GovCERT AUSTRIA

CERT.at

BERICHT INTERNET-SICHERHEIT ÖSTERREICH 2016

GESAMTAUSGABE

Wien, Jänner 2017

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. Sigrid Moser-Sailer, Mag. Markus Gruber, Mag. Patrick Radinger, Bakk.), Bundeskanzleramt (Mag. Heidi Havranek, LL.M., Mag. Gregor Schmied, DI Mag. Andreas Reichard, M.Phil.), CERT.at (Mag. Otmar Lendl, Mag. Christian Proschinger) **Herstellungsort**: Wien. Jänner 2017.

1. VORWORT: STAATSEKRETÄRIN MAG.A MUNA DUZDAR

© BKA

Mag.ª Muna Duzdar
Staatssekretärin für Diversität,
Öffentlichen Dienst und Digitalisierung im Bundeskanzleramt

Es vergeht kaum ein Tag, an dem wir in den Medien nicht mit Berichten über Cyber Angriffe, Datendiebstahl und Kriminalität im Netz konfrontiert sind, sowie mit Fragen, wie wir die Cyber Sicherheit in Österreich gewährleisten können. Als Staatssekretärin für Diversität, Öffentlichen Dienst und Digitalisierung bin ich einerseits für die Verwaltung und die E-Government-Services und auch für die Digitalisierung Österreichs im Allgemeinen verantwortlich. Insbesondere in meiner Rolle als Staatssekretärin für Digitalisierung ist es mir daher ein Anliegen, den Bereich der Cyber Sicherheit wesentlich mitzugestalten. Ich freue mich diese gesellschaftspolitischen Herausforderungen anzunehmen und ihre Bewältigung durch die Setzung konkreter Aktivitäten voranzutreiben.

Der vorliegende Internet-Sicherheitsbericht von CERT.at und GovCERT Austria gibt Ihnen einen Überblick über die in 2016 gesetzten Aktivitäten. Dabei wird beleuchtet, welchen Herausforderungen im Bereich der Cyber Sicherheit wir uns als Staat stellen und worauf sich Österreich in den kommenden Jahren vorbereiten muss, um diese bestmöglich zu bewältigen. Fest steht, das Thema der Digitalisierung betrifft nahezu alle Bereiche unseres Lebens. Digitalisierung ist nicht nur ein technisches und wirtschaftliches Phänomen, sondern auch ein politisches. Der Cyber Raum der Zukunft soll von Offenheit und Freiheit geprägt sein. Normen, Grundsätze und Werte, die wir in der realen Welt leben, müssen auch in der Online-Welt gelten. Dies betrifft vor allem unsere Grundrechte, wie Demokratie und Rechtsstaatlichkeit.

Wir wollen die Digitalisierung gestalten und dürfen davon nicht überrollt werden. Digitalisierung und Cyber Raum sollen sich zum Wohle der Menschen entwickeln und nicht als Bedrohung wahrgenommen werden. Um das zu gewährleisten, müssen wir massiv in unsere gemeinsame Cyber Sicherheit investieren. Diese den Bürgerinnen und Bürgern zu bieten ist ein gemeinsames Anliegen.

Eine wesentliche Maßnahme hierzu war die Verabschiedung der Österreichischen Strategie für Cyber Sicherheit (ÖSCS), die die Bundesregierung 2013 als umfassendes Konzept zum Schutz des Cyber Raums beschlossen hat. Die Gewährleistung von Cyber Sicherheit im nationalen und internationalen Cyber Raum ist darin eine der obersten Prioritäten Österreichs. Zur Bewältigung dieser Herausforderung wurden bereits mehrere Maßnahmen aus der ÖSCS umgesetzt. Dies wurde auch 2016 weiter vorangetrieben. So wurden vier Ziele der Cyber Sicherheit Plattform

(CSP) in Angriff genommen: Die Stärkung der Kommunikation und den Informationsaustausch mit allen Stakeholdern, die Nutzung bestehender Initiativen im Bereich Cyber Sicherheit, der Ausbau der Zusammenarbeit mit privaten Betreibern kritischer Infrastrukturen und weiteren Wirtschaftssektoren, die für die Cyber Sicherheit Österreichs von zentraler Bedeutung sind, sowie die Erhöhung der Kooperation mit Partnern in Richtung Sensibilisierung, Ausbildung, Forschung und Entwicklung. Österreich konnte sich weiters 2016 bei mehreren Cyber Übungen bewähren. Neben der internationalen NATO-Übung "Cyber Coalition" kann hier die vom Bundeskanzleramt organisierte Übung "Cyber Europe Austria 2016", der nationale Ableger der internationalen ENISA-Übung "Cyber Europe", hervorgehoben werden.

Das Jahr 2017 bringt viele wichtige Erneuerungen für Österreich, auch im Bereich Cyber Sicherheit. Mit dem erfolgreichen Abschluss der Verhandlungen einer Europäischen Richtlinie für Netz- und Informationssicherheit (NIS-Richtlinie) konnte 2016 ein wichtiger Grundstein zur Erhöhung der gemeinsamen, europäischen Cyber Sicherheit gesetzt werden, den es nun in ein nationales Gesetz für Cyber Sicherheit umzusetzen gilt. Diese wichtige Aufgabe findet derzeit unter Einbezug aller wichtigen Cyber Sicherheit Stakeholder aus dem öffentlichen wie auch den privaten Sektoren und unter der Koordination des Bundeskanzleramts, welches auch die Verhandlungen bei der Europäischen Union geführt hat, statt. Eines der wichtigsten Anliegen dieser Umsetzung ist eine verstärkte Zusammenarbeit der nationalen Stakeholder im Zuge der Aufgaben, welche an die Mitgliedsstaaten der EU durch diese Richtlinie herangetragen werden. In diesem Sinne kommt dem Bundeskanzleramt als künftige strategische NIS-Behörde die führende Rolle der strategischen Cyber Sicherheit Österreichs zu und damit die Aufgabe, gemeinsam neue Ansätze für die Zukunft zu finden und rechtzeitig die notwendigen Schritte dazu in die Wege zu leiten. Diese Rolle soll im künftigen Gesetz für Cyber Sicherheit institutionalisiert werden.

Cyber Sicherheit ist eine komplexe Angelegenheit, für die es nicht das eine Allheilmittel gibt. Bedrohungen aus dem Cyber Raum können nicht vollständig vermieden, das Risiko aber weitgehend auf ein Niveau reduziert werden, das es der Gesellschaft ermöglicht, weiterhin von den großen Chancen der digitalen Technologie zu profitieren. Viel wurde dazu in Österreich bereits erreicht. Wir werden auch weiterhin gemeinsam mit aller Kraft für Sicherheit im Cyber Raum arbeiten – denn Cyber Sicherheit ist eine gemeinsame Herausforderung für Staat, Wirtschaft und Gesellschaft gleichermaßen.

VORWORT: ING. ROLAND LEDINGER UND MAG. ROBERT SCHISCHKA

© HBF

Ing. Roland Ledinger
Leiter des Bereichs Digitales und E-Government des Bundes im Bundeskanzleramt

© CERT.at

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

Die Digitalisierung der Arbeitswelt verändert unser Berufsleben in einem Maße vergleichbar der industriellen Revolution. Digitalisierung dringt in nahezu alle Lebensbereiche vor: Wir alle können uns ein Leben ohne Informations- und Kommunikationstechnologie (IKT) kaum mehr vorstellen. Doch neben der Vielzahl an Erleichterungen und Vorteilen ist die zunehmende Digitalisierung eine immer größer werdende Sicherheitsgefahr für Privatpersonen als auch Unternehmen. Vor allem Unternehmen sind gefordert, sich noch stärker mit der Sicherheit ihrer IT-Systeme auseinanderzusetzen und eine Cyber Sicherheitsstrategie nicht nur zu entwickeln, sondern auch laufend den aktuellen Herausforderungen entsprechend anzupassen. Denn kein Tag vergeht, an dem Cyber Angriffe nicht Systeme lahmlegen, Sicherheitslücken Datendiebstahl ermöglichen und das Internet zum Eingangstor für diverse Angriffe aus dem Cyber Raum werden.

Im vergangenen Jahr standen vor allem Bedrohungen durch Ransomware und DoS/DDoS Angriffe ((Distributed) Denial of Service) im Fokus und die Anzahl dieser Angriffe steigt laufend. So verzeichnete das Bundeskriminalamt im Jahr 2016 über 10.000 angezeigte Angriffe auf Privatpersonen bzw. Unternehmen, was einem Plus von 11,6 Prozent zum Vorjahr entspricht. Angesichts dieser Zahlen ist davon auszugehen, dass Cyber Crime noch lange eine akute Bedrohung bleiben wird.

Jeder Betreiber von IT-Systemen, vom privaten Heim-PC bis hin zu großen Firmennetzen, sollte sich daher der Gefahr bewusst sein und rechtzeitig entsprechende Maßnahmen treffen. Bislang gibt es keine gesicherten Zahlen über die Gesamthöhe der von Ransomware und DoS/DDoS Angriffen verursachten Schäden bzw. die dadurch lukrierten „Profite" der Angreifer, aber alleine die Gruppe hinter der Ransomware „CryptoWall" erbeutete im Jahr 2015 beispielgebende 325 Mio. US-Dollar weltweit. Angesichts der kontinuierlichen Zunahme der Angriffsformen DoS/DDoS und Ransomware scheint es sich jedoch um ein lohnendes Geschäftsmodell zu handeln – zu Lasten der Betroffenen. Im Jahr 2016 waren erstmals verstärkt auch kleine und

mittelgroße Unternehmen in größerem Umfang Zielscheibe des CEO-Fraud, einem Betrugsversuch mit gefälschten Rechnungen.

Mit der ÖSCS hat die Bundesregierung ein umfassendes und proaktives Konzept zum Schutz des Cyber Raums mit klar geregelten Verantwortlichkeiten entwickelt. CERT.at und GovCERT Austria verstehen sich als aktive Player einer Sektor-übergreifenden Zusammenarbeit mit öffentlichen und privaten Kooperationspartnern. Darüber hinaus ist CERT.at Ansprechpartner bei Angriffen auf die Privatwirtschaft und treten als vertrauenswürdige und anerkannte Informationsdrehscheibe in der Österreichischen Cyber Sicherheit Landschaft auf.

Mit dem vorliegenden Internet-Sicherheitsbericht 2016 von CERT.at und GovCERT Austria machen wir auf die rasant an Bedeutung gewinnende Notwendigkeit von Cyber Sicherheit für unser Land aufmerksam. Aufgrund der Vielzahl an Bedrohungen ist uns ein konzertiertes Vorgehen in Österreich als auch auf EU-Ebene bzw. international besonders wichtig. Um diesen Schulterschluss auf europäischer Ebene zu erreichen, ist die im August 2016 in Kraft getretene Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-Richtlinie) ein großer Schritt in die richtige Richtung zur Abwehr von Cyber Bedrohungen und Hackerangriffen auf kritische Dienste. Die NIS-Richtlinie hat das Ziel, kritische Infrastruktur EU-weit besser gegen Störungen abzusichern. Wie alle Mitgliedstaaten hat Österreich 21 Monate Zeit, die NIS-Richtlinie in nationales Recht umzusetzen – etwa durch die Schaffung eines „Bundesgesetzes für Cybersicherheit" (Arbeitstitel), das bis Mai 2018 erlassen werden muss.

Sichere Netze und Informationssysteme sind die Voraussetzung für das Funktionieren des Binnenmarktes. Durch ein akkordiertes Vorgehen aller Mitgliedstaaten versucht die EU mögliche gravierende Störfälle zu vermeiden. Vor allem die Energiewirtschaft, Wasserversorgung, Logistik/Transport, Finanzwesen, Gesundheitswesen sowie der Informations- und Kommunikationsbereich gelten dabei als besonders relevant. Von der NIS-Richtlinie erfasst sind zudem ausgesuchte digitale Diensteanbieter (beispielsweise Anbieter von Online-Marktplätzen, Online-Suchmaschinen oder Cloud Diensten).

Dies macht deutlich, wie wichtig die Arbeit von CERT.at sowie GovCERT Austria und seinen ExpertInnen hinsichtlich Prävention und Beratung ist. Denn auch im kommenden Jahr werden wir wieder vor großen Herausforderungen stehen, um die Cyber Sicherheit unseres Landes weiterzuentwickeln.

2. DAS IT-SICHERHEITSJAHR 2016 AUS SICHT VON CERT.AT UND GOVCERT AUSTRIA

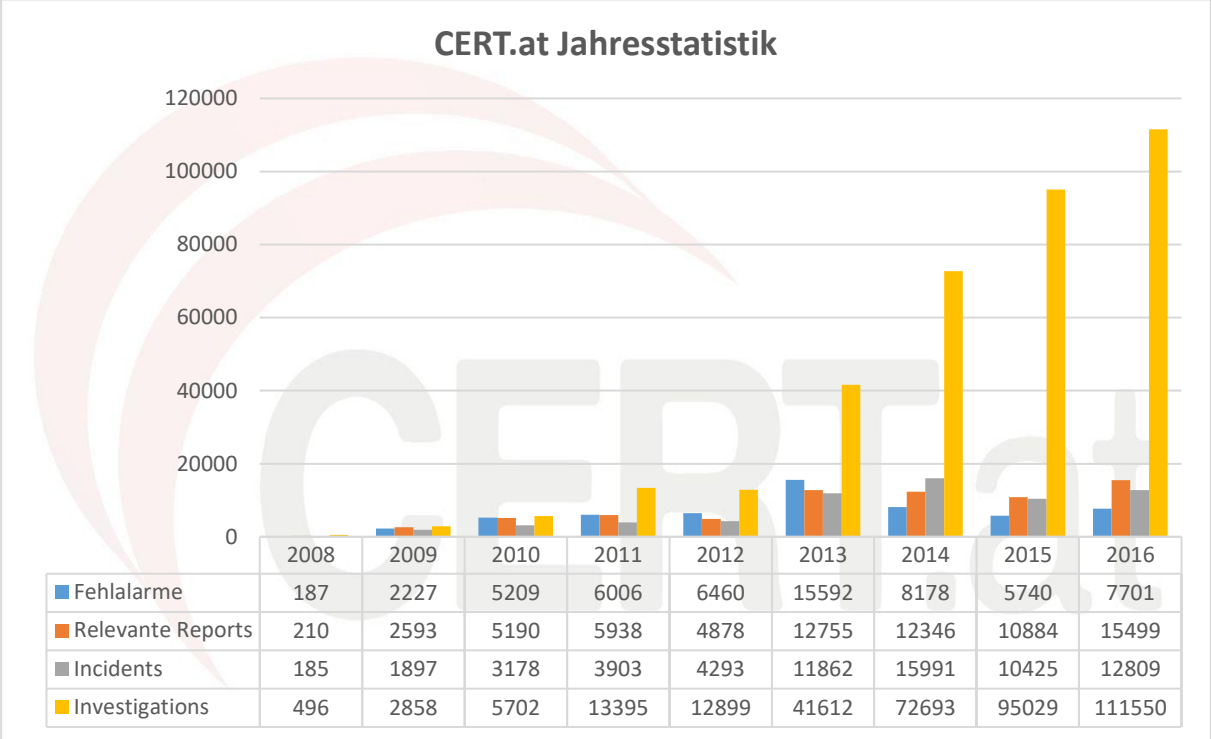
Die Computer Emergency Response Teams, kurz CERTs, sind nationale Ansprechpartner rund um das Thema IT-Sicherheit. Die österreichischen ExpertInnen von CERT.at leisten als Informationsdrehscheibe wichtige Präventions- und Aufklärungsarbeit rund um aktuelle sicherheitstechnische Themen. Dazu gehören Alarmmeldungen (Alerts), Warnungen und auch Empfehlungen – speziell für kleine und mittlere Unternehmen. Gleichzeitig leisten die ExpertInnen von CERT.at auch in akuten Fällen Hilfestellung bei IT-sicherheitstechnischen Angriffen im privatwirtschaftlichen Sektor. Zu den damit verbundenen Aufgaben gehören insbesondere die Koordination und das Informieren der Netzbetreiber (z.B. ISPs) sowie der zuständigen lokalen Security Teams.

CERT.at und GovCERT Austria führen im Zuge ihrer Arbeit umfangreiche Statistiken, die einen Überblick über die aktuelle Internet-Sicherheitslage Österreichs und die wichtigsten Daten des vergangenen Jahres ermöglichen. Auf diese wird in Folge eingegangen.

CERT.at Jahresstatistiken

Das Team von CERT.at führt seit dem Jahr 2008 Gesamt-Jahresstatistiken. Diese beinhalten die Zahl der relevanten Reports, Incidents und Investigations (nachfolgend eingehend erklärt) sowie auch Fehlalarme. Über den gesamten Zeitverlauf – von 2008 bis 2016 – zeigt die Grafik die Intensivierung der Arbeit von CERT.at zur kontinuierlichen Verbesserung der Cyber Sicherheit in Österreich.

Wie in der Abbildung 1 ersichtlich ist, nimmt die Zahl der Investigations durch CERT.at kontinuierlich seit Jahren zu. Im langfristigen Vergleich ist auch das Niveau bei den relevanten Reports und Incidents gestiegen. Im Vergleich zum Vorjahr nahmen sowohl die Reports, Incidents, Investigations als auch die Zahl der Fehlalarme zu.



	2008	2009	2010	2011	2012	2013	2014	2015	2016
Fehlalarme	187	2227	5209	6006	6460	15592	8178	5740	7701
Relevante Reports	210	2593	5190	5938	4878	12755	12346	10884	15499
Incidents	185	1897	3178	3903	4293	11862	15991	10425	12809
Investigations	496	2858	5702	13395	12899	41612	72693	95029	111550

Abbildung 1: CERT.at Jahresstatistik mit Übersicht über Reports, Incidents und Investigations im Zeitverlauf, Quelle: CERT.at

Die wichtigsten einzelnen Kennzahlen 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 (sog. Incident) eingestuft wird und eine aktive Behandlung erfordert. Typische Gründe für eine Beurteilung als irrelevanter Vorfall (Fehlalarm) sind etwa:

- Meldungen zu Problemen, die bereits bereinigt wurden
- Falschmeldungen von einfachen Suchalgorithmen
- mangelnde Zuständigkeit von CERT.at (z.B. die gemeldete IP-Adresse ist nicht in Österreich)
- generische Anfragen (etwa Konferenzeinladungen, Frage zu den Mailinglisten etc.)
- andere E-Mail-Irrläufer/Spam

Abbildung 2 zeigt die relevanten Reports, die im Jahr 2016 an CERT.at gesendet wurden. Die Anzahl der Reports wird pro Monat angegeben und ermöglicht dadurch einen guten Jahresvergleich in den 15 größten Kategorien. Im Schnitt waren es rund 1300 Meldungen pro Monat. Aus den Schwankungen zwischen den Monaten ist nicht viel herauszulesen, der Rückgang gegen Jahresende hängt mit einer Systemumstellung (siehe weiter unten) zusammen.

