BERICHT INTERNET-SICHERHEIT ÖSTERREICH 2013

GovCERT AUSTRIA

CERT.at

Staatssekretär
Dr. Josef Ostermayer

VORWORT

Informations- und Kommunikationstechnologien sind in Österreich und international ein bedeutender Faktor für Wirtschaftswachstum und Beschäftigung. Entscheidend ist, dass Wirtschaft, Verwaltung und Politik in diesem Bereich eng zusammen arbeiten.

Die Vorteile der digitalen Gesellschaft, in der wir leben und arbeiten, sind heutzutage nicht mehr weg zu denken. Obwohl in den letzten Jahren die Zahl jener Menschen, die über einen Internetanschluss verfügen, enorm gestiegen ist, verfügt noch rund ein Fünftel der österreichischen Bevölkerung über keinen Zugang zum Internet. Durch entsprechende Maßnahmen, wie z.B. den weiteren Ausbau im Breitband-Internetbereich, soll jeder Österreicherin und jedem Österreicher die Möglichkeit geboten werden, von der digitalen Vernetzung zu profitieren.

Vor allem die Jüngeren in unserer Gesellschaft wachsen bereits mit Möglichkeiten, aber auch Gefahren auf, mit denen sich davor noch keine Generation auseinandersetzen musste. Einen sicheren, kompetenten und verantwortungsvollen Umgang mit digitalen Medien zu lernen ist eine der aktuellen Herausforderung für Kinder, Jugendliche, aber auch für deren Eltern.

Umfangreiche Vernetzung hat auch ihre Schattenseiten. Bedrohungen und Angriffe über das Internet haben in jüngster Vergangenheit stark zugenommen. So sehr unsere digitale Gesellschaft auch mit Vorteilen verbunden ist, eröffnen sich doch auch Problembereiche und die damit verbundene Frage, wie Wirtschaft, Politik und auch Konsumentinnen und Konsumenten mit negativen Entwicklungen umgehen sollen.

Daher richtet die Bundesregierung – gemeinsam mit den Expertinnen und Experten von CERT.at und GovCERT.gv.at – neben den Chancen für die Bürgerinnen und Bürger den Blick vor allem auch auf Bedrohungen und Gefahren, die das Internet mit sich bringt.

Seit Herausgabe des ersten Internet-Sicherheitsberichts 2010, hat sich auch in Österreich sehr viel auf diesem Gebiet getan. So sind das Computer Emergency Response Team (CERT.at), sowie GovCERT.gv.at für den öffentlichen Bereich, gemeinsam mit dem Bundeskanzleramt und führenden Vertreterinnen und Vertretern aus relevanten, kritischen Infrastrukturbereichen in die Entwicklung einer nationalen Cyber Security Strategie für Österreich eingebunden.

Nur durch einen ganzheitlichen Zugang und eine breite Einbindung aller relevanten Beteiligten, aus dem öffentlichen wie auch aus dem privaten Bereich, sind wir in der Lage, die richtigen Maßnahmen für Sicherheit im Internet zu setzen.

Dr. Josef Ostermayer
Staatssekretär im Bundeskanzleramt

CYBER SECURITY – DIE UNSICHTBARE SICHERHEIT IM ALLTAG

Würde man die Internet-Sicherheitslage in Österreich und der Welt ausschließlich anhand der Berichterstattung in den Medien beurteilen, so zeichnete sich ein düsteres Bild. 2013 wird als Jahr in die Geschichtsbücher eingehen, das massiv von Spionage, Internet-Kriminalität und Bedrohungen aus dem Netz geprägt war. Große Phänomene, die ebenso große Schatten auf unsere zunehmend durch Vernetzung geprägte Gesellschaft werfen.

Doch es gibt auch Lichtblicke: Sicherheit im Allgemeinen und Internet-Sicherheit im Besonderen sind Themenbereiche, die durch die jüngsten Ereignisse stärker denn je in den Fokus der Aufmerksamkeit gerückt sind. Weltweit arbeiten Wirtschaft, Politik und Behörden gemeinsam an Lösungen, wie die Sicherheit im Internet für AnbieterInnen und AnwenderInnen gleichermaßen erhöht werden kann.

