten Öffentlichkeit zur Verfügung zu stellen.

Im Einsatz für mehr Internetsicherheit arbeitet CERT.at auch intensiv mit ausländischen CERTs zusammen und pflegt einen regen Informations- und Erfahrungsaustausch mit ExpertInnen aus aller Welt.

Der CERT-Beirat

In seiner strategischen Ausrichtung wird CERT.at durch einen eigenen CERT-Beirat unterstützt. Dieser bringt als beratendes Organ weitere Sichtweisen und Themenvorschläge ein. Die Mitglieder des Beirats repräsentieren dabei einen Querschnitt der Internet-Community in Österreich, fungieren als BotschafterInnen von CERT.at und unterstützen damit die Vernetzung des Themas Internetsicherheit in Gesellschaft und Politik.

Was CERT.at nicht ist

CERT.at ist keine Ermittlungsbehörde und befasst sich daher nicht mit dem Thema der Strafverfolgung im Internet. So hat CERT.at kein Durchgriffsrecht auf die Netzwerkinfrastruktur Österreichs und kann daher bei Sicherheitsvorfällen nur koordinierend und beratend aktiv werden.

Auch ist CERT.at keine isoliert arbeitende Einrichtung, sondern vielmehr eine koordinierende und informierende Stelle, die bei Angriffen auf Rechner sofort mit den jeweiligen Netzbetreibern und zuständigen Security Teams in Kontakt tritt. CERT.at verfügt über keine „Wunderwaffe“ gegen Sicherheitsprobleme. Die ExpertInnen von CERT.at sehen sich selbst als die „Österreichische Internet-Feuerwehr“, die im Falle des Falles Hilfe zur Verfügung stellt und in enger Abstimmung mit anderen Beteiligten den österreichischen Teil des Internets von Problemen befreit – auf Basis eines freiwilligen Angebots.

GovCERT Austria: Die SpezialistInnen im Behördenbereich

GovCERT Austria ist das Government Computer Emergency Response Team für die öffentliche Verwaltung und die kritische Informations-Infrastruktur (KII) in Österreich. Dabei dient GovCERT Austria auf nationaler Ebene als primäre Anlaufstelle für die einzelnen Stellen der öffentlichen Verwaltung und die Betreiber kritischer Infrastrukturen im Falle einer Cyber Attacke, sofern kein anderes CERT zuständig ist. Auf internationaler Ebene agiert GovCERT Austria als österreichische Kontaktstelle für ausländische Regierungen und internationale Organisationen bei Fragen der IKT-Sicherheit. Es tauscht Informationen und Warnungen mit diesen aus und leitet sie bei Bedarf an inländische InteressentInnen weiter. GovCERT Austria erfüllt dabei seine Arbeit und Aufgaben in enger Personalunion mit CERT.at.

Abbildung 17: Logo von GovCERT Austria, dem Computer Emergency Response Team für die öffentliche Verwaltung

Wichtige Player der Österreichischen Strategie für Cyber Sicherheit (ÖSCS)

Eine effektive Cyber Sicherheitsstrategie bedarf eines dichten und qualitativ hochwertigen Netzwerkes aller Cyber Sicherheits Stakeholder und Strukturen. Dazu gehört auch die Einrichtung eines starken und umfassenden Cyber Sicherheit Krisenmanagements. Im Rahmen der ÖSCS agieren CERT.at und GovCERT Austria als relevante sektorale Meldestellen, die bei Cyber Vorfällen gemeinsam mit weiteren Stellen des öffentlichen und privaten Bereiches aktiv werden. Sie sind die erste Anlaufstelle für Fragen zur Sicherheit im österreichischen Teil des Internets und richten sich dabei primär an Unternehmen, den öffentlichen Sektor, Banken, Institutionen des Gesundheitswesens und große Infrastrukturbetreiber (Telekom, Industrie, Transport), sofern diese über kein eigenes CERT verfügen (z.B. das Energy CERT für den Energiesektor).

CERT-Verbund für mehr Datensicherheit

Wir leben in einer Gesellschaft, die zunehmend von digital vernetzten Informations- und Kommunikationssystemen abhängig ist. Um diese, für das Funktionieren unserer Gesellschaft, essenziellen Systeme verstärkt zu schützen, wurde Ende 2011 auf Initiative des österreichischen GovCERT Austria und des BMLVS ein Österreichischer CERT-Verbund ins Leben gerufen. Im Mittelpunkt der Zusammenarbeit stehen der Schutz von IKT-Infrastrukturen, der Informationsaustausch und die rasche Reaktion auf Bedrohungen. Im Rahmen einer Kooperation arbeiten öffentliche Verwaltung und Privatwirtschaft eng zusammen, um eine ganzheitliche Sichtweise im Kampf gegen Cyber Bedrohungen zu entwickeln. Mitglieder des CERT-Verbunds sind neben GovCERT Austria/CERT.at unter anderem das ACOnet CERT, Raiffeisen-IT CERT, das Bundesrechenzentrum, WienCERT, das milCERT und andere. Durch die Zusammenarbeit soll nicht nur die Qualität der Services steigen, sondern auch ein für den möglichen Ernstfall relevanter Wissensvorsprung aufgebaut werden.