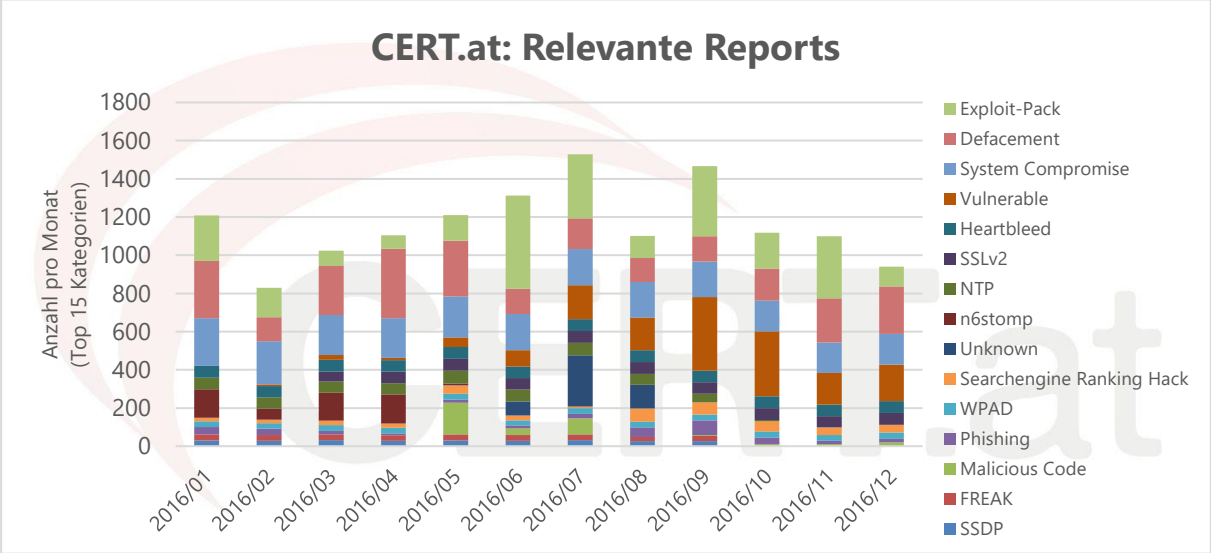


Abbildung 2: Klassifizierung der relevanten Reports nach Bedrohungsformen im Zeitverlauf, Quelle: CERT.at

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 in besonderen Fällen gegebenenfalls auch bei der Problemlösung.

Die Zahl der Incidents liegt immer sehr nahe an der Zahl der relevanten Reports, da nur selten zum gleichen Incident mehrere unabhängige Hinweise (Reports) einlangen.

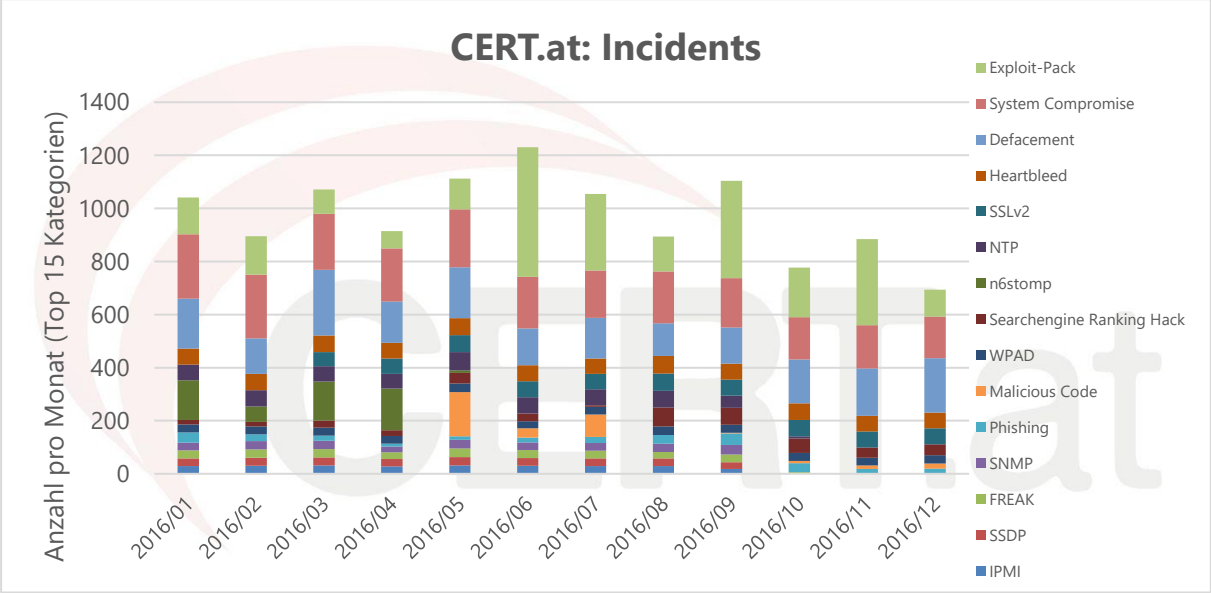


Abbildung 3: Klassifizierung von Incidents nach Bedrohungsformen im Zeitverlauf, Quelle: CERT.at

Die Kontaktaufnahme mit den betroffenen Unternehmen, Organisationen oder PrivatanwenderInnen wird im CERT.at Ticketsystem als „**Investigation**" bezeichnet.

Abbildung 4 zeigt die Zahl der Investigations im Jahr 2016. Eine Investigation ist üblicherweise eine E-Mail an den Netzbetreiber, Webhoster oder Domaininhaber. CERT.at verschickt also an einem typischen Arbeitstag rund 400 E-Mails. Da in vielen Incidents Daten zu mehreren Netzbetreibern enthalten sind, kommen auf einen Incident im Schnitt rund acht Investigations.

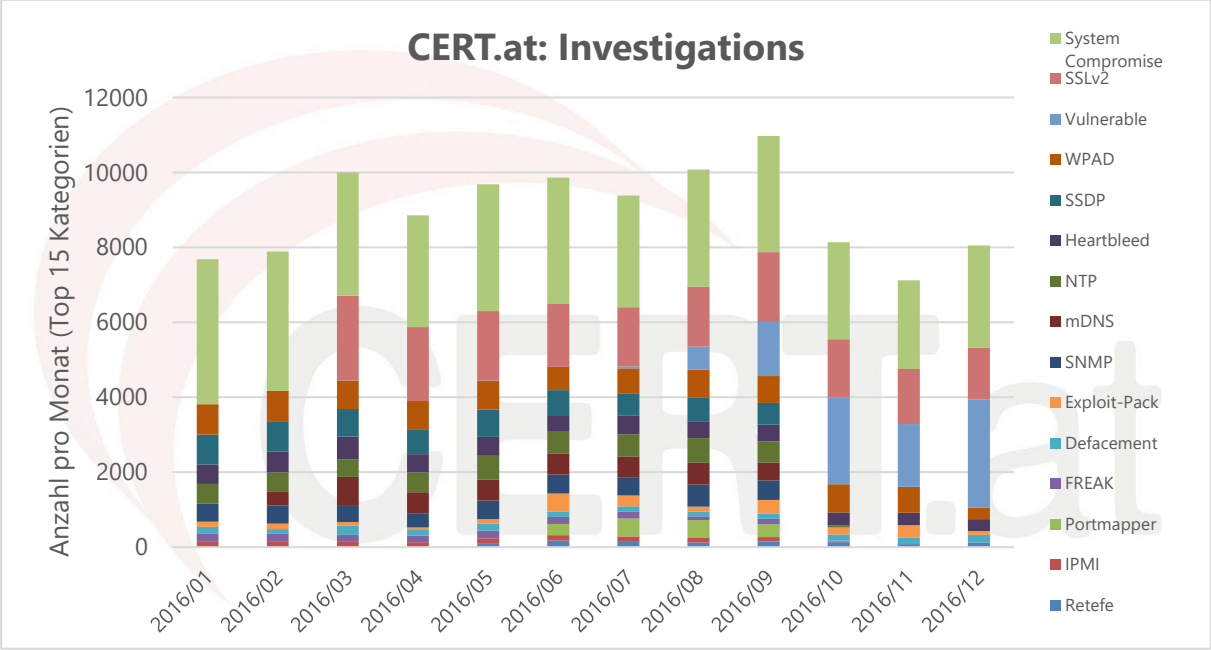


Abbildung 4: Klassifizierung der von CERT.at durchgeführten Investigations nach Bedrohungsformen im Zeitverlauf, Quelle: CERT.at

Im Laufe von 2016 hat CERT.at einen Großteil der alten Scripts zur halbautomatischen Verarbeitung von Informationen über Infektionen und Fehlkonfigurationen durch ein neues System namens IntelMQ ersetzt. IntelMQ (https://github.com/certtools/intelmq) wird als gemeinsames Projekt von mehreren europäischen CERTs als Open Source Software entwickelt, und wurde darüber hinaus im Rahmen der Förderung der EU für CERTs (Connecting Europe Facility Telecom, Cyber Security Call 2+3) als zentrale Komponente erkannt. Im Zuge dieser Umstellung wurde auch die Zuordnung von Einzelereignissen („events": z.B. Zugriff eines PCs auf einen Malware-Kontrollserver, positiver Test eines Servers auf eine Schwachstelle, ...) zu diesen Tickets geändert. Dies ist in den Graphen gut zu erkennen.

Früher wurden alle Datenquellen (etwa Ergebnisse der Scans von ShadowServer, oder Daten von Microsofts Digital Crime Unit) unabhängig voneinander bearbeitet. Da diese typischerweise einmal pro Tag einen Datensatz liefern, ergab sich so pro Quelle ein Report, ein Incident und dann pro vorkommendem Netzbetreiber eine Investigation.

Das neue System basiert auf Events, die jeweils eine einzelne Beobachtung bzw. Messung darstellen. Diese werden täglich pro Kategorie als ein Incident zusammengefasst und verarbeitet. Die dahinterstehende Taxonomie geht ebenfalls aus einer europäischen

Zusammenarbeit hervor. Damit soll erreicht werden, dass sowohl der Datenaustausch zwischen den CERTs, als auch ein länderübergreifender Vergleich der Statistiken, einfacher wird.

Den Effekt in den Graphen der Investigations gut erkennbar: So wurden die getrennten Investigations zu DDoS-Reflektoren per SNMP, NTP oder SSDP in Mails zu verwundbaren Systemen („Vulnerable") zusammengefasst. Da es zwischen den Infektionsdaten-Quellen immer wieder Überschneidungen gibt, ermöglicht diese Vorgehensweise eine Vermeidung mehrfacher Einträge in Investigations und somit eine einfachere Verarbeitung durch die Netzbetreiber.

Da IntelMQ nicht mehr auf tägliche Reports per E-Mail angewiesen ist, ermöglicht dieses System erstmals eine Verarbeitung und Verteilung der Sensordaten in Echtzeit. Es ist geplant, den Netzbetreibern ein Webportal zur Verfügung zu stellen, mit welchem diese die Beschaffenheit der bezüglich ihres Bereiches gesandten CERT-Meldungen selbst konfigurieren können.

Diese Umstellung wird die Vergleichbarkeit der zukünftigen Report/Incident/Investigation Zahlen mit den historischen Daten negativ beeinflussen. Dem ist jedoch entgegenzuhalten, dass die Zahl der E-Mails von CERT.at alleine seit Anbeginn nur bedingt etwas über den Sicherheitsstatus in Österreich ausgesagt hat. Grund dafür ist der Umstand, dass eine E-Mail mit lediglich einer Infektion in dieser Betrachtungsweise einem E-Mail mit tausenden IP-Adressen rechnerisch gleichgestellt wurde.

Aussagekräftigere Lageinformationen bekommt man aus den Daten zu Events, die den folgenden Graphen zugrunde liegen.

Botnetze in Österreich

Die vorhandene Datenbasis hinsichtlich der in Österreich verbreiteten Botnetze hängt sehr stark von der Möglichkeit ab, diese Daten auch erheben zu können. Bessere Daten sind daher vor allem für ältere Botnetze vorhanden, da diese bereits gut analysiert sind und entsprechende Sensoren („Sinkholes") betrieben werden. Darüber hinaus verwenden verschiedene Quellen auch unterschiedliche Bezeichnungen für die gleiche Malware. Dadurch ist die Aggregation aller Quellen in ein konsistentes Bild nicht immer möglich. In der folgenden Grafik werden die Meldungen nach Botnetzen in Österreich dargestellt.

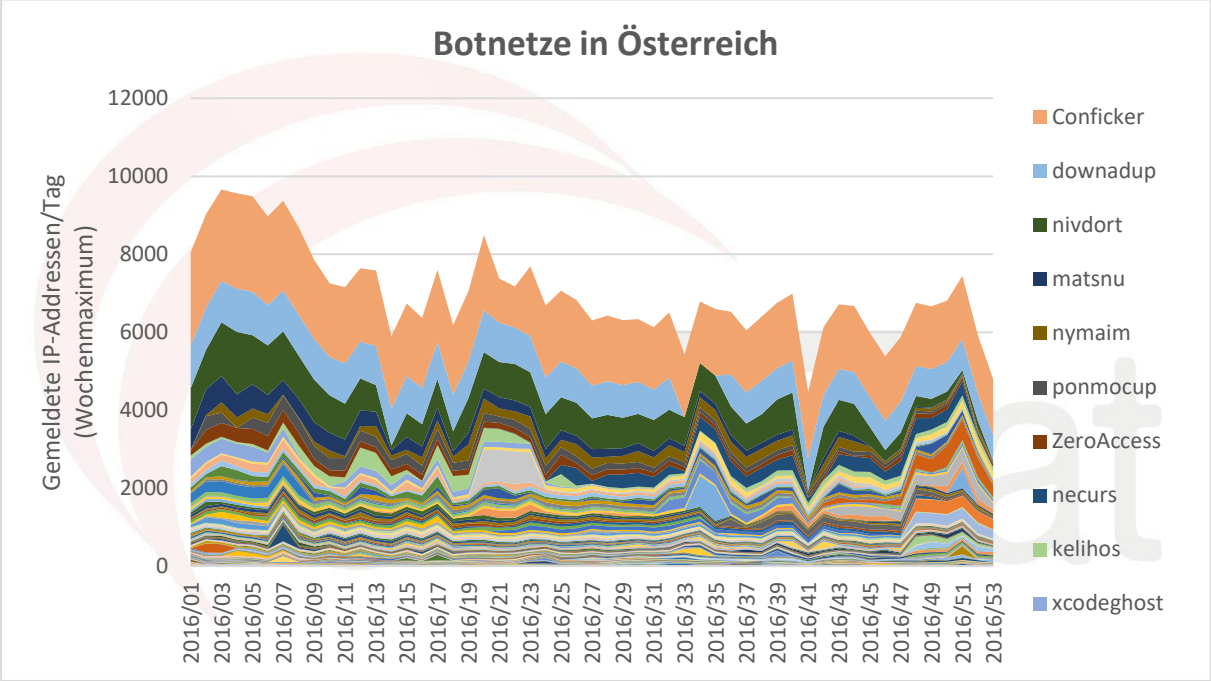


Abbildung 5: Klassifizierung der Meldungen nach Botnetzen im Zeitverlauf (Wochen) des Jahres 2016 bis Anfang 2017, Quelle: CERT.at

Über die vergangenen Jahre hinweg betrachtet zeigt sich folgender Trend:

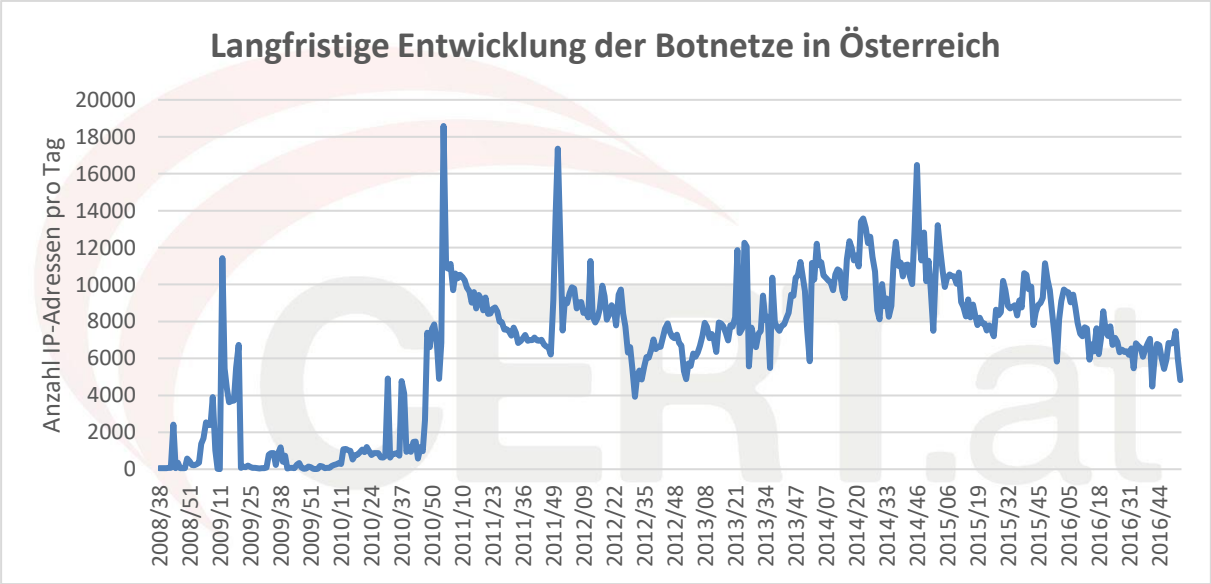


Abbildung 6: Langfristige Entwicklung der Botnetze in Österreich, 2008-2016, Quelle: CERT.at

Da sich im Laufe der Jahre sowohl die verfügbaren Datenquellen von CERT.at, als auch deren Qualität stark verändert haben, ist das Ablesen eines langfristigen Trends nicht möglich. Mit 2017 wird CERT.at diese Datenbasis um einen weiteren Datenlieferanten ausbauen, was zu einem Sprung in dieser Statistik führen wird.

Die Quellen der Daten zu Infektionen

Die den Statistiken zu Botnetzen zugrundeliegenden Daten stammen aus unterschiedlichen Quellen. Durch die diversen Mess- und Erhebungsmöglichkeiten dieser Daten, die von Aktionen von Strafverfolgungsbehörden bis zu Spuren, die Täter selbst hinterlassen reichen, wird ein umfassender Blick auf die IT-Sicherheitslage in Österreich ermöglicht. Zu den diesbezüglichen Quellen gehören:

- Aktionen von Strafverfolgungsbehörden: Diese Daten stammen aus der Beschlagnahmung von Domains oder Servern von Botnetzen. Dabei werden die Steuerserver der Botnetze (sog. „Command and Control Server") durch Sensoren (diese werden „Sinkholes" genannt) ersetzt, die mitprotokollieren, von wo aus infizierte PCs neue Befehle abholen wollen.
- Analyse der Malware und Registrierung der verwendeten Domains: In vielen Fällen wird der „Command and Control Server" nicht über eine konstante Domain angesprochen, sondern über nur kurzfristig gültige Domains, die aus dem aktuellen Datum abgeleitet werden. Wenn eine Analyse der Malware diesen Algorithmus extrahiert, so besteht die Möglichkeit, die verwendeten Domains im Voraus zu berechnen und sie zu registrieren. Damit lassen sich Sinkholes betreiben.
- Verwendet die Malware einen Peer-to-Peer (P2P) Mechanismus für die Kommunikation, so kann man durch eine Teilnahme am P2P Protokoll die Mitglieder des P2P-Netzes bestimmen.
- In manchen Fällen gelingt es der Polizei, SicherheitsforscherInnen oder CERTs Zugang zu Servern der Angreifer zu erlangen. Die dort vorgefundenen Daten können sehr aufschlussreich sein.
- Aktive Suche nach Sicherheitsproblemen: Manche Sicherheitsprobleme können „von außen" überprüft werden. Beispielsweise, ob eine IP-Adresse auf gewisse Protokoll-Anfragen antwortet und sich daher als DDoS-Verstärker missbrauchen lässt.
- Suche mittels Suchmaschinen: Will man nach aktuellen Problemen verwundbarer Webseiten suchen, so kann man dazu auch gängige Suchmaschinen wie Google, Bing usw. benutzen, indem im Quellcode von Webseiten gezielt nach Spuren von eingeschleustem, schadhaften PHP Code gesucht wird (siehe Beispiel über Fake Pharmacy Hacks), was ein Indikator dafür ist, dass eine Webseite für böswillige Zwecke missbraucht wird.
- Blacklisten: Von mehreren Internet Service Betreibern werden „Listen" von als bösartig oder gefährlich eingestuften IP-Adressen, Domains und URLs geführt. Der/Die einfache Internet-NutzerIn sieht den Effekt dieser Blacklists vor allem dann, wenn der Browser vor einem Besuch einer Phishing-Seite warnt.
- Die Täter selber: So melden etwa einige der Einbrecher in Webseiten ihre „Defacements" bei zone-h.org. Gestohlene Daten aus Datenbankeinbrüchen landen auch oft auf „pastebin".