Querschnittsmaterie Internet-Sicherheit

Österreich verfügt mit dem nationalen Computer Emergency Response Team (CERT.at) für den Unternehmens- und mit GovCERT Austria für den Behördenbereich (GovCERT.gv.at) über zwei etablierte Organisationen, die bereits seit 2008 eine aktive Rolle im Kampf gegen Bedrohungen aus dem Internet einnehmen. Die Strukturen und Informationskanäle, die Österreich in den letzten Jahren aufgebaut hat, bilden heute die Grundlage für eine ganzheitliche Betrachtung des Themas Internet-Sicherheit. CERT.at und GovCERT.gv.at sehen sich dabei als verbindendes Element einer Querschnittsmaterie, die alle Teile des öffentlichen wie privaten Leben in Österreich gleichermaßen betrifft.

Die „Internet-Feuerwehr“ Österreichs

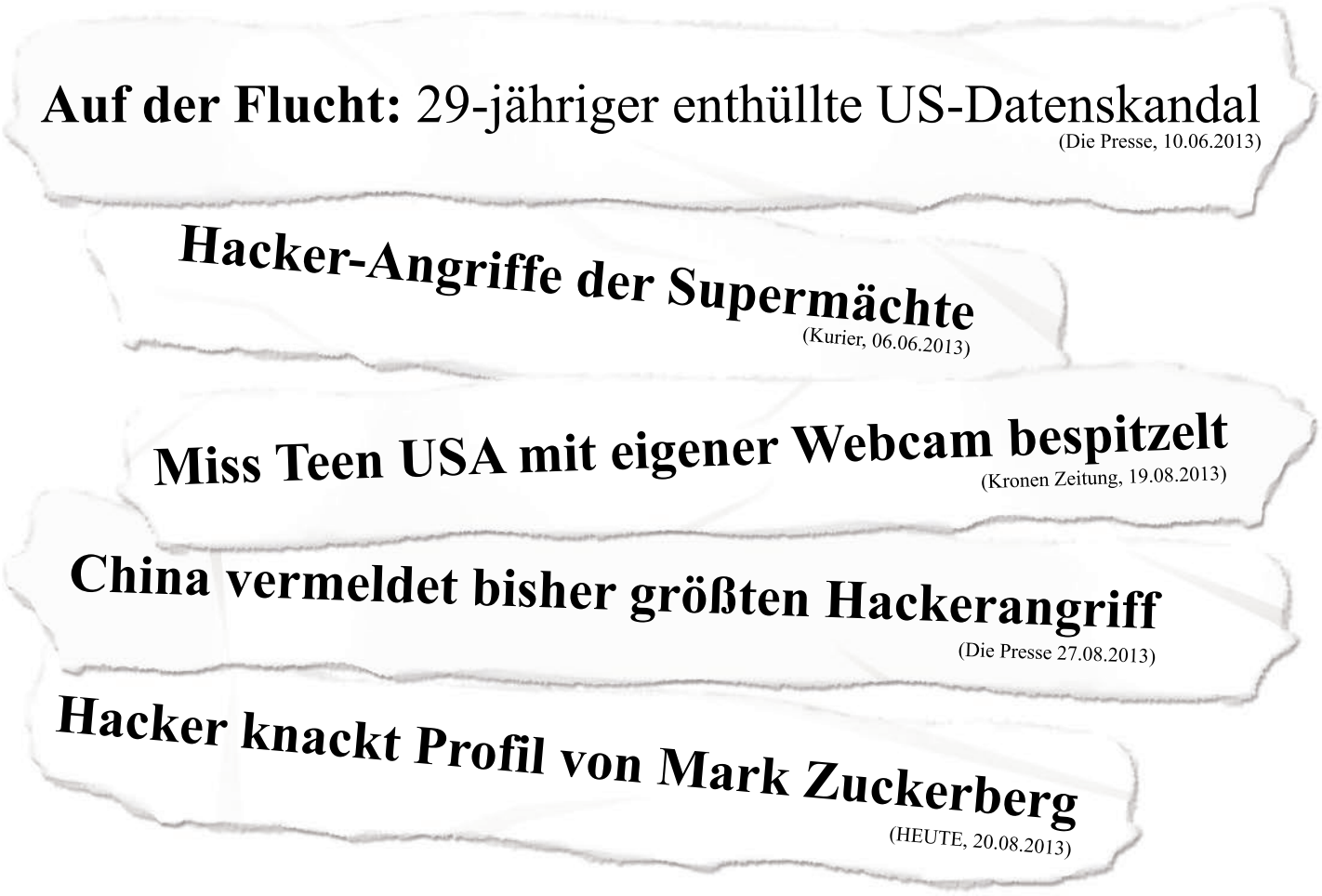
Neben unmittelbarer Hilfe bei akuten Bedrohungen aus dem Internet setzen die ExpertInnen der „Internet-Feuerwehr“ CERT.at und GovCERT.gv.at auch stark auf Maßnahmen im Bereich der Bewusstseinsbildung und Prävention. Denn Sicherheit ist ein unsichtbares Gut. Sie bekommt immer erst dann die nötige Aufmerksamkeit, wenn sie fehlt – und es meistens schon zu spät ist. Mit dem aktuellen Internet-Sicherheitsbericht 2013 geben wir eine Einschätzung der aktuellen IT-Sicherheitslage in Österreich ab und wagen außerdem einen Ausblick auf jene Themen, die das Land und die Welt in Zukunft maßgeblich im Bereich der Cyber Security betreffen werden.