Weitere Informationen:

- Bundeskanzleramt Österreich – Cyber Sicherheit[58]
- Digitales Österreich: http://www.digitales.oesterreich.gv.at
- www.cert.at und www.govcert.gv.at

[58] Quelle: https://www.bka.gv.at/site/7863/default.aspx

12. ABKÜRZUNGSVERZEICHNIS

Abkürzung	Erklärung
AbwA	Abwehramt
ACOnet	Austrian Academic Computer Network (österreichisches Wissenschafts-, Forschungs- und Bildungsnetzwerk)
App	Application
A-SIT	Zentrum für Sichere Informationstechnologie
AD	Access Directory
ATC	Austrian Trust Circle
AV Programm	Anti-Viren Programm
APCIP	Austrian Program for Critical Infrastructure Protection (Österreichische Programm zum Schutz kritischer Infrastrukturen)
APT	Advanced Persistent Threat
BIP	Bruttoinlandsprodukt
BKA	Bundeskanzleramt
BM.I	Bundesministerium für Inneres
BMBF	Bundesministerium für Bildung und Frauen
BMEIA	Bundesministerium für Europa, Integration und Äußeres
BMF	Bundesministerium für Finanzen
BMLVS	Bundesministerium für Landesverteidigung und Sport
BMVIT	Bundesministerium für Verkehr, Innovation und Technologie
BMWFW	Bundesministerium für Wissenschaft, Forschung und Wirtschaft
BPD	Bundespressedienst
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVT	Bundesamt für Verfassungsschutz und Terrorismusbekämpfung
C4	Cyber Crime Competence Center
CCDCoE	Cooperative Cyber Defence Center of Excellence
CE.AT	Übung Cyber Europe Austria
CERT	Computer Emergency Response Team
CII	Critical Infrastructure Information
CKM	Cyber Krisenmanagement
CMS	Content Management System
CSA	Cyber Security Austria
CSC	Cyber Security Center
CSIRT	Computer Security Incident Response Team
CSIS	Center for Strategic and International Studies
CSP	Cyber Security Plattform
CSS	Cyber Sicherheit Steuerungsgruppe
CyCon	NATO Cooperative Cyber Defence Centre of Excellence
DD4BC	Eine Hackergruppe genannt: "DDoS for Bitcoins"
DDoS	Distributed Denial-of-Service Attack
DNS	Domain Name Service
DNSBL	DNS-based Blackhole List bzw. in Echtzeit abfragbare schwarze Listen
DoS	Denial-of-Service Attack
ENISA	Europäische Agentur für Netzwerksicherheit

Abkürzung	Erklärung
ESP	Elekronisches Stabilitätsprogramm
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EVA	Europäischen Verteidigungsagentur
FBI	Federal Bureau of Investigation
FIRST	Forum of Incident Response and Security Teams
GovCERT Austria	Computer Emergency Response Team für die öffentliche Verwaltung
GPS	Global Positioning System
HNaA	Heeresnachrichtenamt
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IT	Informationstechnik
IKT	Informations- und Kommunikationstechnologie
IoT	Internet of Things
IP	Internet Protocol
ISP	Internet Service Provider
ISO	International Organization for Standardization
ITU	International Telecommunication Union
KII	Kritische Informations-Infrastruktur
KIRAS	Österreichische Förderungsprogramm für Sicherheitsforschung
KMU	Klein- und Mittelunternehmen
KSÖ	Kuratorium Sicheres Österreich
LAN	Local Area Network
MD5	Message-Digest Algorithm 5
milCERT	militärisches Computer Emergency Response Team
NATO	North Atlantic Treaty Organization
NIS	Netzwerk- und Informationssicherheit
NIS-RL	Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Europäischen Union
NSA	National Security Agency
NTP	Network Time Protocol
OECD	Organisation for Economic Co-operation and Development
OpenSSL	Open Secure Sockets Layer
ÖSCS	Österreichische Strategie für Cyber Sicherheit
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
PC	Personal Computer
PKI	Public-Key-Infrastruktur
PIN	Persönliche Identifikationsnummer
POODLE	Padding Oracle On Downgraded Legacy Encryption
PUP	potenziell unterwünschte Programme
SHA	Secure Hash Algorithm
SIR	Security Intelligence Report, herausgegeben von Microsoft
SKKM	Staatliches Krisen- und Katastrophenschutzmanagement
SMTP	Simple Mail Transfer Protocol

Abkürzung	Erklärung
SNMP	Simple Network Management Protocol
SPOC	Single Point of Contact
SSDP	Simple Service Discovery Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
SSLv3	SSL-Protokoll Version 3
STS	Staatssekretär/in
TLS	Transport Layer Security
UDP	User Datagram Protocol
UNO	Vereinte Nationen (United Nations Organization)
URL	Uniform Resource Locator
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WPAD	Windows Proxy Auto-Detection

13. ABBILDUNGSVERZEICHNIS