Am 30. November 2016 wurden durch eine breit angelegte Kooperation von Polizei (Europol, Eurojust, FBI...), Staatsanwälten und IT Sicherheitsorganisationen (BSI, Shadowserver, CERTs) die Server und Domains von Avalanche übernommen. Ausschlaggebender Grund dafür war

Avalanches Beteiligung an mehreren großen Botnetzen. Dies war ein wichtiger Schritt in Richtung eines sichereren Cyber Raumes durch internationale Zusammenarbeit.

Dies war ein gutes Beispiel für „Aktionen von Strafverfolgungsbehörden", denn statt der echten Command and Control Server nehmen die infizierten PCs mit Sensoren ("Sinkholes") Kontakt auf, die von Sicherheitsforschern im Auftrag der Polizei betrieben werden. Die so erhaltenen Daten werden an CERT.at übermittelt, das sie wiederum an die Netzbetreiber weiterreicht. Anfänglich wurden mehr als tausend Infektionen in Österreich gemessen:

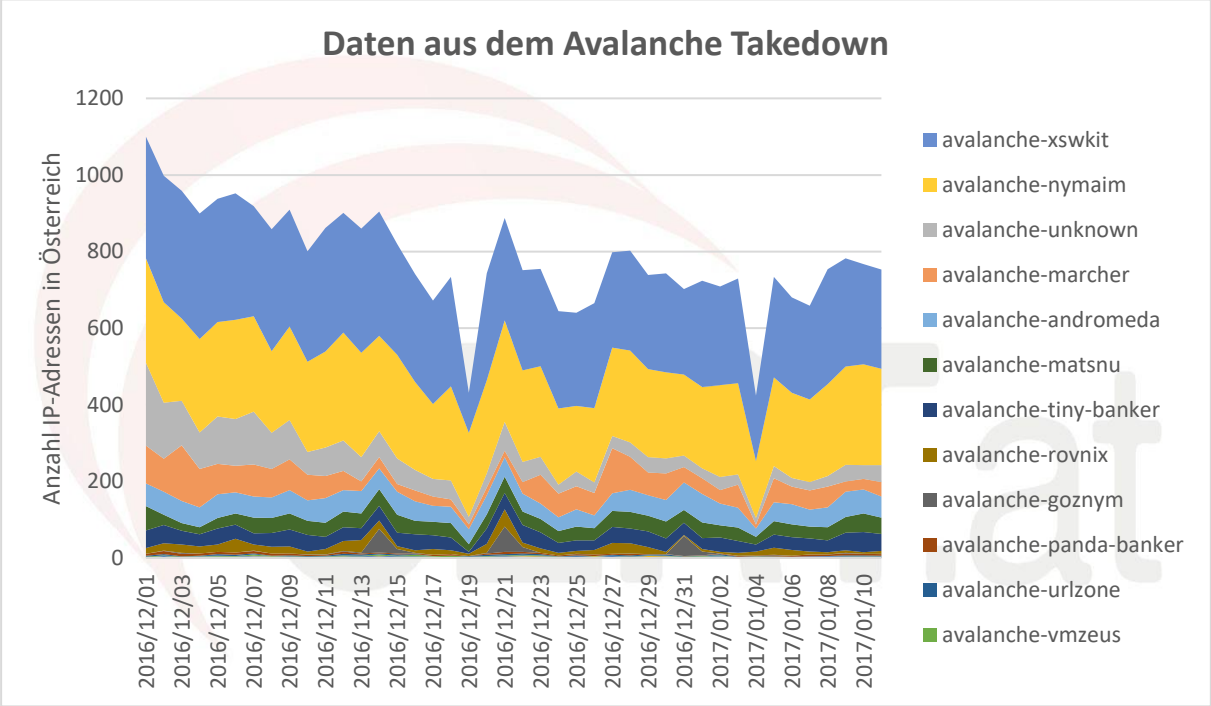


Abbildung 7: Daten aus dem Avalanche Takedown in Österreich, 2016 bis Anfang 2017, Quelle: CERT.at

Denial of Service-Attacken – DoS und DDoS

DoS (Denial of Service) und DDoS (Distributed Denial of Service) Attacken zählen derzeit zu den häufigsten und wirksamsten Cyber Attacken. Vor allem in der Industrie und dem Finanzwesen werden diese Angriffe eingesetzt, um Unternehmen unter Druck zu setzen und hohe Summen an Schutzgeld einzufordern. Auch im Bereich der Cyber Spionage gehören sie mittlerweile zum Standardrepertoire von Angreifern.

DDoS-Attacken legen Webserver oder ganze Netzwerke regelrecht lahm. Im Gegensatz zu einer einfachen DoS-Attacke haben DDoS-Angriffe eine wesentlich höhere Schlagkraft. Mehrere Computer greifen dabei gleichzeitig und im Verbund (beispielsweise über ein Botnetz) eine Webseite oder eine ganze Netzinfrastruktur an. Das angegriffene System wird mit (teils sinnlosen) Anfragen überflutet, die mit den dort zur Verfügung stehenden Ressourcen nicht mehr schnell genug abgearbeitet werden können. Typische DDoS-Angriffe zielen dabei

regelmäßig auf die Überlastung der Internetanbindung, der Ressourcen der Netzwerkkomponenten sowie der Web- und Datenbankserver ab.

Zahlen des aktuellen "DDoS Intelligence Report" von Kasperky für das dritte Quartal 2016 zeigen, dass die DDoS-Attacken in und aus Westeuropa zugenommen haben. Das hat auch der durch einen DDoS-Angriff mit der Malware Mirai (siehe Absatz „Vorkommse 2016 mit Mirai und die Verbindung zu Botnets“) über das Internet der Dinge („Internet of Things“ – IoT) auf den Internetdienstleister Dyn verursachte Ausfall von Online-Angeboten wie Amazon, Netflix, Twitter, Spotify, AirBnB oder Reddit am 21. Oktober 2016 gezeigt. Einzelne DDoS-Attacken können Schäden in Millionenhöhe verursachen. Acht von zehn betroffenen Unternehmen werden im Zeitraum eines Jahres sogar mehrfach angegriffen, wie eine weitere Studie (Quelle: "Corporate IT Security Risks") von Kaspersky Lab belegt, bei der mehr als 4.000 EntscheiderInnen aus kleinen, mittleren und Großunternehmen aus 25 Ländern zu IT-Sicherheitsthemen und in ihren Unternehmen aufgetretenen IT-Sicherheitsvorfällen befragt wurden. Die Zunahme der Angriffe in Westeuropa geht einher mit einer wachsenden Zahl von Command and Control Servern, welche die Botnetze steuern, die häufig für solche Attacken verwendet werden.

DDoS-Angriffe lassen sich im Wesentlichen in **drei Gruppen** kategorisieren:

- **quantitative Angriffe:** Diese versuchen, das Zielsystem durch den Angriff zu überlasten. Dabei kommen in der Regel keine hochspezialisierten Angriffsvektoren zum Einsatz, sondern der gewünschte Effekt wird allein durch die Menge des zustandekommenden Datenverkehrs erzielt.
- **qualitative Angriffe:** Diese versuchen primär, Schwachstellen in Systemen gezielt auszunutzen, um so die Erbringung dieses Dienstes für die dafür vorgesehenen BenutzerInnen einzuschränken oder gänzlich zu unterbinden. Solche Angriffe setzen zumeist ein höheres technisches Niveau der Angreifer voraus.
- **die Kombinationen daraus**: Durch Verschränkung von quantitativen und qualitativen Angriffen können Systeme noch effizienter gestört werden.

DDoS-as-a-Service

Gegenwärtig ist in immer stärkerem Ausmaß die Entwicklung zu beobachten, dass DDoS-Angriffe im Internet einfach "eingekauft" werden können. So bieten im "Darknet" zahlreiche Anbieter gegen vergleichsweise geringes Entgelt die Möglichkeit, Angriffe nach Dauer und Volumen preislich gestaffelt zu ordern. Die Bezahlung erfolgt in den meisten Fällen auf Basis der Cryptowährung Bitcoin.

So funktioniert ein DoS/DDoS-Angriff im Detail

Bei DoS-Angriffen werden häufig Schwächen in Anwendungen, Betriebssystemen oder Webprotokollen ausgenutzt. Die Attacken können in verschiedenen Varianten durchgeführt werden:

- Syn Flooding
  Soll eine TCP-Verbindung - etwa zum Abruf einer Webseite - aufgebaut werden, führt dies zu einem Austausch von SYN- und ACK-Datenpaketen zwischen Client und Server (Handshake). Im Falle eines Syn Flooding-Angriffs werden von den Angreifern viele SYN-Pakete losgeschickt die jeweils eine gefälschte Absender-IP-Adresse enthalten. Das Zielsystem antwortet auf diese mit entsprechenden SYN-ACK-Paketen, nur gehen diese Antworten natürlich an die gefälschten IP-Adressen. Dabei wird jeweils etwas Rechenleistung und für eine gewisse Zeit Speicherkapazität in Anspruch genommen. Je höher die Rate der empfangenen SYN-Pakete ist, umso mehr erfolglose Antwortanfragen werden losgeschickt und Ressourcen gebunden. Sind die Verbindungskapazitäten (TCP State Table) ausgeschöpft, dann kann das System keine weiteren Verbindungen mehr annehmen und ist damit auch für legitime Anfragen nicht mehr erreichbar. Für effektive SYN Flooding Angriffe reichen oft schon Bandbreiten im Bereich von wenigen Mbit/s. Mittels SYN Cookies, welche die Bindung von Ressourcen auf einen späteren Zeitpunkt im Handshake verschieben, lassen sich diese Angriffe allerdings gut abwehren.

- Reflected-DoS-Angriff
  Diese Angriffsvariante zielt auf die Überlastung von Leitungskapazitäten und nutzt legitime, aber schlecht konfigurierte UDP-basierte Server im Internet als Reflektoren/Verstärker von Paketen. Der Angreifer schickt viele (kleine) Anfragen an diese Server, wobei er aber die IP-Adresse des Opfers als Absenderadresse einträgt (IP-Spoofing). Die Server halten diese Anfragen für legitim und beantworten sie mit großen oder mehreren Antwortpaketen. Diese werden aufgrund des IP-Spoofing jedoch an das Opfer anstelle des eigentlichen Senders zugestellt.

  Dadurch hat der Angreifer folgende **Vorteile**:
  - Seine Angriffsbandbreite wird durch die Reflektoren verstärkt.
  - Nutzt er viele verschiedene Server als Reflektoren, so sieht das Opfer breit verteilte Angreifer, die sich nicht einfach mit einer Filterliste ausblenden lassen.
  - Der Standort des Angreifers, bzw. die Quelle der gefälschten Pakete ist schwer auszuforschen.

  Für eine solche DoS-Reflection lassen sich mehrere **Protokolle** zweckentfremden:
  Primär sind das UDP-basierte Protokolle, da hier nicht auf Transportebene mittels eines Handshakes die IP-Adresse des Clients validiert wird. Aktuell sind DNS (Domain Name Service), NTP (Network Time Protocol), SSDP (Simple Service Discovery Protocol) die am häufigsten missbrauchten Protokolle. Aber auch SNMP (Simple Network

Management Protocol), portmapper, chargen und sogar LDAP (Active Directory Pings über UDP) wurden schon bei Angriffen gesehen.

CERT.at informiert laufend die heimischen Netzbetreiber über Server in deren Netzen, die sich für solche Angriffe ausnutzen lassen. Wie Abbildung 8 zeigt, ist es ein langwieriger Prozess, das Netz bezüglich dieser Gefahr zu säubern. Um reflected-DoS zu unterbinden, ist eine globale Anstrengung nötig, denn das Problem ist mit dem Umweltschutz oder der globalen Erwärmung vergleichbar: nur wenn alle an einem Strang ziehen, kann sich die Lage nachhaltig verbessern.

- Angriffe auf Applikationslayer
  Sowohl gegen Webserver, als auch gegen Nameserver wurden in der letzten Zeit spezifische Angriffsmuster beobachtet.

  Ähnlich wie Reflection-Attacks funktionieren Angriffe auf Basis der Wordpress-Pingback Funktion. Dies funktioniert folgendermaßen: Blogs verweisen auf Artikel anderer Blogger, was gerne mit einem Retour-Link („Folgende Blogs zitieren diesen Artikel") beantwortet wird. Im Hintergrund notifiziert der zitierende Blog die Quelle, das dortige Wordpress verifiziert das und setzt erst dann den Pingback Link. Dieses Verifizieren ist jedoch ein Problem: Wenn ein Angreifer tausenden von Wordpress-Installationen mitteilt, dass die Webseite des Opfers gerade einen Link gesetzt hat, dann versuchen sie alle, das zu verifizieren und lösen so Überlast beim Opfer aus.

  Angriffe auf das Domain Name System werden ebenfalls regelmäßig registriert. Aktuell beobachtet man „Random Subdomain Requests" als größte Bedrohung: Hierbei werden aus einem Botnet heraus sehr viele Anfragen zu zufällig gewählten Subdomains des Opfers an beliebige Nameserver gestellt. Diese Randomisierung hebt den Effekt von Caches auf, wodurch eine Flut von Anfragen die Nameserver des Opfers erreicht.

Im Jahr 2016 hat CERT.at die Netzbetreiber in Österreich informiert, welche IP-Adressen in den jeweiligen Netzen für eine DDoS Angriffsverstärkung verwendet werden können. Die Entwicklung wird in Abbildung 8 dargestellt.

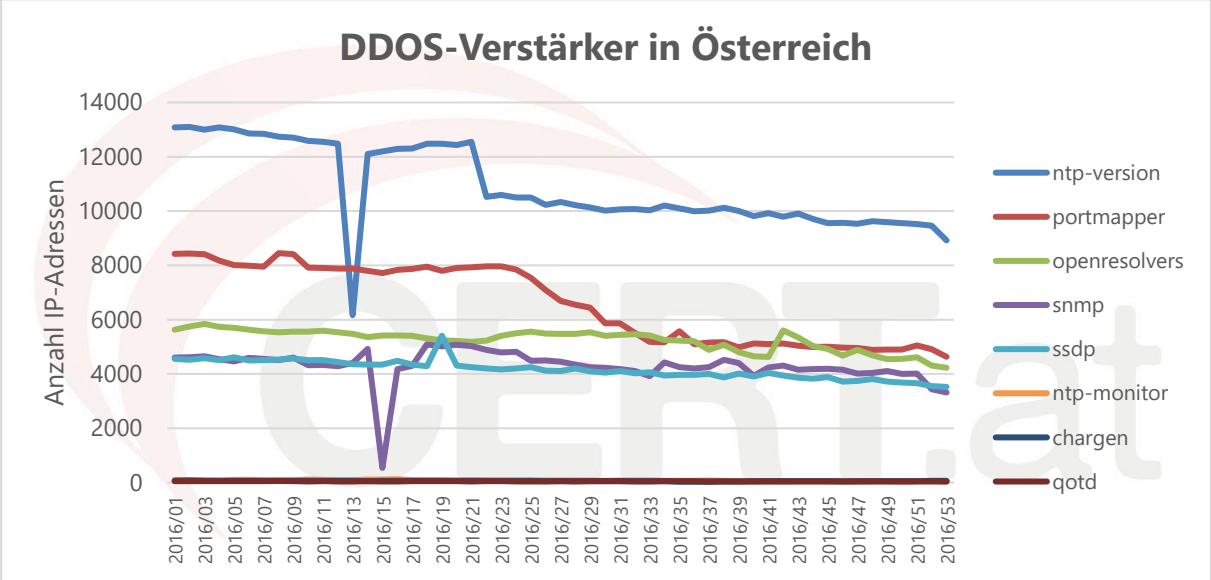


Abbildung 8: Zahl der IP-Adressen als potentielle Angriffsverstärker nach den jeweiligen Netzen im Zeitverlauf, Quelle: CERT.at

Österreichische Unternehmen als Opfer von DDoS-Attacken

In den letzten zwei Jahren hat sich der Kreis der DDoS-Opfer auch in Österreich stark erweitert, vor allem durch das Aufkommen von damit einhergehenden Erpressungen. So gerieten zuletzt etwa auch österreichische Firmen ins Blickfeld der Hacker-Gruppe DD4BC (DDoS for Bitcoins). Initial richteten DD4BC ihre Attacken auf Bitcoin-Webseiten, dann auf Finanzdienstleister, E-Commerce Webseiten und Internet Service Provider. Im Dezember 2015 konnten im Zuge einer Aktion von Europol – unter Federführung des österreichischen Cybercrime-Competence-Centers (C4) im Bundeskriminalamt – die Angreifer gefasst werden.

Auch 2016 gab es Attacken auf österreichische Unternehmen und Organisationen. Prominente Opfer: A1, das Außenministerium, das Bundesheer, die OeNB und der Flughafen Wien. Bei A1 war das Motiv Geld. In einem Erpresserschreiben wurden 100.000 Euro in Bitcoins verlangt. Erst als die Erpresser erkannten, dass die Techniker von A1 imstande waren, den Angriff abzuwehren, gaben sie auf. Die Suche nach den Angreifern gestaltete sich jedoch schwierig, da diese aus mehreren Ländern operierten, unter anderem aus Osteuropa und China. In anderen Fällen waren die Angriffe politisch/nationalistisch motiviert.

Entwicklungen von DoS/DDoS-Angriffen im Zeitverlauf

Lange galt eine Attacke, die 2013 von einem damals 16-jährigen Briten durchgeführt wurde, als größter DDoS-Angriff. Er brachte es ExpertInnen zufolge auf etwa 300 Gigabit pro Sekunde. Im September 2016 wurde eine Attacke bekannt, die diesen Wert deutlich übertraf. Das Opfer war der französische Hoster OVH, der mit bis zu 1,1 Terabit pro Sekunde angegriffen wurde.

DoS/DDos Attacken: Wie man sich schützt und bei Angriffen verhalten sollte

Für Denial of Service oder Distributed Denial of Service Attacken gilt im Grunde dieselbe ernüchternde Tatsache wie in jedem Bereich von IT-Security: Einen vollständigen Schutz gibt es nicht. Wer aber einige grundsätzliche Maßnahmen ergreift, reduziert die Chance auf erfolgreiche Angriffe jedoch deutlich. Umso wichtiger ist es daher, sich frühzeitig vorzubereiten und nicht erst nach einer etwaigen Attacke, mit Überlegungen dazu anzufangen.