Robert Schischka, Leiter von CERT.at

Roland Ledinger, Leiter des Bereiches IKT-Strategie des Bundes im Bundeskanzleramt

INHALT

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 (MARKUS GRUBER, STEFANIE BRAMBÖCK) **GRAFIK:** CREATIVEDIRECTOR.CC LACHMAIR GMBH. **VERLAGS- UND HERSTELLUNGSORT:** WIEN. NOVEMBER 2013



IM FOKUS: INTERNET-SICHERHEIT BETRIFFT UNS ALLE

ExpertInnen sind sich einig: Die Bedrohung aus dem Internet nimmt zu. Staaten, Organisationen und BürgerInnen sind verstärkt Ziele von Cyber Angriffen.

„Sie haben keine Ahnung, was alles möglich ist." Mit diesem Satz ging Whistleblower Edward Snowden im Juni 2013 an die Öffentlichkeit und sprach erstmals über die Ausmaße der umfassenden und systematischen Überwachungs- und Spionagepraktiken von amerikanischen und anderen Geheimdiensten.

Die Enthüllungen von Snowden führten weltweit zu einer verstärkten öffentlichen Diskussion über Internet-Spionage und Cyber Crime[1]. Seither sind Überwachungsprogramme wie PRISM, sowie die systematische und umfassende Überwachung von Internet-BenutzerInnen und ihrer Daten Bestandteile des Diskurses über Internet-Kriminalität. Es war dies der öffentliche Beweis

[1] Unter Cyber Crime wird die kriminelle Nutzung von Informations- und Kommunikationstechnik verstanden.

dafür, dass hinter Internet-Spionage und -Überwachung nicht nur Einzeltäter, erfahrene Hacker, oder kriminelle Banden und Organisationen stehen, sondern auch staatliche und politische Akteure. Die Risiken reichen mittlerweile von der Überwachung privater Bankkonten, über Unternehmens- und Wirtschaftsspionage bis hin zur Bedrohung ganzer Staaten. Die Angreifer verfolgen verschiedenste Ziele und verwenden dabei ein kaum überschaubares Arsenal an Tools und Techniken. Die sich aus Cyber Crime und Cyber Spionage ergebenden Bedrohungen für Institutionen, Unternehmen und Menschen sind längst Realität geworden, und nehmen in ihrer Intensität stetig zu.

Hackerangriffe im Mittelpunkt medialer Berichterstattung

Auch der Blick auf vergangene Schlagzeilen österreichischer Medien spiegelt das breite Spektrum des Themas Cyber Sicherheit wider. Dabei standen vor allem Hackerangriffe im Mittelpunkt der Berichterstattungen.

Im Mai 2013 wurde eine österreichische Bank Opfer eines Hackerangriffes, bei dem Aktivitäten-Protokolle von Onlinebank-KundInnen angegriffen und eingesehen wurden. Wie viele der hunderttausenden Online-KundInnen während der insgesamt dreitägigen Attacke betroffen waren, wurde nicht bekanntgegeben. Auch eine österreichische Interessenvertretung wurde im März dieses Jahres Opfer des Online-Kollektivs Anonymous Austria (AnonAustria). Über den Twitter-Account @AnonAustria wurden Namen und E-Mail-Adressen von tausenden Mitgliedern veröffentlicht, die Website der Interessenvertretung war stundenlang nicht erreichbar.

Im September 2013 wurde bekannt, dass es in den vergangenen Jahren einen massiven Hackerangriff auf den Server eines österreichischen Verlages gegeben hatte. So sollen Millionen Datensätze mit KundInnen- und Verkaufsdaten geknackt worden sein. Auch Livingsocial, der Schnäppchen-Dienst von Amazon, war Gegenstand österreichischer Zeitungsschlagzeilen. 50 Millionen der insgesamt 70 Millionen KundInnen von Livingsocial waren betroffen und es wurden Namen, E-Mail-Adressen, Geburtsdaten und verschlüsselte Passwörter abgegriffen und gehackt.

Nicht nur Unternehmen und KonsumentInnen, sondern auch Regierungen und Staaten sind den Angriffen von Hackern ausgesetzt. So berichtete das belgische Außenamt von einem Lauschangriff, bei dem die Computersysteme mit Spionagesoftware infiltriert wurden. In Südkorea wurden Hackerangriffe auf mehrere Fernsehsender und Banken bekannt. Auch China wurde im August 2013 Opfer des nach eigenen Angaben bisher größten Hackerangriffes auf chinesische Websites. Rund acht Millionen Seiten waren stundenlang nicht erreichbar.

Beliebtes Ziel von Hackern sind auch berühmte Persönlichkeiten. In den USA und auch hierzulande sorgte der Fall der „Miss Teen USA“ für Schlagzeilen. Die 19-Jährige wurde durch ihre eigene Webcam bespitzelt und anschließend mit Fotos erpresst. Auch Berichte über gehackte E-Mail-Konten der Familie der ehemaligen US-Präsidenten George W. Bush und George H. Bush „zierten“ österreichische Medien.

Welche Motive stecken hinter den Angriffen?

Zum Schutz vor Angriffen aus dem Internet ist es notwendig, sich mit den unterschiedlichen Einfallstoren, Motiven und Techniken zu beschäftigen. Nur so können adäquate und ef-

fektive Sicherheitsvorkehrungen und Maßnahmen getroffen werden. Das World Economic Forum (WEF) teilt Cyber Risiken in fünf Kategorien ein, die Auskunft über Motiv und Ursprung eines Cyber Angriffes geben. Diese fünf Kategorien sind: „Hacktivism", Wirtschaftsspionage, regierungsgetriebene Angriffe, Terrorismus und Betrug.[2]

Das Phänomen „Hacktivism" zielt insbesondere auf das Erreichen einer medialen Aufmerksamkeit. Weitere Motive von Hackern sind das Aufdecken von Sicherheitslücken, der Kampf gegen die angebliche Beherrschung des Internets durch Behörden und Unternehmen und weitere politische Ziele. Wirtschaftsspionage bezeichnet die illegale Beschaffung und Verwertung von Unternehmensinformationen und -daten. Regierungsgetriebene Angriffe werden auf Grund von politischen Interessen an Staatsgeheimnissen ausgeführt. Und Staaten nutzen Computerprogramme als Waffen gegen andere Nationen. Auch globale Terrororganisationen nutzen das Internet zunehmend für die Ausbildung und Rekrutierung zukünftiger Mitglieder. Die größte Bedrohung für Privatpersonen im Internet stellt aktuell jedoch kommerzieller Betrug dar – sehr verbreitet sind etwa Betrugsfälle durch Pishing und im Versandhandel sowie Ransomware.
Internet-Kriminelle sind heute international vernetzt und agieren verstärkt arbeitsteilig. Schadprogramme oder komplette kriminelle Infrastrukturen werden in Foren einer Untergrundwirtschaft zum Verkauf oder Miete (Software-as-a-service/Malware-as-a-service) angeboten. Die technische Abwicklung von Spam-Kampagnen erfolgt über Schwarzmärkte, in denen mit Infrastruktur zum Spamversand und auch mit Listen von E-Mail-Adressen gehandelt wird. Hacker und vor allem Spammer sehen sich zunehmend als Geschäftsleute in diesem immer lukrativer werdenden Markt.

Sicherheitsbewusstsein noch immer gering

Trotz der auch medial kommunizierten Cyber Angriffe ist das Sicherheitsbewusstsein – insbesonders im Umgang mit mobilen Endgeräten – sehr gering. Dieser Leichtsinn öffnet Cyber Crime Tür und Tor. Die Hälfte der Smartphone- und Tablet-BenutzerInnen verwendet keine Passwörter, Sicherheitssoftware oder Backup-Systeme und etwas mehr als die Hälfte der NutzerInnen weiß nicht, dass es auch für mobile Geräte bereits Sicherheitssysteme und -produkte gibt. Dies ist insbesondere bedenklich, da bereits 49% der Menschen ihre mobilen Geräte sowohl privat als auch in der Arbeit nutzen.