Die wichtigsten und **wirksamsten Maßnahmen** sind:

- **Anforderungsanalyse:** Grundlage für das Ergreifen von Sicherheitsmaßnahmen ist eine exakte Kenntnis, welche Verfügbarkeitsanforderungen für welche Dienste (Webserver, Email, Internetzugang, …) gelten. Eine Business Impact Analyse, die auch konkrete Schadenssummen bei Ausfällen beziffert, ist nötig, damit die Kosten für die Gegenmaßnahmen im Verhältnis zu dem damit abgewehrten Schaden stehen.
- **Bestandsaufnahme:** Eine gute Kenntnis der eigenen IT-Infrastruktur und vor allem des Netzwerks und dessen Leistungsgrenzen sind für gezielte Verbesserungen unerlässlich. In vielen Fällen kann erst durch Lasttests bestimmt werden, welche Komponente einen Engpass darstellt.
- **Strategie:** Alle Personen, die mit dem Netzwerk und letztendlich der gesamten IT-Infrastruktur zu tun haben, müssen anhand einer genau definierten Strategie Hand in Hand daran arbeiten, diese umzusetzen. Gerade bei IT-Security sind individuelle Guerilla-Aktionen oder unkoordiniertes Vorgehen gefährlich.
- **Aktives Monitoring:** Alle laufenden Prozesse müssen von einem Monitoring-System überwacht werden, idealerweise 24 Stunden am Tag, sieben Tage die Woche. Mittlerweile gibt es Anbieter, die mit Managed Monitoring aus der Cloud eine günstige, einfach skalierbare und sehr schnell einsetzbare Lösung anbieten und auch etwaige Alarme vorsortieren, damit CIOs oder IT-LeiterInnen nicht mit Fehlalarmen unnötig Zeit verlieren.
- **Härten der Peripherie:** Alle Komponenten der IT-Infrastruktur und des Unternehmensnetzwerkes müssen einem technischen Mindeststandard entsprechen oder auf diesen gebracht werden. Hierbei spricht man vom „Härten der Infrastruktur". Das gilt für die Hardware ebenso wie für die Software. Alle Anwendungen sollten immer auf dem neuesten Release-Stand sein und alle Patches und Updates regelmäßig installiert werden. Ob die Konfiguration aller Systeme auch bzgl. DoS-Angriffen optimal ist, kann nur durch Tests festgestellt werden.
- **Partnersuche:** Eine Organisation kann im eigenen Haus keine DDoS-Angriffe abwehren, die bereits ihre Anbindung an das Internet überlasten. Dafür ist entweder die Mithilfe der ISPs, oder einer Cloud-basierten Lösung nötig. Auch das sollte man schon im Vorfeld vertraglich vereinbaren und testen.

Wie schon erwähnt, ist es trotz aller präventiven Maßnahmen nicht möglich, einen Vorfall komplett auszuschließen oder zu verhindern. Sollte es dennoch zu einem Vorfall kommen, ist es vor allem wichtig, schnell und koordiniert vorzugehen. Dann gibt es eine gute Chance, dass

sich der Schaden in Grenzen hält und schnell behoben werden kann. Auch dieser Angriffsfall sollte in eine umfassende Security-Strategie einfließen. Doch laut einer Studie von F5 Networks verfügt über ein Drittel aller befragten Unternehmen nicht einmal über einen Notfallplan.

Bei den Sofortmaßnahmen im Falle eines Angriffs muss zwischen quantitativen und qualitativen Angriffen unterschieden werden. Erstere haben nicht nur einen Ursprung sondern mehrere, um ein erforderliches Volumen zu generieren. In diesem Fall müssen alle Datenpakete, die sich eindeutig dem Angriff zuordnen lassen, priorisiert, limitiert oder blockiert werden. Bei einem qualitativen Angriff ist die Chance groß, dass der Angriff lediglich von einer begrenzten Anzahl von IP-Absender-Adressen oder überhaupt nur einer einzigen erfolgt. Bei rechtzeitiger Erkennung sollte die entsprechende Adresse vom Router oder der Firewall gefiltert werden.

Mögliche Folgen von DoS/DDoS-Attacken

Die Folgen eines DoS oder DDoS-Angriffs können sehr vielfältig sein und hängen von der Art des Angriffs, der Verwundbarkeit des Systems, dem attackierten Unternehmen und seiner IT- und Netzwerkumgebung ab. In vielen Unternehmen wird noch immer die landläufige Meinung, dass sich mit längeren Ladezeiten oder dem Ausfall eines Dienstes/einer Website der Schaden erledigt hat, vertreten.

Untersuchungen von Kaspersky Lab zufolge kostet eine DDoS-Attacke ein mittelständisches Unternehmen durchschnittlich 50.000 US-Dollar. Großunternehmen müssen nach einem DDoS-Angriff hingegen mit bis zu 417.000 US-Dollar weit mehr aufwenden. Etwaige Folgekosten für externe IT-ExpertInnen, Consultants oder AnwältInnen sind hier noch nicht einberechnet. Natürlich entstehen einem Unternehmen auch Nachteile, die sich nicht unmittelbar finanziell messen lassen wie ein Imageverlust, negative Berichterstattung und damit verbundener Vertrauensverlust.

Neben den finanziellen Folgen müssen Unternehmen aber auch damit rechnen, während einer DoS/DDoS-Attacke ihrer Geschäftstätigkeit nicht wie gewohnt nachgehen zu können: Laut einer weiteren Kaspersky-Studie aus dem Jahr 2014 hatten 61 Prozent der Unternehmen während einer DDoS-Attacke damit zu kämpfen, dass sie zeitweise keinen Zugang zu kritischen Unternehmensinformationen hatten. 38 Prozent glauben, dass die Attacken negative Folgen für die Reputation des Unternehmens hatten., was sich bei 26% auch in steigenden Versicherungsprämien niederschlug.

Vorkommnisse 2016 mit Mirai und die Verbindung zu Botnets

Mirai ist eine Schadsoftware für „Internet of Things"-Geräte, die unter speziellen Linux-Varianten laufen, mit deren Hilfe Botnetze aufgebaut werden können. Damit lassen sich beispielsweise gezielte Angriffe durch absichtliche Überlastungen von Netzen durch DoS oder DDoS-Attacken organisieren. Mirai befällt Internet-of-Things-Systeme und schaltet dann die infizierten Geräte mit anderen zu einem Botnet zusammen.

Gerade im letzten Quartal 2016 haben sich die Angriffe in Verbindung mit Mirai-Botnets stark gehäuft:

- Der Internet-Dienstleister Dyn ist Mitte Oktober das Opfer einer Attacke mit zig-Millionen involvierter IP-Adressen geworden. Durch den Angriff auf Dyn waren Zugänge zu Diensten wie Twitter, Spotify, Paypal, Netflix, Airbnb oder Amazon für viele NutzerInnen in den USA, Europa, Japan und Australien mehrere Stunden lang nicht zu erreichen. Die Angreifer haben für die Attacke zu einem großen Teil mit dem Internet der Dinge (IoT) verbundene Geräte wie Webcams, Router, Drucker, TV-Festplatten-Receiver oder sogar Babyphones genutzt.
- Ende November versuchte Mirai auch, über eine Sicherheitslücke der Wartungsprotolle TR-069 und TR-064 in Modems von DSL und Kabelkunden einzudringen. Im Falle der Deutschen Telekom führte das dazu, dass knapp eine Million Menschen ohne Internet waren, weil deren Modems von diesen Anfragen in ihrer Funktion gestört wurden.

ExpertInnen zufolge müssen EndanwenderInnen, aber auch Hersteller, ihre Einstellung zum Thema Sicherheit grundlegend überdenken. Man sollte keinesfalls davon ausgehen, dass die installierten IoT-Geräte sich selbständig um deren Wartung kümmern. Einige der Kameras, die im Zuge des Mirai-Angriffs auf Dyn gehackt wurden, hätten laut einhelliger Meinung der ExpertInnen allerdings auch niemals zum Verkauf zugelassen werden dürfen. Gerade Billigherstellern wird häufig unterstellt, unzureichende oder sogar keinerlei Schutzmechanismen in ihren Geräten eingeplant zu haben.

Es liegt in der Verantwortung der AnwenderInnen, die Standardeinstellungen zu ändern, für Verschlüsselung zu sorgen und regelmäßig nach Firmware-Updates zu suchen, wenn man Angreifern nicht Tür und Tor öffnen will, um ein verwundbares IoT-Gerät infiltrieren zu können. Auch Standardpasswörter in jeglichen netzwerktechnisch erreichbaren Geräten sind ein großes Problem und sollten immer – vor deren effektiven Einbringung in das Netzwerk - geändert werden, vor allem wenn die Geräte auch noch direkt aus dem Internet erreicht werden können.

Abbildung 9 gibt einen Überblick über die Infektionen in Verbindung mit Mirai-Botnets in Österreich seit Oktober 2016, wobei ein Anstieg gegen Ende des Jahres zu verzeichnen war.

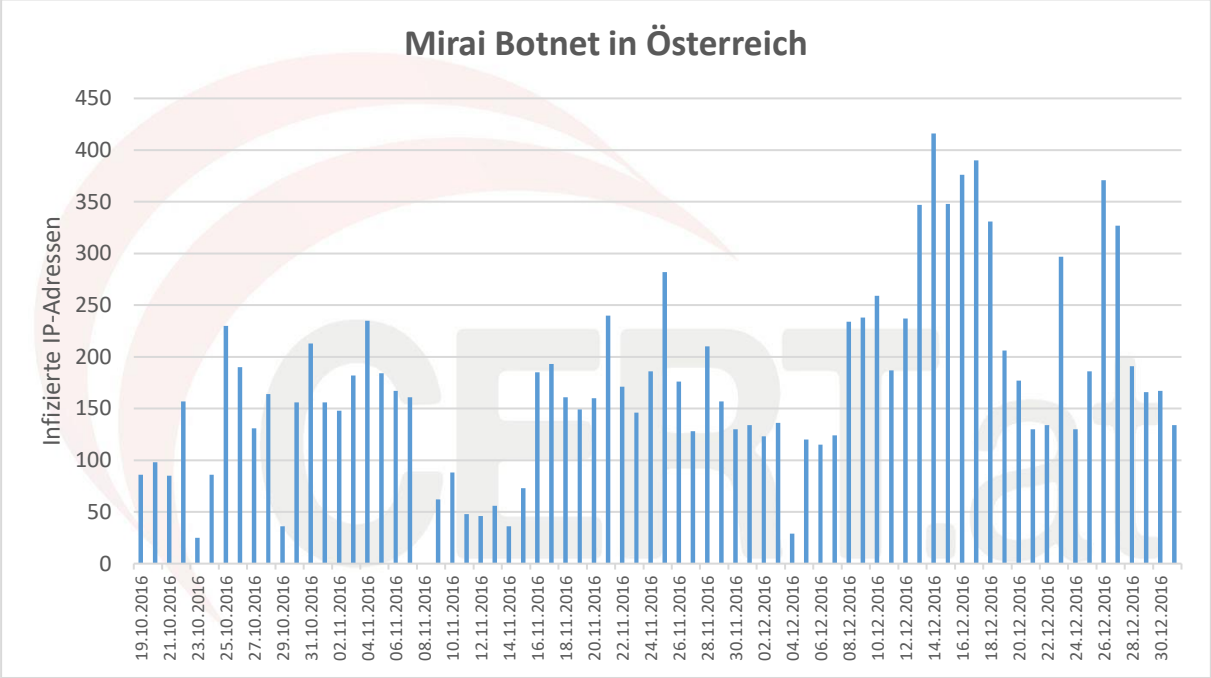


Abbildung 9: Vorfälle in Verbindung mit Mirai seit Oktober 2016 (pro Tag) in Österreich. Quelle: CERT.at

Ransomware

Ransomware ist inzwischen der profitabelste Malware-Typ in der Geschichte der IT. Dabei erpressen Cyber Angreifer ComputernutzerInnen, indem sie ein Endgerät sperren oder die Daten auf dem Computer mit einer mehr oder weniger starken Verschlüsselung unlesbar machen und für die Herausgabe des Schlüssels Lösegeld, meist in Form von sogenannten Bitcoins, verlangen.

Auf internationaler Ebene wurden im Jahr 2015 fast 40 Prozent der Unternehmen Opfer eines Ransomware-Angriffs (Quelle: Report von Malwarebytes: "State of Ransomware"). Der Schaden durch die Ransomware variiert, er reicht von Schäden bei einzelnen Personen bis zur Notwendigkeit, auf Notfallsprozeduren umzusteigen, von Umsatzverlusten bis hin zur Unterbrechung der Geschäftstätigkeit. Die geforderten Summen schwanken ebenfalls, die Bandbreite reichte von 500 Euro bis hin zu 140.000 Euro. Die Bereitschaft, das Lösegeld zu bezahlen reichte global von 3% (USA), bis zu 75% (Kanada) - im Schnitt waren es 37%.

Wichtig zu wissen ist, dass keine Branche von Ransomware-Angriffen unbehelligt geblieben ist. In der ersten Jahreshälfte 2016 wurden Wohlfahrtsverbände, Nichtregierungsorganisationen sowie Elektronik-Unternehmen verstärkt angegriffen. Auch PrivatanwenderInnen werden immer wieder Opfer von Ransomware-Attacken (Quelle: Cisco 2016 Midyear Cybersecurity Report).

Entwicklung von Ransomware in Österreich

Anfang 2016 war auch in Österreich ein starker Anstieg an Ransomware zu verzeichnen. So hat das heimische Unternehmen IKARUS Security Software in dieser Zeit bis zu 25.000 Infektionsversuche durch Erpresser-Trojaner pro Tag registriert - vor allem E-Mails sind ein effizienter und beliebter Verbreitungsvektor. Im Sommer ist die Zahl der Angriffe derart angewachsen, dass das Bundeskriminalamt (BKA) mit „Clavis" eine Sonderkommission (SOKO) im Cybercrime-Competence-Center (C4) des Bundeskriminalamts eingerichtet hat. Die derzeit vier SOKO-MitarbeiterInnen übernehmen seit Gründung die Bearbeitung aller bundesweit angezeigten Ransomware-Fälle – aktuell sind es rund 30 neue Vorfälle pro Woche.

Bei den heimischen Vorfällen haben sich vor allem zwei Angriffsvektoren herauskristallisiert. Bei der als Bewerbungsschreiben getarnten Variante versendeten die Täter E-Mails mit schadhaftem Inhalt. Wurde eine Datei in einem Anhang oder ein Downloadlink geöffnet, installierte sich ein Ableger der Ransomware "Cerber". Die Folge: Die Daten auf sämtlichen Computern und Laufwerken wurden verschlüsselt und waren nicht mehr abrufbar.

Das gleiche passierte bei den Phishing-Mails, die als Online-Rechnung des Stromversorgers Verbund AG getarnt waren. Sie enthielten die Schadsoftware Cryptolocker, die Dateien auf dem PC verschlüsselt.

Funktionsweise und Verbreitung von Ransomware

Ransomware kann grundlegend in folgende zwei Kategorien unterteilt werden:

- Bei Locker-Ransomware wird der Computer des Betroffenen gesperrt und kann nicht mehr verwendet werden, bis ein entsprechendes Lösegeld zur Entsperrung bezahlt wurde. Bekannteste Vertreter sind die seit ca. 2011 im Umlauf befindlichen „Polizeitrojaner" (auch als BKA Trojaner und GVU Virus bekannt).
- Bei Crypto-Ransomware werden mittels kryptografischer Verfahren gezielt Dateien und Dokumente auf dem Computer des Betroffenen verschlüsselt. Aufgrund ihrer aggressiveren Natur haben sich in den vergangenen Jahren besonders Crypto-Ransomware-Varianten bei Cyber Angreifern durchgesetzt. Bekannte Vertreter sind Cryptowall, CryptoLocker, Locky und TeslaCrypt. Eine Übersicht über alle Ransomware-Varianten, die von Sicherheitsforschern gepflegt wird, steht mit Anfang 2017 bei über 200 Einträgen.

Um die Schadsoftware zu verbreiten, kommen mit präparierten E-Mails und Web-Seiten meist bewährte Taktiken zum Einsatz. Neben dem Ausnutzen von Schwachstellen in Programmen bedienen sie sich dabei auch des sogenannten "Social Engineering", indem NutzerInnen unter Vorgabe falscher Informationen dazu gebracht werden, ihre Systeme mit Malware zu infizieren. Trotz der Einfachheit der Mittel bleiben diese Taktiken schwer zu entdecken.

Ransomware-bezogene Spam-Nachrichten enthalten typischerweise bösartige Anhänge (Makros, JavaScript,...), die als Downloader für die tatsächliche Ransomware dienen.

Beispielsweise verwendet die CryptoLocker Kampagne einen bösartigen E-Mail Anhang, der ZeuS/ZBOT herunterlädt. Dieser Information Stealer lädt dann CryptoLocker auf das System und führt diesen aus.

Einige Crypto Ransomware-Familien nutzen Makros, auch um einfache Sandbox-Techniken zu vermeiden. Der Nutzer muss per Hand die in das bösartige Dokument eingebetteten Makros aktivieren, damit die Infektion des Systems gelingt. Hier spielen wiederum die bereits erwähnten Social Engineering-Köder und die menschliche Psyche eine entscheidende Rolle. Locky Crypto („Locky") ist ein bekanntes Beispiel für den Einsatz von bösartigen Makro-Anhängen.

Auch JavaScript-Anhänge wurden gefunden, die automatisch Ransomware-Varianten herunterladen, so etwa XORBAT, ZIPPY, TeslaCrypt 4.0 oder CryptoWall 3.0. Die Angreifer nutzen ebenso VBScript, um Locky und Cerber zu verteilen. Damit kann die Schadsoftware einer Erkennung durch einfache Scanner entgehen.

Generell wenden die Angreifer bei E-Mails mit Ransomware einfache Maßnahmen an, um möglichst wenig aufzufallen. So vermeiden sie es etwa, die Inboxen mit einem Schwall an Spam zu überfluten und verschicken relativ kleine Mengen zu unterschiedlichen Tageszeiten. Damit können herkömmliche Spam-Filter keine verdächtigen Aktivitäten notieren.

Eine andere Strategie der Angreifer ist es, in möglichst viele Webseiten sogenannte Exploit Packs einzubetten, die den Browser der BesucherInnen angreifen. Sind der Browser oder eine Erweiterung des Browsers (z.B. Java, Flash oder PDF) veraltet und weisen eine Schwachstelle auf, so wird diese beim Besuch einer solchen Webseite ausgenützt, um eine Codeausführung auf dem jeweiligen System zu erreichen.

Schutz und Maßnahmen gegen Ransomware

Es gibt keine Wunderwaffe gegen Ransomware, daher ist es wichtig, mehrstufige und einander ergänzende Maßnahmen zu setzen. Welche konkret am besten sind, hängt stark von den jeweiligen Gegebenheiten ab. CERT.at hat mit dem Whitepaper "Empfehlungen zu Ransomware" die wichtigsten Gegenmaßnahmen zusammengefasst.

Proaktiver Schutz: Ransomware-Angriffe können eingedämmt werden, wenn die initiale Codeausführung verhindert wird. Folgende Strategien sind hilfreich:

- **Sicherheitsbewusstsein der User:** Ein verdächtiges E-Mail, das ungelesen gelöscht wird, richtet keinen Schaden an.
- **Effektive Filterung von E-Mails:** Im besten Fall werden E-Mails mit gefährlichem Inhalt erst gar nicht zugestellt, sondern bereits im Vorfeld am E-Mail Gateway aussortiert. Insbesondere alle Dateitypen, die neben reinen Daten auch Code enthalten können, sind gefährlich. Dabei geht es nicht nur um die offensichtlichen wie .exe und .bat, sondern (unter anderem) auch um .cpl, .dll, .ocx, .sys, .scr, .drv, .efi, .fon, .pif, .hlp, .lnk, .js, .chm, .vbs.
- **Schutz des Browsers:** Dazu gehört etwa, dass die Software immer auf dem neuesten Stand ist. Zudem ist es sinnvoll, auf Erweiterungen wie Flash und Java, die für normales Surfen kaum mehr notwendig sind, vollständig zu verzichten. Darüber hinaus empfiehlt sich der Einsatz von Script-Blockern.
- **Automatische Ausführung von Makro-Code in Office-Programmen deaktivieren**: Makros werden häufig in Office-Dateien eingesetzt. Es besteht somit Infektionsgefahr, wenn Office-Programme so eingestellt sind, dass sie Makro-Code ohne Nachfrage ausführen. Man sollte etwa in Outlook und Word das automatische Ausführen von Makro-Code daher deaktivieren.