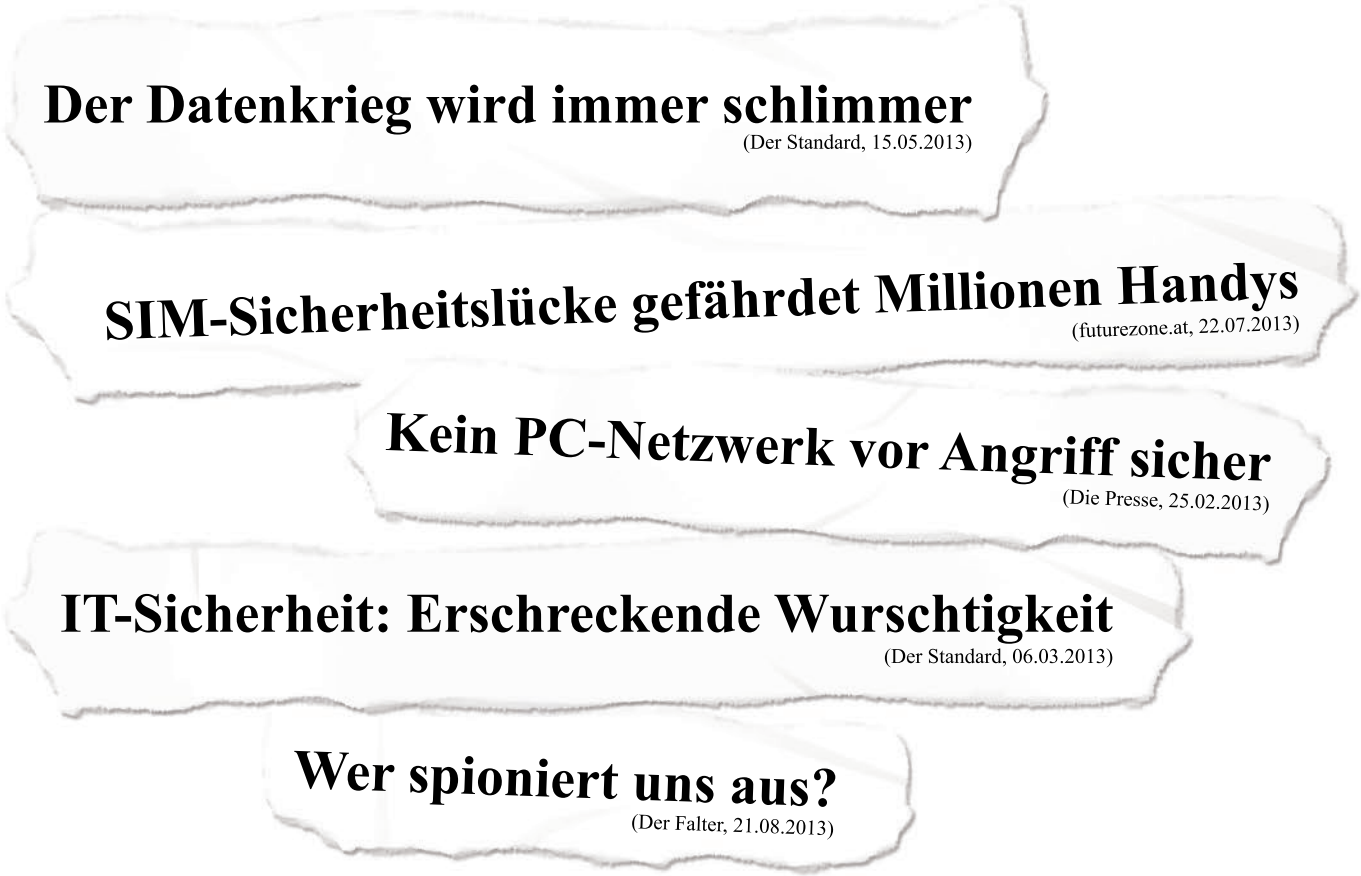
Viele BürgerInnen gehen noch sehr sorglos mit den neuen digitalen Kommunikationsmedien um. Insbesondere Jugendliche vertrauen hinsichtlich des Datenschutzes den BetreiberInnen sozialer Netzwerke. Nur jede/r zweite 10- bis 18-Jährige/r hat an ihren/seinen Datenschutzeinstellungen bereits einmal etwas geändert. Wobei sich hier langsam eine Trendwende abzeichnet und Jugendliche beginnen, vorsichtiger zu werden.

Auch viele Unternehmen verwenden veraltete Software und tauschen diese, trotz Kenntnis über deren Schwachstellen, nicht aus. Auch bei Webauftritten besitzt Sicherheit noch keine Priorität und allzu oft siegt bei der Wahl von Webhostern der Preis über die Qualität. Jedoch wären mit dem Einsatz der richtigen Schutzsoftware, regelmäßigen externen Audits, sowie durch Information und Schulung der MitarbeiterInnen viele Angriffe auf Unternehmen vermeidbar.

Internationale Strategien und Zusammenarbeit sind nötig

Der Kampf gegen Kriminalität im Internet wird zu einer Schlüsselfrage der digitalen Informationsgesellschaft. Der Schutz von kritischer Infrastruktur – dazu zählen etwa Energieversorgung, Finanzwesen, Krankenhäuser oder

[2] World Economic Forum: Risk and Responsibility in a Hyperconnected World. Pathways to Global Cyber Resilience, 2012



das Internet an sich – muss gewährleistet sein, da ihr Ausfall durch Cyber Attacken zu weitreichenden Schäden und schweren Beeinträchtigungen der modernen Gesellschaft führen würden.

Die Sicherung der digitalen Infrastruktur und der Schutz vor Cyber Angriffen und Internet-Spionage gewinnen auch als Standort- und Wettbewerbsfaktor zunehmend an Bedeutung. Der jährliche Schaden, der auf Internetkriminalität zurückzuführen ist, wird allein in Österreich auf mehr als sechs Millionen Euro geschätzt. Allein im ersten Halbjahr 2013 wurden in ganz Österreich über 6.400 Delikte im Bereich der IT-Kriminalität zur Anzeige gebracht.[3] Der weltweite Schaden wird von Interpol auf mehr als 750 Milliarden Euro geschätzt. Täglich werden ca. 1 Million Menschen Opfer von Internetkriminalität.[4]

Die internationale Zusammenarbeit und der Austausch von bewährten Verfahren sind notwendig, um die Sicherheit der digitalen Infrastruktur nachhaltig zu gewährleisten. Kein Staat und kein Unternehmen kann dies alleine bewerkstelligen. Effektive Strategien und Maßnahmen müssen sowohl innerhalb von Institutionen als auch länderübergreifend wirken.

Cyber Security braucht Eigenverantwortung

Cyber Crime und Cyber Security betreffen uns daher alle. Jeder Computer und jedes internetfähige Device kann zur Angriffsfläche oder potenziellen -waffe werden, mit oder ohne Willen der BesitzerInnen. Dies bedeutet aber auch, dass jede und jeder Einzelne einen Beitrag zu mehr Sicherheit im Netz leisten kann. Neben der Weiterentwicklung von Strategien, Prozessen und Produkten für Cyber Security ist auch die Eigenverantwortung der Behörden, Unternehmen und BürgerInnen ein notwendiger Bestandteil eines effektiven Sicherheitssystems. Es geht darum, bereits frühzeitig Bewusstsein für Sicherheitsthemen zu schaffen und zu stärken, sowie über Risiken, Lösungen aber auch Chancen zu diskutieren. Vor allem Jugendlichen, die die zukünftigen BenutzerInnen, EntwicklerInnen und BetreiberInnen dieser Infrastrukturen sind, muss sehr früh ein Bewusstsein für den sicheren Umgang mit dem Internet mitgegeben werden. Denn Cyber Security kann es nur im Zusammenspiel mit dem informierten und selbstbestimmten Umgang mit neuen digitalen Kommunikationsmedien geben.