Backup: Aktuelle, sichere, verfügbare und getestete Sicherheitskopien der Daten sind eines der wirkungsvollsten Mittel gegen die Auswirkungen von Ransomware.

- Zu beachten ist, dass die Backups nicht von der Ransomware mitverschlüsselt werden können. So ist etwa eine dauerhaft an den PC/Server angesteckte USB-Platte für solche Fälle kein wirksames Backup.
- Bei Backups in die Cloud muss sichergestellt werden, dass auch auf "alte" Versionen der gesicherten Dateien zugegriffen werden kann. Im schlimmsten Fall werden bei der Synchronisation mit der Cloud die Kopien durch die bereits von der Ransomware verschlüsselten Dateien überschrieben.
- Die empfohlene Frequenz von Backups hängt vom Umfeld ab, für Firmen ist ein tägliches Backup in den meisten Fällen sinnvoll. Regelmäßiges Testen und Üben der Wiederherstellung von Daten gehören ebenso zu einer guten Backupstrategie wie längerfristiges Aufheben von einzelnen Backupständen.

Rettung der Daten: Manchmal machen die Programmierer von Ransomware Fehler bei der Umsetzung der Verschlüsselung oder dem Schlüsselmanagement. Daher gelingt es Sicherheitsforschern immer wieder, Werkzeuge zur Datenrettung zu erstellen. Die zentrale Anlaufstelle dazu ist die Webseite https://www.nomoreransom.org/, die von Europol koordiniert wird. Zur Identifikation der Ransomware, deren Opfer man geworden ist, dient die Seite https://id-ransomware.malwarehunterteam.com/.

Weitere relevante Vorfälle 2016

Gefälschte Rechnungen bleiben eine beliebte Betrugsmasche

Neben dem Versuch, die technischen Schwachstellen in IT-Systemen gezielt aus den Angeln zu heben, bleibt auch der Mensch selbst das Ziel von Cyber Angriffen. Unternehmen sind dabei primär im Fokus. So gab es auch im Jahr 2016 einige prominente Opfer der Betrugsmasche durch gefälschte Rechnungen. Bei diesen Angriffsmethoden geht es den Angreifern vor allem darum, gefälschte Rechnungen raffiniert zu tarnen und in der Folge durch die getätigten Überweisungen Geld zu verdienen.

Zwei wesentliche Methoden welche sich des zuvor bereits erwähnten "Social Engineering" bedienen haben das Cyber Jahr 2016 geprägt: Die Variante des „**Business E-Mail Compromises**" und des „**CEO-Fraud**". Beim sogenannten **Business E-Mail Compromise** stellt ein Unternehmen zunächst per Mail eine „normale" Rechnung an ein anderes Unternehmen. Nach ein paar Stunden wird ein zweites E-Mail gesandt – diesmal von einem neu registrierten, gefälschten Domain-Namen, der sich oft nur durch einzelne Buchstaben unterscheiden lässt. Im Vorfeld haben die Angreifer somit bereits die bestehende Kommunikation zwischen den Unternehmen abgefangen. Die Folge-E-Mails zeichnen sich dadurch aus, dass sie mit dem vorherigen E-Mail ident sind, jedoch auf ein geändertes Empfängerkonto hinweisen, was in dem E-Mail auch begründet wird (beispielsweise wird eine Kontosperrung durch die Finanz aufgrund eines Audit angegeben). Kommt es in der Folge zu Rückfragen durch den Rechnungsempfänger, wird wiederum vom Angreifer mit gefälschten Dokumenten geantwortet. Sofern der Betrugsversuch durch den Rechnungsempfänger nicht erkannt wird, erfolgt eine Überweisung auf ein falsches Konto – das Konto des Angreifers.

Der sogenannte **CEO-Fraud** bedient sich einer „internen" Variante des Rechnungsbetruges. Hier geben sich Angreifer als Teil des Unternehmens – z.B. als Geschäftsführer oder Finanzvorstand – aus und fordern von MitarbeiterInnen eine dringende Überweisung, beispielsweise durch eine gefälschte E-Mail an die Buchhaltung. Auch hier wurde im Vorfeld bereits die firmeninterne Struktur zum Zwecke des Angriffs ausspioniert, sodass durch die Vorgabe umfangreicher Kenntnisse über das Unternehmen der Betrugsverdacht minimiert wird. Mit dem Hinweis auf die geheime und dringende Überweisung werden die MitarbeiterInnen zum Durchführen einer Überweisung auf ein falsches Konto gebracht.

Prävention und Maßnahmen bei gefälschten Rechnungen

Die wichtigste Frage ist in beiden Fällen die Kontrolle der Quelle und des Inhalts der E-Mails. Dazu gehören Komponenten wie die Absenderadresse oder Rechtschreibfehler beim Absender, die ein Indikator für eine Fälschung sein können, um den versuchten Diebstahl frühzeitig zu erkennen. Grundsätzlich ist es in Unternehmen von Bedeutung, ein Security Management einzuführen, das die Awareness der MitarbeiterInnen für diese und ähnliche Attacken hebt und u.a. auch strenge Regelungen für die Freigabe von Überweisungen beinhaltet.

Im Angriffsfall sollte umgehend Anzeige erstattet und die Bank informiert werden. Darüber hinaus ist die Cyber Crime Meldestelle des BM.I und das Team von CERT.at idealerweise zu informieren.

DROWN-Angriff bedrohte SSL Webserver

Anfang des Jahres 2016 fand die veraltete SSLv2-Verschlüsselung öffentliche Beachtung, da diese Schwachstelle durch die sogenannten DROWN-Angriffe (Decrypting RSA with Obsolete and Weakened eNcryption) ausgenutzt werden kann. Verwendet ein Server das obsolete SSLv2-Protokoll, können durch DROWN auch Clients angegriffen werden, die durch TLS 1.2 verschlüsselte Verbindungen nutzen. Durch ältere Versionen von OpenSSL können sich Angreifer zudem noch leichter einen Bug zunutze machen, um Verbindungen zu entschlüsseln. Bereits im März 2016 wurden durch CERT.at alle in Österreich betroffenen Netzbetreiber informiert. Seit 3. März 2016 testet CERT.at täglich alle Mail und Webserver von .at-Domains auf SSLv2-Support. Für Serverbetreiber ist hierbei vor allem von Bedeutung, im Bereich TLS Settings stets up-to-date zu sein bzw. laufende Aktualisierungen durchzuführen.

Nimmt man die rund 1,2 Millionen Domains unter .at als Datenbasis, so werden diese von rund 190.000 Webservern und 100.000 Mailservern betrieben. Ein laufender Test dieser Server auf die Verfügbarkeit der SSlv2-Protokolls findet die folgende Entwicklung:

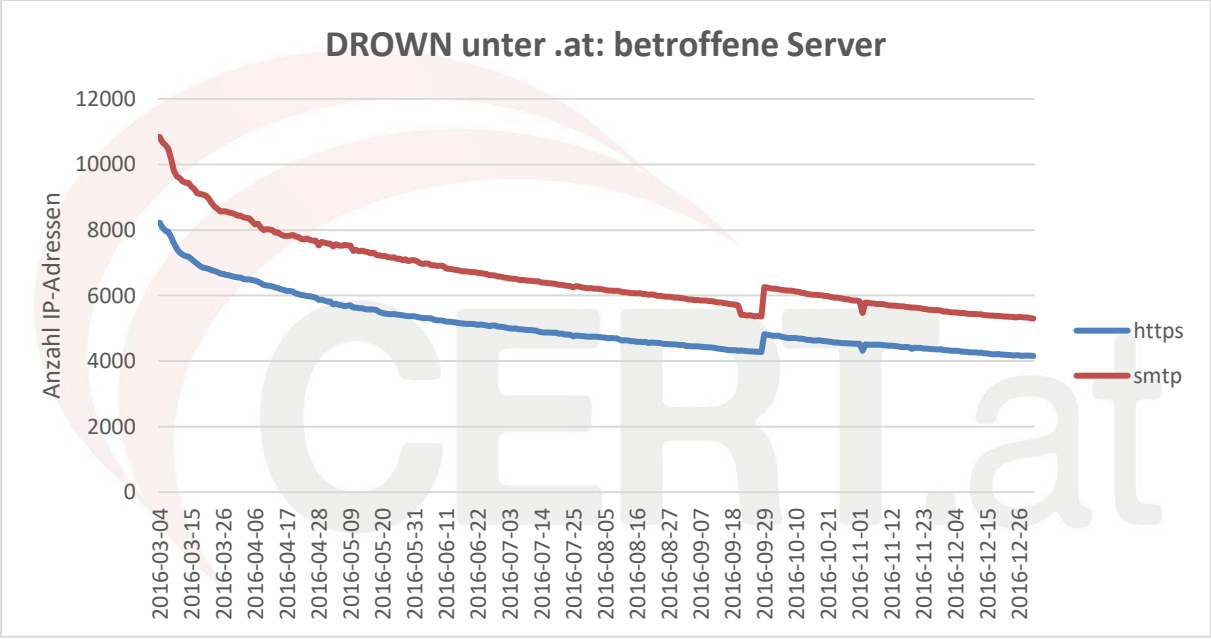


Abbildung 10: DROWN unter .at: betroffene Server im Jahr 2016, Quelle: CERT.at

Der Sprung Ende September ergibt sich aus einer Aktualisierung der Domainliste und der Zuordnung von Domains auf IP-Adressen.

Heartbleed

Im April 2014 wurde der „Heartbleed" Bug in OpenSSL gefunden. CERT.at hat damals – genauso wie 2016 bei DROWN – Tests gestartet, um die Betroffenen zu warnen. Seit damals hat sich der Graph der betroffenen Server so entwickelt:

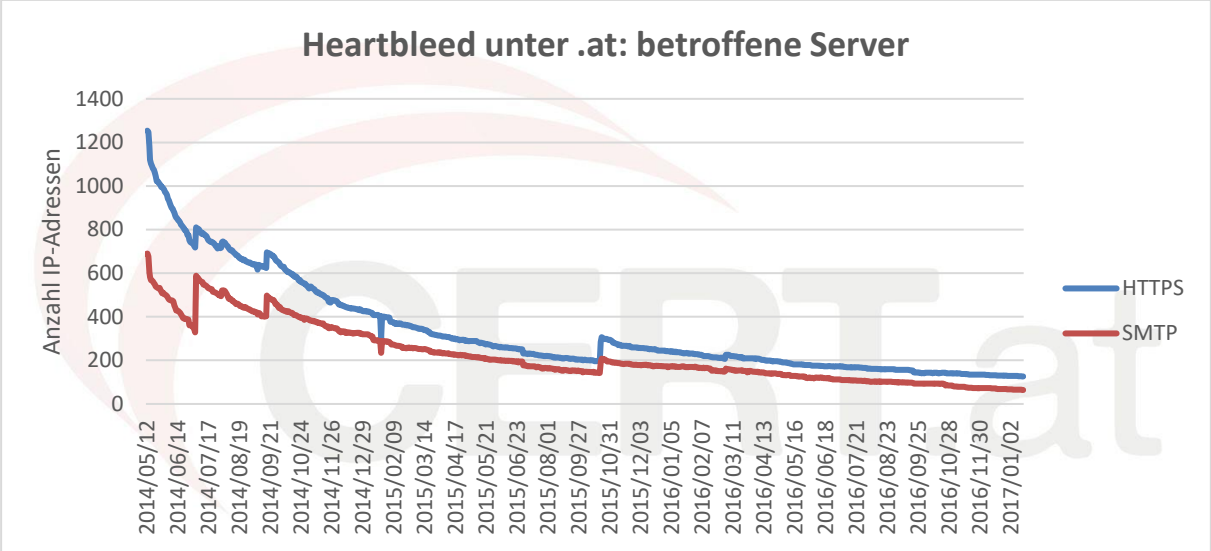


Abbildung 11: Heartbleed unter .at: betroffene Server, Mitte 2014 bis Anfang 2017, Quelle: CERT.at

3. CYBER ÜBUNGEN: WICHTIGER BEITRAG ZUM SCHUTZ DER IKT-INFRASTRUKTUR

Das Stichwort "Digitalisierung" ist Synonym für einen stetigen Wandel. Dieser Wandel betrifft sowohl die zivile Gesellschaft als auch die Wirtschaft, die Politik und im Speziellen die Informations- und Kommunikationstechnologie (IKT) selbst. Mit zunehmender Nutzung des Cyber Raumes ist eine steigende Bedrohung durch kontinuierlich neue digitale Angriffsvarianten verbunden. Alleine ein Blick auf die Statistik der angezeigten Cyber Straftaten ist ein Beleg dafür: Im Jahr 2006 wurden in Österreich 3.257 Cyber Straftaten zur Anzeige gebracht – 2015 stieg diese Zahl bereits auf 10.010 Anzeigen (Quelle: BM.I). Bei diesen Zahlen ist zu berücksichtigen, dass die Dunkelziffer sehr hoch ist. Viele Fälle werden aus Angst (etwa wegen möglicher Auswirkungen auf die eigene Reputation), oder weil sie nur kleinere Vergehen betreffen, nie zur Anzeige gebracht werden. Cyber Delikte werden von Betroffenen oft auch gar nicht oder nur sehr spät bemerkt, was u.a. im Bereich der Industriespionage oft der Fall ist.

Im Rahmen der Österreichischen Strategie für Cyber Sicherheit (ÖSCS) wurden – durch Zusammenarbeit des BMEIA, des BM.I, des BMLV unter Federführung des Bundeskanzleramts – diese Entwicklungen im Rahmen der Ziele und Handlungsfelder berücksichtigt. Um den neuesten Stand der Entwicklungen auch in der Praxis Rechnung tragen zu können, spielen Cyber Übungen eine zentrale Rolle. Das Training für den Ernstfall überprüft die Praxistauglichkeit der organisatorischen Strukturen, Pläne und Notfalldokumentation, der Handlungsabläufe im Sinne der in der ÖSCS definierten Handlungsfelder, um stressbedingte Fehleranfälligkeit zu minimieren und überprüft bereits umgesetzte Maßnahmen.

Immer mehr Bereiche benötigen verstärkte Cyber Sicherheit

Vorsicht ist besser als Nachsicht. Ein sicherer und verlässlicher Cyber Raum hat demnach Bedarf an regelmäßigem Training und dem Üben spezifischer Angriffsszenarien. Die europäische IKT-Industrie ist eine der fortschrittlichsten weltweit, sicherheits- und wirtschaftspolitisch relevant und stellt daher eine besondere Zielscheibe für Cyber Angriffe dar. Den europäischen Binnenmarkt für das digitale Zeitalter „sicherheitsfit" zu machen kann einen wirtschaftlichen Mehrwert von 415 Mrd. Euro generieren und zudem zahlreiche neue Arbeitsplätze in der Zukunft schaffen. Zudem wird ein gesamtheitlicher Ansatz zum Schutz kritischer Infrastrukturen immer wichtiger. Aus diesem Grund wird im Rahmen von Cyber Übungen der Schutz kritischer Infrastrukturen besonders stark forciert. Im diesjährigen Bericht Internet-Sicherheit 2016 wird daher ein Überblick über die wichtigsten Cyber Übungen mit österreichischer Beteiligung im Jahr 2016 und ihre inhaltlichen Aufgabenstellungen gegeben.

Cyber Europe 2016 – Die größte pan-europäische Cyber Übung

Alle zwei Jahre organisiert die Europäische Agentur für Netzwerk- und Informationssicherheit (ENISA) die mittlerweile umfassendste internationale IT-Notfall- und Krisenübung „Cyber Europe". Im Jahr 2016 fand die Cyber Europe bereits zum vierten Mal statt und konzentrierte sich diesmal auf Übungsszenarien rund um die Sektoren IT, Telekommunikation und der Cyber Sicherheitsindustrie. Österreich beteiligt sich seit dem Jahr 2010 an der Cyber Europe. Dies wird in Form einer parallel abgehaltenen, nationalen Übung, in diesem Jahr der „CE.AT 2016", unter Federführung des BKA realisiert.

Die Cyber Europe 2016 wurde in zwei Phasen unterteilt. Die erste Übungsphase startete bereits im April 2016 und dauerte bis Oktober. Diese ausgedehnte erste Phase diente dazu, eine Vielzahl an relevanten Sicherheitsvorfällen und Angriffsszenarien zu Übungszwecken innerhalb einer sicheren Übungsumgebung, bereitgestellt durch die ENISA, ausführlich zu analysieren.

In der zweiten Phase, die am 13. und 14. Oktober 2016 durchgeführt wurde, konzentrierten sich die über 700 Cyber SicherheitsexpertInnen aus 30 EU und EFTA-Staaten sowie aus über 300 Organisationen auf das Übungsszenario einer simulierten, großen internationalen Cyber Krise, welche auf Daten aus der ersten Phase basierte. Es galt, Lösungsansätze für Vorfälle bzgl. Drohnen, Cloud Computing, mobile Malware oder Ransomware auf lokaler, nationaler und europäischer Ebene zu finden. Die umfassende Übung bezog auch Komponenten wie mediale Berichterstattung, die Auswirkung auf Unternehmen und den öffentlichen Sektor sowie die sozialen Medien mit ein und markierte eines der bislang realistischsten Szenarien für eine Cyber Übung.

Das vorrangige Ziel der Übung war die Verbesserung der Kooperation auf nationaler sowie europäischer Ebene – vor allem hinsichtlich der Prozess- und Kooperationsmechanismen der NIS-Richtlinie. Gleichzeitig wirken die Erkenntnisse die Cyber Europe 2016 auch auf die Ziele und Handlungsfelder der ÖSCS ein. Neben der Ausarbeitung von Handlungsempfehlungen aus den Resultaten spielen die Kontinuität von Cyber Übungen und das regelmäßige Überprüfen der Strukturen und Prozesse eine große Rolle, um mit den Entwicklungen von Cyber Bedrohungen Schritt halten zu können und so eine nachhaltige Widerstandsfähigkeit dagegen zu erreichen.

Cyber Europe Austria 2016 (CE.AT 2016)

Die CE.AT 2016 wurde in Österreich durch das BKA am 13. Oktober 2016, bereits zum dritten Mal parallel zur pan-europäischen „Cyber Europe", erfolgreich durchgeführt. Im Vorfeld der Übung wurden zwei wesentliche Ziele definiert: Die Fortsetzung des Optimierungsprozesses der Kollaborations- und Koordinationsstrukturen zwischen privaten und staatlichen AkteurInnen und das Aufzeigen von übergreifenden Stärken und Schwächen bei der Kommunikation und Kollaboration zwischen den TeilnehmerInnen selbst. An der CE.AT 2016 nahmen insgesamt zehn Organisationen aus dem öffentlichen und dem privaten Sektor teil.

Das umfassende Übungs-Szenario orientierte sich an jenem der internationalen „Cyber Europe 2016" Übung und wurde auf spezifische österreichische Begebenheiten angepasst. Neben den simulierten Cyber Angriffen auf Webseiten und Online Anwendungen der öffentlichen Verwaltung und der ISPs, wurden darüber hinaus die Auswirkungen der Attacken auf die mediale Öffentlichkeit einbezogen. Mit Fortdauer der Übung wurden die Szenarien ausgeweitet, was zu einer zunehmenden Übungskomplexität führte. Neben der Auswertung von im Vorfeld definierten Leistungskennzahlen wurde somit auch die Krisenkommunikation gegenüber der Öffentlichkeit für den Ernstfall geprobt.

Auf Basis der Ergebnisse und durch die Erfüllung der im Vorfeld definierten Übungsziele konnten durch die CE.AT 2016 wichtige Lessons Learned für die Zukunft gewonnen werden. Dazu gehört, dass das Vorhandensein und die reibungslose Zusammenarbeit von Strukturen für den Austausch von Informationen und für die Erstellung eines Gesamtlagebilds von maßgeblicher Bedeutung für die erfolgreiche Bewältigung einer Cyber Krise ist. Die in der ÖSCS definierte „Operative Koordinierungsstruktur"", welche während der CE.AT 2014 erstmals zum Einsatz kam, konnte bei der CE.AT 2016 erneut beübt werden. Auch der Sektor- übergreifende Informationsaustausch und die Kooperation zwischen Stakeholdern stellen einen Schlüssel für ein funktionierendes Frühwarnsystem und die Bewältigung von groß angelegten Cyber Angriffen dar. Die Ergebnisse der Cyber Europe Austria 2016 konnten an jene der vergangenen Übungen aus den Jahren 2012 und 2014 anschließen und belegen damit den Erfolg der durchgeführten Cyber Übung.

Planspiel des Kuratorium Sicheres Österreich (KSÖ)

Im Mai dieses Jahres fand das dritte vom KSÖ veranstaltete Planspiel zum Thema Cyber Krisenmanagement statt. Unter Teilnahme des CSC wurde mit dem BKA, dem BM.I, dem BMLVS sowie Unternehmen aus der Wirtschaft am 9. Mai 2016 in dem Übungsszenario die Praxistauglichkeit der damaliger Überlegungen zur nationalen Umsetzung der europäischen NIS-Richtlinie überprüft. Insgesamt mehr als 100 Personen aus 14 Organisationen aus Wirtschaft und Verwaltung waren an der Übung beteiligt. Diese Teilnehmerzahl belegt das hohe Interesse und die zunehmende Notwendigkeit einer stärkeren Zusammenarbeit sowie Kommunikation zwischen Behörden und Unternehmen bei Ernstfällen. Wie sich während dieser Übung zeigte, wurde CERT.at von vielen Übungsteilnehmern, insbesondere aus dem privaten Sektor, in der intraorganisatorischen Kommunikation als erster Ansprechpartner bei technisch-organisatorischen Fragestellungen und bei der Informationsverteilung und –weiterleitung auf Ebene der IKT-Administration und –Betrieb kontaktiert (Quelle: KSÖ). Dies belegt die wichtigen Rollen die CERT.at und GovCERT als Informationsdrehscheiben und kompetente Ansprechpartner für Stakeholder in der Österreichischen Cyber Sicherheit Landschaft wahrnehmen.

European Standard Operating Procedures Exercise (EuroSOPEx)

Ein Zusammenschluss europäischer CERTs hat mit Hilfe der ENISA damit begonnen, eine Reihe von Prozessen zu definieren, wie CERTs während eines Cyber Angriffs international in einer strukturierten Form miteinander kooperieren sollen. Diese Initiative nennt sich „European Standard Operating Procedures" (SOPs), welche im Juni 2016 von mehreren europäischen CERTs in Form einer Cyber Übung (EuroSOPEx) erprobt wurden. Österreich beteiligte sich an dieser Übung mit dem GovCERT am 2.6. 2016. Im Laufe der simulierten Kriseneskalation ist gemäß der SOPs die Abhaltung einer Telefonkonferenz vorgesehen, in welcher sich die CERTs über die weitere Vorgehensweise laufend koordinieren. Das GovCERT nahm in dieser Telefonkonferenz die koordinierende Rolle ein.

Cyber Coalition

Die Cyber Coalition wird jährlich von der NATO organisiert. An ihr sind rund 600 internationale TeilnehmerInnen aus 28 NATO-Nationen und 7 NATO-Partnerstaaten beteiligt. Als Partnerstaat werden von österreichischer Seite die Cyber Übungen der NATO vom Bundesministerium für Landesverteidigung und Sport (BMLVS) koordiniert. Auch die Experten des GovCERT nahmen an der Übung teil.

Die Cyber Coalition hat das Ziel die technischen und operationellen Abläufe und Entscheidungsprozesse zwischen den länderübergreifenden TeilnehmerInnen zu trainieren und zu verbessern. Die simulierten Angriffe machten eine koordinierte Zusammenarbeit der ÜbungsteilnehmerInnen notwendig. Dadurch wurden vor allem die Kommunikation und der länderübergreifende Informationsaustausch im Falle eines Cyber Angriffs erprobt. Dies zielte gleichzeitig auch auf eine Verbesserung der jeweiligen nationalen Verteidigungsstrategien ein. Die Cyber Coalition fand in diesem Jahr bereits zum neunten Mal statt.

Crossed Swords

Die „Crossed Swords" Übung priorisiert das Finden von Schwachstellen und Verwundbarkeiten in IT-Systemen und legt das Training der ExpertInnen auf Basis eines Verteidigungsszenarios an. Diese ebenfalls vom NATO „Cooperative Cyber Defence Centre of Excellence" organisierte Übung fand in diesem Jahr vom 9. bis 11. Februar 2016 statt. Österreich war durch das milCERT vertreten.

Übungen sind Investition in eine sicherere Cyber Zukunft

Die Organisation und die Teilnahme an Cyber Übungen sind mit dem Einsatz zeitlicher und finanzieller Ressourcen verbunden. Gleichzeitig erhöht dies jedoch die Resilienz gegenüber Cyber Angriffen um ein Vielfaches und kann so hohe Folgekosten und Schäden durch infizierte Systeme oder beschädigte Netzwerke im Falle einer Cyber Attacke vermeiden.

Die definierten strategischen Ziele der ÖSCS können nur durch praktische Vorbereitung und regelmäßiges Training in die Tat umgesetzt werden. Cyber Übungen spielen für die reale Abwehrfähigkeit daher eine bedeutende Rolle. Sowohl im privatwirtschaftlichen Bereich –

beispielsweise bei einem Angriff auf ein Unternehmen mittels Zero-Day-Lücken – als auch im staatlichen Bereich, unter anderem beim Schutz kritischer Infrastrukturen, sind solche Übungen eine wichtige Voraussetzung für eine koordinierte und strukturierte Abwehr im Krisenfall.

4. NIS-RICHTLINIE: UMSETZUNG AUS ÖSTERREICHISCHER SICHT

Am 7. Februar 2013 hat 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 den Vorschlag für eine **Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-Richtlinie)** veröffentlicht. Das Bundeskanzleramt führte die Verhandlungen zur NIS-Richtlinie im Rat der Europäischen Union vor Ort in Brüssel und ist verantwortlich für die nationale Koordinierung der Umsetzung; zu diesem Zweck wurde unter Vorsitz des Bundeskanzleramtes eine legistische Arbeitsgruppe eingerichtet. Die Richtlinie ist am 8. August 2016 in Kraft getreten und muss binnen 21 Monaten (Mai 2018) in den EU-Mitgliedstaaten in nationales Recht umgesetzt werden.

NIS-Richtlinie

Mit der NIS-Richtlinie soll EU-weit ein hohes Sicherheitsniveau der Netz- und Informationssysteme erreicht werden. Dazu haben (1) die Mitgliedstaaten unter anderem eine nationale NIS-Strategie zu erarbeiten und (2) bestimmte Unternehmen aus wirtschaftlich oder gesellschaftlich wichtigen Sektoren adäquate Sicherheitsmaßnahmen einzuführen und gröbere Störfälle zu melden.

Jeder Mitgliedstaat hat darüber hinaus ein oder mehrere Computer Security Incident Response Teams (CSIRT) einzurichten, denen u.a. Aufgaben wie die mögliche Entgegennahme von Cyber Vorfallsmeldungen, die Ausgabe von Frühwarnungen, die Reaktion auf Sicherheitsvorfälle oder auch die dynamische Analyse von Risiken und Vorfällen zukommen. Österreich verfügt mit dem GovCERT und dem CERT des Energiesektors (Austrian Energy CERT) bereits jetzt über einige CSIRTs, welche im Sinne der NIS-Richtlinie als Meldestellen für freiwillige und verpflichtende Vorfallsmeldungen aus dem jeweiligen Sektor (öffentlicher Sektor für GovCERT, Energiesektor für AEC) fungieren sollen.

Weiters sind in den Mitgliedstaaten ein oder mehrere nationale Behörden („NIS-Behörden") einzurichten, die unter anderem die Bewertung der Sicherheit von Netz- und Informationssystemen vornehmen und verbindliche Anweisungen zur Abhilfe bei festgestellten Mängeln erteilen können. Als Verbindungsstelle zwischen den Mitgliedstaaten, der Kooperationsgruppe und dem CSIRT-Netzwerk ist zudem in jedem Mitgliedstaat die Einrichtung einer nationalen zentralen Anlaufstelle („Single Point of Contact"; SPOC) vorgesehen.

Österreichische Umsetzung der NIS-Richtlinie

Wie auch auf Richtlinien-Ebene sind die obersten Ziele des nationalen Gesetzgebers die Prävention gegen Sicherheitsvorfälle die Netz-und Informationssysteme betreffen sowie die Gewährleistung einer raschen und professionellen Reaktion auf solche Sicherheitsvorfälle.

Zu diesem Zweck sollen die (teilweise schon bestehenden) nationalen Strukturen samt Aufgabenzuteilungen und Befugnisse durch gesetzliche Regelungen festgelegt werden. Bei Erarbeitung des Gesetzes soll darauf geachtet werden einen gut funktionierenden Koordinationsmechanismus zu schaffen, da die NIS-Richtlinie viele unterschiedliche Bereiche betrifft. Diese sind für Betreiber wesentlicher Dienste die Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Trinkwasserversorgung, Gesundheitsdienste und Internetinfrastrukturen. Weiters sind von der Richtlinie auch bestimmte (größere) digitale Diensteanbieter betroffen, welche Online Marktplätze, Suchmaschinen oder Cloud Computing Dienste anbieten.

Es soll ein Rechtsrahmen geschaffen werden, in dem sowohl Betreiber wesentlicher Dienste als auch digitale Diensteanbieter adäquate Sicherheitsmaßnahmen einführen und erhebliche Störfälle melden. Zudem soll die Möglichkeit geschaffen werden, dass sich die von einem Störfall betroffenen Einrichtungen untereinander freiwillig mit den Computer-Notfallteams und staatlichen Stellen auf der Basis gegenseitigen Vertrauens über Risiken, aktuelle Bedrohungen und Vorfälle austauschen können.

Das Bundeskanzleramt koordiniert derzeit eine interministerielle Arbeitsgruppe, welche sich mit der Verfassung des Bundesgesetzes Cyber Sicherheit (Arbeitstitel) befasst.

Nutzen für BürgerInnen und Unternehmen

Für BürgerInnen und Unternehmen ist das Funktionieren z.B. der Strom- oder Trinkwasserversorgung, des Flug- und Straßenverkehrs oder der Gesundheitsversorgung essentiell. Angriffe auf die IKT-Systeme dieser Sektoren können zu massiven und auch langwierigen Beeinträchtigungen führen.

Online-Marktplätze oder Suchmaschinen sind zwar nicht Teil der Grundversorgung, doch viele Unternehmen und BürgerInnen sind vom reibungslosen Funktionieren des Internets abhängig. Viele Unternehmen bieten ihre Dienste und Produkte via Internet an, der Ausfall von Online Marktplätzen oder Online Suchmaschinen kann zu erheblichen Gewinneinbußen führen. Auch im privaten Bereich würde es zu einer Beeinträchtigung des Alltagslebens kommen.

Unternehmen speichern Daten digital (ob in einer Cloud oder lokal) ab, ein Cyber Angriff kann hier massive Schäden anrichten und zudem – über das betroffene Unternehmen hinaus – das Vertrauen in IKT beeinträchtigen.

5. Die Österreichische Strategie für Cyber Sicherheit: Status quo und Ausblick

Österreichische Strategie für Cyber Sicherheit

Mit der Österreichischen Strategie für Cyber Sicherheit (ÖSCS) hat die 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. Die nationale und internationale Absicherung des Cyber Raums ist eine der obersten Prioritäten Österreichs. So sind ein offenes und freies Internet, der Schutz personenbezogener Daten, die Unversehrtheit von miteinander verbundenen Netzwerken die Grundlage für globalen Wohlstand, Sicherheit und Förderung der Menschenrechte.

Gemäß der ÖSCS ist auf den bestehenden operativen Strukturen aufbauend, eine Struktur zur Koordination auf der operativen Ebene zu schaffen. Diese Struktur soll den unverzüglichen Austausch aktueller Informationen über Cyber Sicherheitsvorfälle und die Umsetzung entsprechender Gegenmaßnahmen sicherstellen. In ihrem Rahmen werden ein periodisches und anlassbezogenes operatives Cyber Lagebild für Österreich erstellt und gesamtstaatliche Notfallmaßnahmen im Rahmen des Cyber Krisenmanagements (CKM) unterstützt und koordiniert.

IKDOK nimmt zentrale Aufgaben der operativen Koordinierungsstruktur wahr

Die zentralen Aufgaben der operativen Koordinierungsstruktur werden vom »Inneren Kreis der operativen Koordinierungsstrukturen« (*IKDOK*) wahrgenommen. Diese interministerielle Gruppe setzt sich aus gleichwertigen Vertretern aus BKA/GovCERT, BM.I und BMLVS zusammen. Regelmäßige interministerielle Abstimmungen stellen die reibungslose Zusammenarbeit in diesem komplexen Umfeld sicher. Im Cyber Krisenfall (zivil) wird die Koordination innerhalb der operativen Koordinierungsstruktur durch das Cyber Security Center im BMI wahrgenommen, im Fall der militärischen Landesverteidigung (Cyber Defence) durch das Cyber Verteidigungszentrum im BMLVS.

Der IKDOK bildet im Krisenfall, unterstützt durch den äußeren Kreis der operativen Koordinierungsstruktur, die direkte Schnittstelle zum Cyber Krisenmanagement (*CKM*). Die Mechanismen des CKM lehnen sich eng an die bereits erprobten Abläufe des staatlichen Krisen- und Katastrophenschutzmanagements (*SKKM*) an. Eine zentrale Herausforderung für die an der operativen Koordinierungsstruktur beteiligten Ressorts ist derzeit, die in Beschlussfassung befindliche EU NIS-Richtlinie auf nationaler Ebene umzusetzen und in den bestehenden Strukturen abzubilden.

CSS koordiniert die Implementierung der ÖSCS entlang von sieben Handlungsfeldern
Die Implementierung der ÖSCS ist ein permanenter Prozess, der von einer eigenen Cyber Sicherheit Steuerungsgruppe (*CSS*) koordiniert wird. Diese Steuerungsgruppe unterstützt im Rahmen eines Implementierungsplans mit klar geregelten Verantwortlichkeiten die Umsetzung der Strategie. Im Rahmen des ÖSCS wurden zur Umsetzung sieben Handlungsfelder definiert:

Handlungsfeld 1: Strukturen und Prozesse
Ein zentrales Anliegen im Rahmen der ÖSCS ist die Stärkung bestehender Cyber Strukturen. Zur Schaffung einer gesamtstaatlichen Struktur zur Koordination auf operativer Ebene wurde unter dem Vorsitz des Bundeskanzleramtes die Cyber Sicherheit Steuerungsgruppe (CSS) beauftragt.

Handlungsfeld 2: Governance
Die Arbeitsgruppe Ordnungspolitischer Rahmen wurde beauftragt, einen Bericht über die Notwendigkeit der Schaffung zusätzlicher rechtlicher Grundlagen, regulatorischer Maßnahmen und nicht-rechtlicher Selbstverpflichtungen für die Gewährleistung der Cyber Sicherheit in Österreich zu erstellen. Nach Erstellung eines Zwischenberichts im April 2015 wurde Anfang 2016 der Endbericht vorgelegt, in welchem der Rahmen für die Umsetzung der in der NIS-Richtlinie vorgegebenen Maßnahmen definiert wird. Seit 2014 wird außerdem unter der Verantwortung des CSS ein jährlicher Bericht zur Cyber Sicherheit in Österreich erstellt und veröffentlicht.

Handlungsfeld 3: Kooperation Staat, Wirtschaft und Gesellschaft
Die im März 2015 gebildete Cyber Sicherheit Plattform (CSP) gewährleistet einen periodischen Informationsaustausch zwischen Stakeholdern aus Wirtschaft, Wissenschaft und öffentlicher Verwaltung. Zu den wesentlichsten Aufgaben der CSP zählen neben dem periodischen Informationsaustausch zu wesentlichen Fragen der Cyber Sicherheit zwischen Stakeholdern aus Verwaltung, Wirtschaft sowie Wissenschaft und Forschung auch die Schaffung sogenannter „Branchen-CERTs“, welche in den Sektoren der kritischen Infastrukturen derzeit entstehen. Ebenfalls ein wichtiges Ziel der CSP ist die Initiierung von Kooperationen zwischen den beteiligten Partnern in den Bereichen Sensibilisierung und Ausbildung sowie Forschung und Entwicklung.

Die CSP fungiert als Dach für bereits bestehende Kooperationsformate (wie zB Austrian Trust Circle, KSÖ Cyber Sicherheit Forum, A-SIT, CSA) und berät bzw. unterstützt die Cyber Sicherheit Steuerungsgruppe. Für kleine und mittlere Unternehmen besteht ein Cyber Sicherheit Schwerpunkt mit einem Fokus zur Bewusstseinsbildung für Vorsorgebedarf und Risikoprävention, welcher vom BMWFW koordiniert wird.

Handlungsfeld 4: Schutz kritischer Infrastrukturen
Am 4. November 2014 beschloss die Bundesregierung das Österreichische Programm zum Schutz kritischer Infrastrukturen (APCIP). 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

Als zentrales Internetportal für Themen rund um die Sicherheit in der digitalen Welt fungiert seit Februar 2013 als interministerielle Initiative, in Kooperation mit der österreichischen Wirtschaft, das IKT-Sicherheitsportal (www.onlinesicherheit.gv.at). Dieses Handlungsfeld unterstützt auch die IT-Strategie "efit21 – digitale Bildung" des BMB. Dieses hat das Ziel der Vermittlung digitaler Kompetenzen an SchülerInnen sowie an Lehrende. Des Weiteren wurden auch das C4 Präventionsprojekt "Cyber.Kids" und das Projekt "Click & Check" umgesetzt, in welchem in Schulen Jugendliche ab 14 Jahren über die Gefahren von Internet und Cyber Crime durch speziell ausgebildete PräventionsbeamtInnen informiert werden. Liegen neue Erkenntnisse vor, so leitet das Cyber Crime Competence Center (C4) auch aktuelle Warnmeldungen von der C4 Meldestelle für Cyber Crime an Medien weiter.

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.

Aktueller Stand zur Umsetzung ÖSCS

Im Jahr 2015 wurde der Bundesregierung ein Umsetzungsbericht vorgelegt. Grundlage für die Umsetzung der Strategie ist ein Implementierungsplan mit klar geregelten Verantwortlichkeiten, dessen Abarbeitung von der Cyber Sicherheit Steuerungsgruppe (CSS) gesteuert und überprüft wird. Bis auf wenige Punkte wurden die Maßnahmen dieses Implementierungsplans bereits erfolgreich umgesetzt.