[3] Bundesministerium für Inneres, Bundeskriminalamt Österreich: Kriminalstatistik 2013
[4] 2013 Norton Report

IM GANZEN: ÖSTERREICHISCHE STRATEGIE FÜR CYBER SICHERHEIT

Die moderne vernetzte Gesellschaft von heute eröffnet uns eine Vielzahl von Chancen und Möglichkeiten. Um diese Vorteile nutzen zu können, braucht es eine verlässlich und sicher funktionierende digitale Infrastruktur. Die Gewährleistung von Sicherheit im Cyber Raum ist in diesem Zusammenhang eine zentrale, gemeinsame Herausforderung für Staat, Wirtschaft und Gesellschaft. Internet-Kriminalität, Wirtschafts- und Industriespionage sowie immer aggressiveren Bedrohungen aus dem Netz lassen sich längst nicht mehr durch Einzelmaßnahmen Einhalt gebieten. Vielmehr erfordern die hohe Dynamik sowie die Vielfalt an Angriffs- und Bedrohungsformen ein gemeinsames, koordiniertes Vorgehen – sowohl auf österreichischer als auch internationaler Ebene.

Weitere Informationen sowie den Bericht "Nationale IKT-Sicherheitsstrategie Österreich" auf www.digitales.oesterreich.gv.at

Die ÖSCS steht unter www.bka.gv.at zum Download bereit.

Bundeskanzleramt im Zeichen von Cyber Sicherheit

Die nationale und internationale Absicherung des Cyber Raums ist eine der obersten Prioritäten Österreichs und nimmt daher auch im Bundeskanzleramt einen hohen Stellenwert ein. Mit der Entwicklung der Nationalen IKT-Sicherheitsstrategie für Österreich (2011) und in weiterer Folge der Österreichischen Strategie für Cyber Sicherheit (2013) wurden entscheidende Weichenstellungen für die Sicherheit Österreichs im digitalen Raum gesetzt.

Ausgangspunkt IKT-Sicherheitsstrategie Österreich

Das Bundeskanzleramt hat aufgrund seiner Koordinationsrolle in enger Zusammenarbeit mit anderen Ministerien im November 2011 den Startschuss für die größte Cyber Sicherheits-Initiative in Österreich gegeben. Rund 130 TeilnehmerInnen aus relevanten Bereichen des privaten wie auch öffentlichen Sektors haben in monatelanger Arbeit in fünf Arbeitsgruppen Antworten auf aktuelle Cyber Security Fragen erarbeitet. Im Fokus der Arbeitsgruppen standen Themen wie Awareness, kritische Infrastrukturen, Bildung und Forschung, Stakeholder und Strukturen, sowie Risikomanagement. Für diese wurde der jeweilige Status Quo erhoben und strategische Ziele, Strukturen und Maßnahmen daraus abgeleitet. Die Ergebnisse wurden anschließend in der Nationalen IKT-Sicherheitsstrategie Österreich zusammengefasst.

Weiterentwicklung zur Österreichischen Strategie für Cyber Sicherheit

Aufbauend auf den zahlreichen Initiativen, Maßnahmen und Umsetzungsplänen von BKA, BM.I, BMLVS und BMeiA erfolgte im September 2012 der Startschuss für die Erarbeitung einer ganzheitlichen Österreichischen Strategie für Cyber Sicherheit (ÖSCS). Die Österreichische Sicherheitsstrategie, die Nationale IKT-Sicherheitsstrategie sowie die von BM.I/KSÖ ausgearbeiteten Cyber Security Ansätze lieferten maßgebliche Inhalte für die Entwicklung der ÖSCS. Weitere Inputs kamen auch aus den strategischen Studien der ENISA und OECD. Im März 2013 wurde die ÖSCS schließlich im Ministerrat verabschiedet.

Handlungsfelder, Maßnahmen und Aktionen

Anhand von sieben zentralen Handlungsfeldern wurden im Rahmen der ÖSCS 15 Maßnahmen mit 38 Aktionen entwickelt, die schrittweise seit dem Frühjahr 2013 umgesetzt werden. Aktuell liegen die Schwerpunkte vor

allem in der Schaffung einer Struktur auf operationaler Ebene, der Gestaltung eines ordnungspolitischen Rahmens, der Entwicklung einer Plattform sowie der Erarbeitung einer integrierten Sicherheitskommunikationsstrategie.

Sensibilisierung auf mehreren Ebenen

Die im Rahmen der ÖSCS entwickelten Maßnahmen und Aktionen, die sich derzeit in Umsetzung befinden, sollen vor allem zu einer Sensibilisierung für Cyber Sicherheitsthemen auf mehreren Ebenen beitragen – insbesondere bei den BürgerInnen. Die hohe Komplexität und technologische Dimension von Cyber Sicherheit führen auf Seite der AnwenderInnen oft zu Verwirrung und Abschreckung. Für eine nachhaltige Sensibilisierung der BürgerInnen ist es daher essenziell, Komplexität zu reduzieren und Informationen anwenderfreundlich aufzubereiten.