Die neu eingerichteten Strukturen, Prozesse und Aktivitäten stellen die staatliche Organisation von Cyber Sicherheit in Österreich auf eine tragfähige und robuste Basis:

- Die Cyber Sicherheit Steuerungsgruppe (CSS) hat ihre Tätigkeit als strategisches Steuerungselement 2013 aufgenommen.
- Bisher hat die Cyber Sicherheit Steuerungsgruppe (CSS) neun Sitzungen abgehalten.
- Zur Vertiefung der Kooperation mit der Wirtschaft wurden im Rahmen der Cyber Sicherheit Plattform VertreterInnen aus den Sektoren Energie, Finanzen, Internet Service Provider, Industrie, Gesundheit, Transport und Kommunikation in die CSS eingebunden.
- Eine gesamtstaatliche Struktur zur Koordination auf der operativen Ebene wurde geschaffen.
- Zur Bewältigung von Cyberkrisen wurde ein Cyber Krisenmanagement (CKM) eingerichtet.
- Sämtliche neu definierten Strukturen und Prozesse basieren auf bereits etablierten und bewährt effektiven Cyber Strukturen (z. B. CERTs). Eine Stärkung dieser bestehenden Cyber Strukturen ist ein zentrales Anliegen der ÖSCS.
- Die interministerielle Arbeitsgruppe Ordnungspolitischer Rahmen erarbeitete einen Bericht über die Notwendigkeit der Schaffung zusätzlicher rechtlicher Grundlagen, regulatorischer Maßnahmen und nicht-rechtlicher Selbstverpflichtungen für die Gewährleistung der Cyber Sicherheit in Österreich.
- Die NIS-Richtlinie ist zusammen mit den Ergebnissen aus der Arbeitsgruppe Ordnungspolitischer Rahmen sowie jenen der von KSÖ und ATC durchgeführten Workshops mit Wirtschaft und Wissenschaft die Basis für das zukünftige „Bundesgesetz für Cybersicherheit" (Arbeitstitel); es wird von der im Bundeskanzleramt eingerichteten legistischen Arbeitsgruppe erarbeitet.

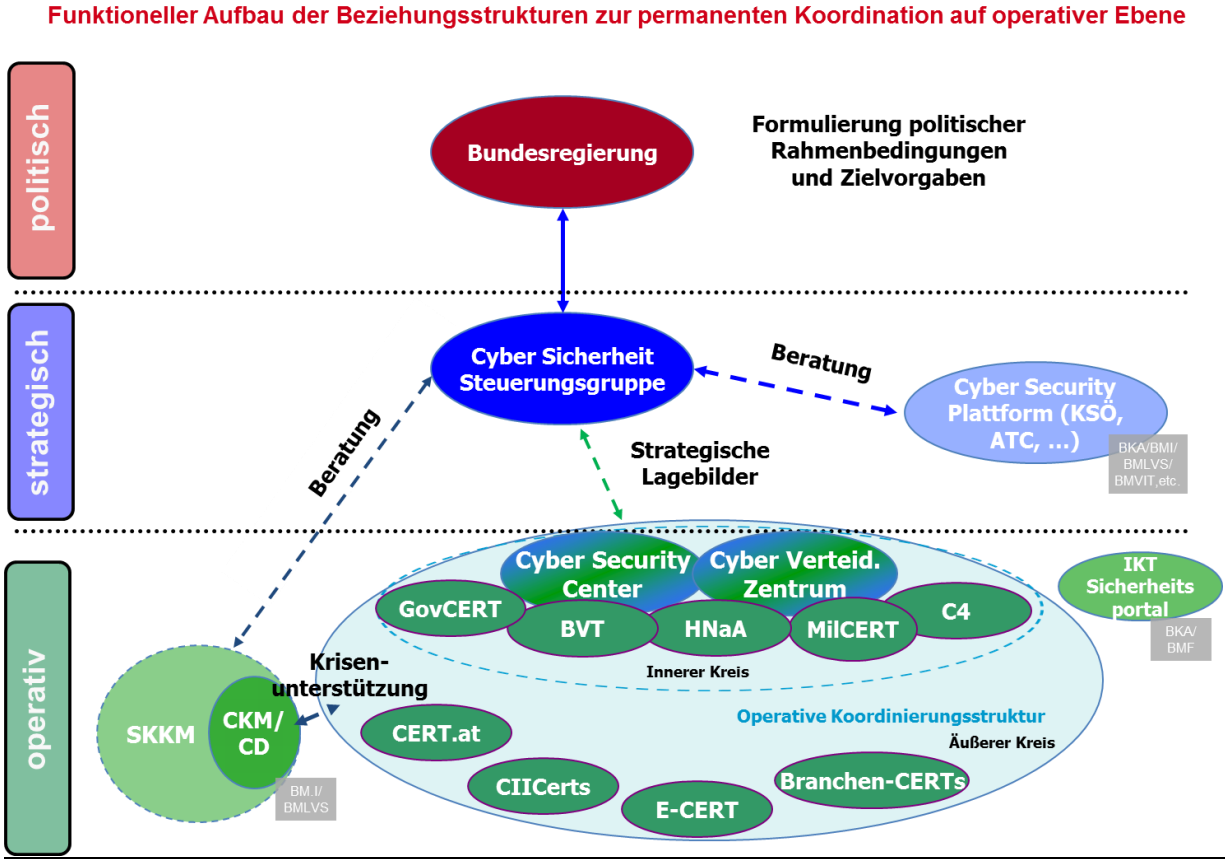


Abbildung 12: Operative Koordinationsstruktur bei der Umsetzung der ÖSCS, Quelle: BKA

Cyber Sicherheit Plattform (CSP) & Cyber Sicherheit Steuerungsgruppe (CSS)

Die vom Bundeskanzleramt als Public-Private-Partnership ins Leben gerufene Cyber-Sicherheit-Plattform ist die zentrale Plattform Österreichs für die Kooperation zwischen dem öffentlichen Sektor und Betreibern kritischer Infrastrukturen in Sachen Cyber-Sicherheit und dem Schutz kritischer Infrastrukturen. Zusammen mit den von CERT.at und dem Bundeskanzleramt eingerichteten Austrian Trust Circles werden so unter Fortführung und Nutzung bestehender Initiativen SicherheitsexpertInnen verschiedener Branchen und Sektoren miteinander vernetzt, um im Anlassfall die richtigen Kontakte verfügbar zu haben und einen reibungslosen Informationsfluss zwischen Stakeholdern aus öffentlicher Verwaltung, Wirtschaft und Wissenschaft sicherzustellen.

Die Cyber-Sicherheit-Plattform dient auch dem Ausbau eines Netzwerks branchenspezifischer Computer Emergency Response Teams (CERTs) aus den kritischen Infrastruktur-Sektoren, damit diese im Fall einer Cyber Attacke auf branchenspezifische Fachexpertise zur Bewältigung zurückgreifen können. Diese Branchen-CERTs erbringen einerseits dank ihrem sektor-spezifischen Know-How dem jeweiligen Sektor kritischer Infrastrukturen wichtige CERT-Dienstleistungen, andererseits erfüllen sie die von der NIS-Richtlinie geforderte Funktion einer Meldestelle für meldungspflichtige Cyber Vorfälle. Darüber hinaus berät und unterstützt die CSP auch die Cyber Sicherheit Steuerungsgruppe (CSS) in strategischen Fragen der Cyber Sicherheit.

Die Konstituierung der Plattform erfolgte im März 2015, im selben Jahr wurden die Vorsitzenden der CSP (welche sich aus der Wirtschaft rekrutieren) bestellt und die Geschäftsordnung formal angenommen. Darüber hinaus wurde eine Themenlandkarte über Cyber Sicherheit Aktivitäten und Initiativen in Österreich präsentiert, sowie eine Arbeitsgruppe im Themenbereich „Standardisierung" eingerichtet, welche bei der zweiten Arbeitssitzung im Juni 2016 ihre Arbeitsergebnisse präsentierte.

Cyber Security Center (CSC) & Cyber Defence Center (CDC)

Die Rahmenbedingungen für die Errichtung und den Betrieb des Cyber Security Centers (CSC) im BM.I sind in der ÖSCS, im Arbeitsprogramm der österreichischen Bundesregierung 2013 - 2018, sowie in der Cyber Sicherheitsstrategie des BM.I festgeschrieben. Gestartet wurde das Projekt zum Aufbau des CSC im Jahr 2014, die Aufnahme des operativen Vollbetriebs ist per Dezember 2017 geplant.

Ziel des Projekts ist die Schaffung von Strukturen und Prozessen zur Steigerung der Cyber-Sicherheit in Österreich. Am Ende soll das CSC im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) eingerichtet und eine Aufbau- und Ablauforganisation für alle Cyber Security-Aufgabenbereiche sein.

Das CSC nimmt eine koordinierende Position im IKDOK ein. Zu den Aufgaben des CSC zählt u.a. das Entgegennehmen von freiwilligen sowie auch verpflichtenden Störfall-Meldungen relevanter IT-Sicherheitsvorfälle. Verpflichtende Meldungen gemäß der NIS-Richtlinie bzw. des künftigen „Bundesgesetzes für Cyber Sicherheit" (Arbeitstitel) werden dem CSC von den Meldestellen (CSIRTs, Computer Security Incident Teams), an welche diese Meldungen zuerst von den Betroffenen gemeldet werden, in Reinform (d.h. nicht anonymisiert) weitergeleitet. Bei freiwilligen Meldungen geschieht dies ebenso, allerdings werden diese dem CSC in anonymisierter Form von den Meldestellen (CSIRTs) weitergeleitet, d.h. nicht in Reinform.

Alle Meldungen, welche das CSC erhält (d.h. verpflichtende und freiwillige) werden in weiterer Folge unmittelbar der IKDOK zur Verfügung gestellt. Ebenso erstellt das CSC auf Basis aktueller Meldungen und Vorfälle ein Gesamtlagebild über den jeweils aktuellen Stand der Cyber Sicherheit in Österreich. Im Unterschied zu einzelnen Unternehmen, kann das CSC IKT-Sicherheitsvorfälle in einen größeren Zusammenhang stellen und bei einer durch Cyber Probleme ausgelösten Krise schnellstmöglich mit dem bestehenden staatlichen Krisen- und Katastrophenmanagement zusammenarbeiten.

Eine weitere zentrale Aufgabe des CSC ist die Präventionsarbeit in Form von Awareness-Veranstaltungen, Vorträgen oder Beratungsgesprächen. Besonderer Wert wird dabei auf eine gute Zusammenarbeit mit der Wirtschaft (Public-Private-Partnership) und den bestehenden Cyber Sicherheitsinitiativen und Strukturen in Österreich gelegt. Es ist auch ein explizites Ziel,

die Branchen in ihrer Selbstorganisation und in ihrer Vernetzung im Bereich der Cyber Security zu unterstützen.

Der Schwerpunkt für das Jahr 2016 war das Erreichen des organisatorischen Probebetriebs. Seit dem zweiten Halbjahr 2015 nimmt das CSC die ihm übertragenen Aufgaben auf der operativen Ebene wahr, indem die interministeriellen Abstimmungen im Rahmen des IKDOK institutionalisiert wurden. Initiiert wurde auch die erforderliche Vernetzung mit allen relevanten nationalen wie internationalen Partnern.

GovCERT Austria und CERT.at

GovCERT Austria ist das nationale CERT (Computer Emergency Response Team) der öffentlichen Verwaltung und Teil des IKDOK. Als österreichischer Cyber Security Point-of-Contact (PoC) ist das GovCERT mit internationalen Organisationen und Ansprechpartnern wie der European GovCERT Group oder der Central European Cyber Security Plattform vernetzt. Angesiedelt im Bundeskanzleramt, arbeitet das GovCERT zur Wahrnehmung seiner Aufgaben eng mit dem österreichischen CERT (CERT.at) in Form einer Public-Private-Partnership (PPP) zusammen. CERT.at stellt im Zuge dieser PPP die Ressourcen für die Wahrnehmung operativer Aufgaben des GovCERT zur Verfügung und führt im Zuge dessen auch vorbeugende Maßnahmen wie Früherkennung, Öffentlichkeitsarbeit und Beratung und Unterstützung im Anlassfall auf Anfrage durch. CERT.at versteht sich als Kontaktpunkt für sicherheitsrelevante IKT-Ereignisse in Österreich und dient hier als erfahrene, vertrauenswürdige und in der Branche sowohl national wie auch international anerkannte Informationsdrehscheibe.

Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT)

Das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) schützt verfassungsmäßige Einrichtungen der Republik Österreich und deren Handlungsfähigkeit. Das BVT ist dem Charakter nach eine Sicherheitsbehörde. Es ist zuständig für die Zusammenarbeit mit ausländischen Sicherheitsbehörden und Nachrichtendiensten. Organisationsrechtlich ist es Teil der Generaldirektion für die öffentliche Sicherheit des BM.I. Die laufenden Lagebeurteilungen und Gefährdungseinschätzungen der im BVT angesiedelten Analyseeinheit, bilden eine wichtige Entscheidungsgrundlage für die strategische Leitung sowie für die Steuerung und Koordination der daraus resultierenden Personen- und Objektschutzmaßnahmen. Dadurch können präventiv potentielle Gefahren erkannt und in weiterer Folge rasch und flexibel der jeweiligen Situation angepasste Entscheidungen zur Gefährdungsreduzierung getroffen werden.

Zu den Kernaufgaben des BVT zählen die Bekämpfung extremistischer und terroristischer Phänomene, der Spionage, des internationalen Waffenhandels, des Handels mit Kernmaterial und der organisierten Kriminalität in diesen Bereichen. Das Schwergewicht im Tätigkeitsbereich des BVT liegt nach wie vor in der Bekämpfung des internationalen Terrorismus als Teil einer nationalen und gesamteuropäischen Strategie.

Heeresnachrichtenamt (HNaA)

Das Heeresnachrichtenamt (HNaA) ist für die Erarbeitung des strategischen Lagebildes vor allem in Bezug auf internationale Akteure und Entwicklungen zuständig. Der Beitrag des HNaA soll in ein gesamtstaatliches Lagebild einfließen und dient als mögliche Entscheidungsgrundlage für die oberste politische und militärische Führung. Weiters ist das HNaA für die frühzeitige Erkennung von potentiellen Cyber Bedrohungen aus dem Ausland zuständig und unterstützt im Fall eines großangelegten Cyber Angriffes auf nationale Infrastrukturen mit den zur Verfügung stehenden Methoden eine Identifikation der Angreifer.

Cyber Verteidigungszentrum (CVZ) und militärisches Computer Emergency Response Team (milCert)

Dem Auftrag des aktuellen Regierungsprogramms folgend, sowie den militärischen Erfordernissen einer leistungsfähigen militärischen Landesverteidigung im Cyber Raum entsprechend, werden die neuen Organisationseinheiten „Cyber Verteidigungszentrum" (CVZ) im Abwehramt und „militärisches Computer Emergency Response Team" (milCERT) im Führungsunterstützungszentrum und damit im Rahmen der bestehenden Organisation des BMLVS etabliert.

Während das milCERT primär für BMLVS-interne Aufgabenstellungen vorgesehen ist und maßgeblich dem Schutz der militärischen IKT-Infrastruktur dient, tragen das CVZ und das milCERT gemeinsam zur Erfüllung von gesamtstaatlichen Aufgaben des BMLVS/ÖBH im Sinne des Souveränitätsschutzes im Rahmen der Umfassenden Landesverteidigung und Umfassenden Sicherheitsvorsorge bei. Das CVZ ist auch in der Lage, Aufgaben einer operativen NIS-Behörde für Angelegenheiten, die in das Aufgabengebiet der militärischen Landesverteidigung fallen, zu übernehmen.

Cyber Crime Competence Center (C4)

Das Cyber Crime Competence Center (C4) ist die nationale und internationale Koordinierungs- und Meldestelle Österreichs zur Bekämpfung der Cyberkriminalität. Das Zentrum setzt sich aus technisch und fachlich hochspezialisierten ExpertInnen aus den Bereichen Ermittlungen, Forensik und Technik zusammen. Die Cyber Crime-Meldestelle des C4 ist zum einen die Kontaktstelle zur Bevölkerung für Cyber Kriminalität. Sie gibt per E-Mail sowie auch telefonisch Auskunft und steht bei für entsprechende Anfragen zur Verfügung. Dadurch können dort unter anderem frühzeitig neue Phänomene erkannt werden. Zum anderen ist sie auch Schnittstelle zum CSC und internationale Kontaktstelle in Cyber Crime Angelegenheiten. Eine weitere wichtige Aufgabe ist die Ansprechstelle für alle Polizeidienststellen im Zusammenhang mit Cyber Crime. Nachdem im Jahr 2014 der organisatorische und technische Aufbau abgeschlossen wurde konnte 2016 die Umsetzung des Personalkonzeptes mit 49 MitarbeiterInnen weiter vorangetrieben werden.

Cyber Sicherheit im Bundeskanzleramt

Zusätzlich zu den zuvor beschriebenen Organisationseinheiten setzt das Bundeskanzleramt selbst auch eine Reihe an Maßnahmen und Aktivitäten zur Erhöhung der Cyber Sicherheit in Österreich, insbesondere im strategischen Bereich und bei der nationalen wie auch internationalen Kooperation.

Das Bundeskanzleramt ist seit Jahren die strategische Koordinationsstelle für Cyber Sicherheit in Österreich. Es koordiniert die Erstellung, Vorbereitung und Umsetzung von Cyber Sicherheit Strategien in Österreich und ist damit eine der treibenden Kräfte für die Errichtung einer robusten nationalen Cyber Sicherheit Architektur. Das BKA hat den Vorsitz in der nationalen Cyber Sicherheit Steuerungsgruppe (CSS), wo wichtige nationale Themen der Cyber Sicherheit vorgeklärt und als Ministeratsvorträge der Regierung zur Entscheidung vorgelegt werden. Die CSS dient hat gegenüber der Bundesregierung auch eine beratende Funktion in Angelegenheiten der Cyber Sicherheit.

Als künftige strategische NIS-Behörde wird das Bundeskanzleramt seine zentrale Rolle für strategische Cyber Sicherheit in Österreichs intensivieren. Es hat damit die wichtige Aufgabe, gemeinsam mit allen Stakeholdern neue Ansätze für die Zukunft zu finden und rechtzeitig und proaktiv die notwendigen Schritte für ein tragfähiges und sicheres digitales Fundament in Österreich in die Wege zu leiten.

Eine gerade sehr aktuelle Verantwortung des Bundeskanzleramts ist die Erarbeitung eines österreichischen Cybersicherheitsgesetzes. Dafür wurde unter der Koordination des BKA eine legistische Arbeitsgruppe gegründet, die sich aus Vertretern verschiedener Ressorts zusammensetzt. Ihre Aufgabe ist die legistische Umsetzung der europäischen NIS-Richtlinie in Österreich, und die Schaffung einer gesetzliche Grundlage für alle derzeit anstehenden Themen der Cyber Sicherheit in Österreich.

Das Bundeskanzleramt vertritt Österreich in zahlreichen europäischen und internationalen Foren, stimmt österreichische Positionen interministeriell ab und bringt diese in die Gremien ein. So führte das Bundeskanzleramt für Österreich etwa die Verhandlungen über die NIS-Richtlinie der EU, war ein aktiver Mitverfasser der europäischen NIS-Strategie und ist Österreichs Vertreter in der Ratarbeitsgruppe für Cyber Angelegenheiten.

Im Zuge der Umsetzung der NIS-Richtlinie ist das BKA regelmäßiger Teilnehmer an den Treffen der NIS-Kooperationsgruppe. Diese Gruppe wurde eingesetzt um die strategische Zusammenarbeit und einen regelmäßigen Informationsaustausch zwischen den Mitgliedsstaaten der EU zu gewährleisten, um Vertrauen aufzubauen und ein hohes gemeinsames Sicherheitsniveau zu erreichen. Dies sind zentrale Anliegen der NIS-Richtlinie.

An der Arbeit der Europäischen Netzwerk und Informationssicherheit Agentur (ENISA) ist das Bundekanzleramt in vielfältiger Weise beteiligt. Es stellt nicht nur den Österreichischen Liaison Officer zur ENISAund ist damit in engstem Kontakt zur Agentur, auch ist es an etlichen Aktivitäten national und international federführend für Österreich tätig. So koordiniert das

Bundeskanzleramt etwa die Teilnahme Österreichs an der Cyber Sicherheit Awareness-Kampagne "European Cyber Security Month" und steuert und veranstaltet alle zwei Jahre die nationale Planung und Abhaltung der größten pan-europäischen Cyber Übung (Cyber Europe) zum Beübung der gesamtstaatlichen Cyber Krisenprozesse. Ein besonderer Fokus liegt dabei auf der nationalen Koordination und Kommunikation im Cyber Krisenfall, sowie der Zusammenarbeit zwischen der öffentlichen Verwaltung und der Privatwirtschaft, die auch in die Aufplasnung der Übung eingebunden wird.

Innerhalb der OSZE stellt das BKA den technischen Focal Point für Cyber Sicherheit in der Arbeitsgruppe zur Etablierung von vertrauensbildenden Maßnahmen im Cyber Space. Das Thema Cyber Sicherheit ist für Österreich, das 2017 unter der Federführung des BMEIA den Vorsitz der OSZE übernommen hat, auch dort von hoher Bedeutung.

In der OECD Arbeitsgruppe „Working Party On Security and Privacy in the Digital Economy" erstellt das BKA zusammen mit den anderen OECD Staaten Analysen und High Level Empfehlungen für Regierungen und nationale Stakeholder zu den Themen Cyber Sicherheit und Datenschutz.

In der NATO Partnership For Peace ist das BKA zusammen mit den anderen nationalen Sicherheitsressorts engagiert. Hier geht es um friedenserhaltende und friedensschaffende Missionen, aber auch um gegenseitiges Fördern von Cyber Sicherheit Kompetenzen, wie gemeinsamen Cyberübungen oder das Bereitstellen von Ausbildungsmöglichkeiten im Bereich Cyber Sicherheit.

Obwohl die Tätigkeit des Bundeskanzleramts im Bereich Cyber Sicherheit schwerpunktmäßig auf strategischer Ebene stattfindet, unterhält es mit dem österreichischen GovCERT auch eine operativ agierende Einheit. Neben der nationalen Wahrnehmung operativer Aufgabe durch das GovCERT in der Bereitstellung von CERT-Dienstleistungen für die öffentliche Verwaltung sowie als Teilnehmer im IKDOK und im CERT-Verbund, vertritt das GovCERT Österreich auch in der European Governmental CERT (EGC) Group, in dem durch die NIS-Richtlinie begründeten CSIRT-Netzwerk sowie in bi- und multilateralen Netzwerken wie zum Beispiel in der rein deutschsprachigen DACH Gruppe oder in der Central European Cyber Security Platform (CECSP), einer Gruppe aus 5 benachbarten Staaten, die sich zweimal jährlich zu Plenarsitzungen treffen und gemeinsam Cyberübungen abhalten.

Nicht zuletzt betätigt sich das BKA auch als Bedarfsträger in einer Reihe von Cyber Sicherheit Forschungsprojekten im Rahmen des Sicherheits-Förderungsprogramms KIRAS.

6. AUSTRIAN ENERGY CERT

Die österreichische Elektrizitäts- und Erdgaswirtschaft als Best Practice Beispiel zur Stärkung der IT-Sicherheitskompetenz kritischer Infrastrukturen

Die Elektrizitäts- und Erdgaswirtschaft ist ein zentraler Teil der kritischen Infrastrukturen Österreichs. Beeinträchtigungen in der Energieversorgung oder gar ein flächendeckendes Blackout aufgrund von gravierenden Cyber-Angriffen auf die IT-Systeme der Energieversorger sind potenzielle Risiken, für die es entsprechende Gegenmaßnahmen zu setzen gilt – das Austrian Energy CERT (AEC) ist eine davon. Durch die kürzlich erfolgte Gründung und dem Start der Aufbauphase des AEC setzt Österreich eine wichtige Maßnahme zur Stärkung der IT-Sicherheitskompetenz kritischer Infrastrukturbetreiber um. Ein Beispiel, das auch in anderen Sektoren Schule machen soll und auch bereits aufgegriffen wurde.

Hilfe zur Selbsthilfe im Vordergrund

Österreich setzt zur Erhöhung der IT-Sicherheit kritischer Infrastrukturen auf den Ansatz der sektoralen Kooperation und Zusammenarbeit. Durch die Schaffung organisatorischer Rahmenbedingungen in Form branchenspezifischer CERTs, wird so eine tragfähige Grundlage für die Verbesserung der IT-Sicherheit in einem Bereich der kritischen Infrastruktur Österreichs geschaffen. Deren Ziel ist es, ExpertInnen aus dem jeweiligen Sektor zu vernetzen, damit diese sich auf laufender Basis über aktuelle und potenzielle neue Gefährdungssituationen austauschen und sich besser darauf vorbereiten können. Bei branchenspezifischen CERTs steht – wie auch am Beispiel des Austrian Energy CERT ersichtlich wird – die Hilfe zur Selbsthilfe im Mittelpunkt. Denn niemand kennt die Besonderheiten und Herausforderungen einer Branche so gut, wie die jeweiligen Organisationen und Unternehmen selbst.

2016 – Beginn der Aufbauphase des Austrian Energy CERT

Diesem Grundgedanken folgend wurde Mitte 2016 das Austrian Energy Computer Emergency Response Team gegründet, das sich seit November 2016 im Aufbau befindet. Dabei handelt es sich um ein, von der österreichischen Elektrizitäts- und Erdgaswirtschaft gemeinsam betriebenes Computer-Notfallteam. Es wurde ins Leben gerufen, um die Resilienz der betroffenen Organisationen und Unternehmen gegenüber Sicherheitsvorfällen in Informations- und Kommunikationstechnologien nachhaltig zu sichern und kontinuierlich zu verbessern.

Stärkung der IT-Sicherheitskompetenz der österreichischen Elektrizitäts- und Erdgaswirtschaft

Die Hauptaufgaben des Austrian Energy CERTs dienen der Stärkung der IT-Sicherheitskompetenz der Branche. Im operativen Tagesgeschäft umfassen diese insbesondere das laufende Security Incident Management, also die Bearbeitung und Einschätzung von täglich eingehenden Anfragen und Sicherheitsmeldungen sowie die Koordination aller involvierten IT-SicherheitsexpertInnen. Neben diesen Kernaufgaben zählen noch das

kontinuierliche News- und Technologiemonitoring zur Einschätzung aktueller IT-Sicherheitsthemen, die Durchführung von Schulungstätigkeiten, die Teilnahme an nationalen wie auch internationalen Cyber-Sicherheitsübungen, Forschungsprojekten oder Workshops sowie die Mitarbeit bei der Erstellung technischer Sicherheitskonzepte für die Elektrizitäts- und Erdgaswirtschaft zum Aufgabenspektrum. Das AEC fungiert außerdem im Kontext von nationalen und internationalen Security Incidents als branchenspezifischer Single Point of Contact, um eine schnelle und effiziente Kommunikation zu gewährleisten.

Unabhängig, vernetzt und integriert

Die Etablierung des Austrian Energy CERT als branchenspezifische IT-Sicherheitsplattform ist Teil jener Maßnahmen, die im Rahmen der Umsetzung der NIS Richtlinie und der damit in Kontext stehenden Österreichischen Strategie für Cyber Sicherheit erfolgen, um die IT-Sicherheit kritischer Infrastrukturen zu erhöhen. Als Alleinstellungsmerkmale des AEC sind dabei insbesondere dessen Unabhängigkeit sowie die national wie auch international herausragende Vernetzung der IT-SicherheitsexpertInnen zu erwähnen. In der Rolle als branchenspezifisches Computer Security Incident Response Team (CSIRT) wird es dabei in weiterer Folge auch als Meldestelle für die verpflichtende bzw. freiwillige Bekanntgabe von IT-sicherheitsrelevanten Vorfällen fungieren. Weitere Vorteile ergeben sich außerdem durch die bestmögliche Integration in das nationale CERT. Das AEC befindet sich seit November 2016 in der Aufbauphase und wird voraussichtlich Mitte 2017 den Probebetrieb aufnehmen. Der Start des Vollbetriebs ist im Laufe des Jahres 2018 geplant.

Gastkommentar Ing. Mag. Stefan Wagenhofer, Vorsitz der Arbeitsgemeinschaft Austrian Energy CERT: Beweggründe aus Sicht der Elektrizitäts- und Erdgaswirtschaft

© privat

Ing. Mag. Stefan Wagenhofer
Vorsitz Arbeitsgemeinschaft Austrian Energy CERT

„Die Elektrizitäts- und Erdgaswirtschaft hat 2016 mit dem Aufbau eines brancheneigenen CERT (Computer Emergency Response Team) begonnen. Sie setzt durch die Installation des Austrian Energy CERT (AEC) einen wichtigen Schritt zur Umsetzung der Strategien zur Erhöhung der Resilienz der Energiewirtschaft gegenüber IKT-Attacken, -Gebrechen und -Fehler im Energiesektor. Die energieversorgenden Unternehmen stellen damit im Sinne ihrer Kunden einen weiteren wichtigen Baustein für die Stärkung der IKT-Sicherheit zur Verfügung und unterstützen die Ziele der Österreichischen Strategie für Cybersicherheit.
Das AEC entspricht auch den Empfehlungen der „European Union Agency for Network and Information Security" (ENISA) und den Vorgaben der europäische Netzwerk- und Informationssystemsicherheits-Richtlinie (NIS-Richtlinie).

Durch den gemeinsamen Aufbau eines brancheneigenen CERTs werden Bewusstsein und Prävention im Energiesektor gestärkt. Jedes einzelne Energieunternehmen kann im Notfall auf Experten und ein eigenes, auf Energiefragen spezialisiertes Notfallteam zugreifen.

Im AEC können bereits Vorfälle und Situationen analysiert werden, welche noch nicht in die Meldeverpflichtung der NIS-Richtlinie fallen. Damit sollen frühzeitig Entwicklungen oder Bedrohungsszenarien für den Energiesektor im Bereich IKT-Sicherheit erkennbar und die Zusammenarbeit mit Sicherheitsexperten sowie den Behörden verbessert werden.

Insbesondere durch intensiven Know-how-Austausch zwischen den Unternehmen und dem AEC, durch gegenseitiges Vertrauen und durch die Kenntnis der im Energiesektor verwendeten Systeme, ist es dem AEC möglich, auf den Sektor zugeschnittene Informationen und frühzeitige Warnungen auszusprechen. Auf dieser Basis soll die Elektrizitäts- und Erdgaswirtschaft in der Lage sein, rascher und gezielt auf Bedrohungen reagieren zu können.

Das Austrian Energy CERT wird sich in den in der Branche bereits etablierten Risikoanalyse-Prozess mit einbringen und damit insbesondere den präventiven Bereich stärken und weiter ausbauen. Dadurch werden die obersten Ziele der Branche – eine sichere Versorgung mit Energie und bestmöglichste Qualität der Versorgung – konsequent weiterverfolgt.

Besonders hervorzuheben ist die mit der Risikoanalyse etablierte Public-Private-Partnership (PPP), wodurch die Zusammenarbeit zwischen Energiesektor und den Behörden noch intensiver geworden ist. Mit dem PPP wird zudem gewährleistet, dass die geplanten, aus der Risikoanalyse abgeleiteten Maßnahmen praxistauglich und zielgerichtet sind."

Ing. Mag. Stefan Wagenhofer
Vorsitz ARGE AEC

„KraftCERT" als Best Practice Beispiel aus Norwegen

Während sich das Austrian Energy CERT derzeit im Aufbau befindet, kann sein Pendant in Norwegen bereits auf einige Jahre erfolgreicher Arbeit zurückblicken. Das so genannte „KraftCERT" wurde am 30. Oktober 2014 von den Energieunternehmen Statnett, Statkraft und Hafslund auf Basis einer Initiative von NorCERT sowie der Norwegischen Wasserressourcen- und Energiedirektion (NVE) gegründet, um die gesamte Energieindustrie bei der Prävention und Abwehr von Sicherheitsvorfällen zu unterstützen.

Gastkommentar Margrete Raaum, CEO KraftCERT: Erfahrungen aus norwegischer Sicht und Bedeutung der nationalen wie auch internationalen Zusammenarbeit

„Starting up the Norwegian energy CERT has been quite a learning curve, both for the constituents and us. The initial set of services is not the same set of services that we see a demand for today, but keeping the model open to changes has proved a success. The constituents receive support in improving both detection and incident response, and together with the utilities we push to improve the security in services delivered to the utilities from service providers. We have found that there is a need for a greater understanding of the criticality of this sector amongst many vendors.

In our daily work, we chose to focus on personal meetings for increased trust and improved information sharing, and unsurprisingly this has shown to be the right direction. We also chose to keep a steady pace and not rush neither the processes nor the utilities, and this has kept us out of trouble with growing pains. We are now ready to grow and we are currently mapping out both more resources and new services, and continuously a robust international sharing network. We already have a good collaboration with CERT.at and the energy CERT of Austria, and we are looking forward to working even closer together."

Margrete Raaum
CEO KraftCERT

Abbildung 13: Das Logo des norwegischen KraftCERT (© KraftCERT)

Weitere Informationen:

- www.energy-cert.at (Website des Austrian Energy CERT derzeit im Aufbau, Anm.)
- www.kraftcert.no (Website des norwegischen Energy CERT)

7. FRAGELISTE: WIE GEHT MEIN UNTERNEHMEN MIT SICHERHEITSPROBLEMEN UM?

Eine Auswahl wichtiger Fragen von UnternehmensentscheiderInnen an ihre IT-Verantwortlichen zur Einschätzung der IT-Sicherheitslage eines Unternehmens

Cyber Angriffe können jedes Unternehmen betreffen. Egal, ob es sich dabei um einen börsennotierten Konzern, ein mittelständisches KMU oder Ein-Personen-Unternehmen handelt. Während große Firmen für gewöhnlich über entsprechendes Know-how in eigenen IT-Abteilungen verfügen, sind vor allem Kleine und Mittlere Unternehmen häufig nur unzureichend gegen Bedrohungen aus dem Netz abgesichert – und stellen somit in den Augen von Cyber Angreifern ein vergleichsweise leichtes Ziel dar.

Diese Liste versteht sich hierbei nicht als allumfassende Aufzählung sämtlicher kritischer Bereiche, sondern will gezielt organisatorische Themen abseits der klassisch rein technisch fokussierten Maßnahmen wie etwa Backup, Passwortrichtlinien oder physikalische Sicherheit ansprechen.

Informationsfluss

- Wie und vor allem wer erfährt im Unternehmen von IT-Sicherheitsproblemen (wenn beispielsweise Dritte auf eine Sicherheitslücke gestoßen sind und diese melden wollen)?
- Gibt es dazu eine klar definierte Prozesskette, wie (Weiter-)Meldungen & Eskalationen zu erfolgen haben?
- Verfügt das Unternehmen über ein entsprechendes Social Media bzw. Medienmonitoring, um allfällige Sicherheitsvorfälle in Verbindung mit dem eigenen Firmen- oder Produktnamen selbst erkennen zu können, sobald darüber berichtet wird?

Verantwortlichkeiten

- Gibt es im Unternehmen für alle relevanten Systeme und Services klare Verantwortlichkeiten bzw. Zuständige mit entsprechenden Stellvertretungs-regelungen?
  (Hinweis: Das betrifft in diesem Kontext alles, was einem Unternehmen potenziellen Schaden zufügen kann und inkludiert insbesondere auch extern gehostete oder outgesourcte Projekt- oder Produkt-Webseiten)

Abläufe

- Wenn ein IT-Sicherheitsvorfall eingetreten ist: Gibt es entsprechende Einsatz- oder Ablaufpläne?
  (Hinweis: Idealerweise nach unterschiedlichen Kategorien sortiert; beispielsweise ob es sich um ein rein internes Problem handelt, es bereits öffentlich bekannt ist oder womöglich sogar personenbezogene Daten im Sinne des österreichischen Datenschutzgesetzes betroffen sind).

Erreichbarkeit

- Ist die Erreichbarkeit der wichtigsten Unternehmensbereiche (beispielsweise Geschäftsführung, IT/Technik, Presse/PR) auch außerhalb der Bürozeiten sichergestellt?

Vertrauenswürdigkeit externer Dienstleister

- Sind alle extern zugekauften Dienstleistungen (von Co-Location bis hin zur Cloud) mit entsprechenden Security Service-Level-Agreements (SLA) versehen, als vertrauenswürdig einzustufen und verfügen die Dienstleister über eine entsprechende Zertifizierung (zB ISO 27001)?

Versicherung

- Welche IT-Risiken eines Unternehmens sind prinzipiell versicherbar?
- Bei welchen könnte das aus Sicht des Unternehmens auch wirtschaftlich vernünftig sein?

Eigene Zertifizierung

- Was wäre der Aufwand einer IT-Security-Zertifizierung (zB ISO 27001) und was der potenzielle Nutzen aus Sicht des Unternehmens (zB aus Sicht von IT, Marketing, neuen Auftragsmöglichkeiten etc.)?

Kritische Infrastruktur & Auswirkungen der europäischen NIS-Richtlinie

- Wie ist das Unternehmen auf die Anforderungen der europäischen NIS-Richtlinie (siehe Kapitel 4) und der damit verbundenen nationalen Umsetzung vorbereitet?
- Ist das Unternehmen womöglich selbst der "kritischen Infrastruktur" zuzuordnen?

Investitionen

- Wieviel Aufwand (sowohl personell wie auch finanziell) wird derzeit in IT-Security-Themen investiert?
- Wie ist das Verhältnis von reiner Angriffs-Abwehr (Prävention) zu Erkennung erfolgreicher Angriffe (Detection) im Unternehmen?

Verhaltensregeln

- Gibt es im Unternehmen klare Richtlinien zu Privatnutzung, Verhaltensregeln und Themen wie Smartphones/Tablets und BYOD (Bring Your Own Device, Anm.)?
- Kann jedes Gerät im Unternehmensnetzwerk (inkl. BYOD) einem Benutzer bzw. einem Verantwortlichen zugeordnet werden und ist sichergestellt, dass alle Geräte (insb. auch BYOD) auf aktuellem Stand und entsprechend sicher konfiguriert sind?

Sollten im Zuge der Beantwortung dieser Fragen Unklarheiten oder weitere offene Fragen auftauchen, empfehlen CERT.at und GovCERT.gv.at den Unternehmen jedenfalls, sich intern wie auch extern – beispielsweise durch externe IT-SicherheitsexpertInnen – näher mit dem Thema IT-Sicherheit zu befassen.

Neben jenen Maßnahmen, die zur Prävention von IT-Sicherheitsvorfällen gesetzt werden, sind darüber hinaus auch Maßnahmen (Investitionen und personelle Ressourcen) in die Angriffserkennung („Detection“) sowie die proaktive Systemwartung und Vorfallsbehandlung („Remediation“) von hoher Bedeutung.

8. 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 neun Personen und wird von Robert Schischka geleitet.

Abbildung 14: Das 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 Cyber Sicherheit 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 eines Cyber Angriffs, sofern kein anderes CERT (etwa ein Branchen-CERT, so wie z.B. das Austrian Energy CERT für den Energiesektor) 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 15: Das 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 Stakeholder und 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 Austrian 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 der 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, 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
- Digitales Österreich: http://www.digitales.oesterreich.gv.at
- www.cert.at und www.govcert.gv.at

9. GLOSSAR

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
CHARGEN	Character Generator Protocol
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

Abkürzung	Erklärung
ENISA	Europäische Agentur für Netzwerksicherheit
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-Richtlinie	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

Abkürzung	Erklärung
SMTP	Simple Mail Transfer Protocol
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

10. ABBILDUNGSVERZEICHNIS