IKT-Sicherheitsportal bietet Rat und Hilfe gegen Cyber Kriminalität

Mit dem IKT-Sicherheitsportal wurde bereits eine erste, zentrale Maßnahme im Rahmen der IKT-Sicherheitsstrategie erfolgreich umgesetzt. Auf www.onlinesicherheit.gv.at finden KonsumentInnen, Eltern, Kinder und Jugendliche aber auch UnternehmerInnen, Lehrende und SeniorInnen aktuelle Informationen, wie sie sich gegen die wachsende Internetkriminalität schützen können. Im Zentrum stehen Tipps für sicheres Surfen, der Schutz der Privatsphäre, Urheberrecht und Infos über versteckte Kosten im Netz. Ergänzt werden diese Inhalte um Erklärungen zu Cyber Mobbing, Einkäufen über das Internet und viele weitere Themen mehr. Unternehmen und die öffentliche Verwaltung erhalten außerdem Informationen zur Sicherheit bei Software-Entwicklung und zum Schutz ihrer IT-Infrastruktur.

EU-Strategie für ein offenes, freies und chancenreiches Internet

Auch auf europäischer Ebene ist Internet-Sicherheit ein bestimmendes Thema. Mit der

> *Der Schutz des Cyber Raums ist zu einer der wichtigsten Aufgaben unserer Zeit geworden.*

Cyber Sicherheitsstrategie hat die EU Anfang 2013 dargelegt, wie die europäischen Werte der Freiheit und Demokratie gefördert und die digitale Wirtschaft auf Basis einer sicheren Grundlage weiter wachsen kann. Die EU-Strategie beinhaltet konkrete Maßnahmen zur Erhöhung der Widerstandsfähigkeit der Informationssysteme im Cyber Raum, zur Eindämmung von Cyber Kriminalität, zur Stärkung der internationalen Cyber Sicherheitspolitik sowie der Cyber Verteidigung der EU.

Zur Umsetzung der EU-Strategie hat die EU-Kommission einen Vorschlag für eine begleitende Richtlinie zur Netz- und Informationssicherheit (NIS) veröffentlicht. Diese zielt auf den Aufbau von gemeinsamen Sicherheitsstandards sowie eines europäischen Frühwarnsystems und Kooperationsnetzes ab. In den Mitgliedsländern soll es künftig eigene, für NIS zuständige Behörden geben. Außerdem hat jeder Staat eigene NIS-Strategien sowie nationale NIS-Kooperationspläne auszuarbeiten, die in einen übergreifenden Plan auf europäischer Ebene einfließen.

Mit einer Verabschiedung der Richtlinie durch EU-Parlament und -Rat ist 2014 zu rechnen. Die NIS-Richtlinie setzt mit den verankerten Regelungen auch Meilensteine für die Umsetzung der Österreichischen Strategie für Cyber Sicherheit. Österreich hat bereits bei der Erstellung der Strategie auf die sich abzeichnenden europäischen Entwicklungen im Cyber Security Bereich Rücksicht genommen. Somit ist gewährleistet, dass Österreich bereits heute mit den wesentlichen Grundelementen der NIS-Richtlinie konform ist.

Webtipps

IKT-Sicherheitsportal:
www.onlinesicherheit.gv.at

Digitales Österreich:
www.oesterreich.gv.at

Infos zu EU-Sicherheitsthemen:
www.eu-info.tradepress.eu

IM PORTRAIT: CERT.AT UND GOVCERT.GV.AT

CERT.at – die österreichische Internet-Feuerwehr

CERT.at ist das österreichische Computer Emergency Response Team (CERT) und wurde 2008 gemeinsam mit GovCERT.gv.at vom Bundeskanzleramt in Kooperation mit nic.at eingerichtet. Die klassischen Aufgaben eines Computer Emergency Response Teams sind mit jenen einer Feuerwehr vergleichbar: Das CERT wird in erster Linie bei akuten Sicherheitsbedrohungen und Ereignissen aktiv. Dies geschieht durch Verständigung seitens betroffener Stellen oder auf Basis eigener Recherchen. Auch Meldungen über Sicherheitsprobleme von Dritten nimmt CERT.at gerne entgegen ("responsible disclosure").

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 (7 FTE) und wird von Robert Schischka geleitet.

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. Zusätzlich bearbeitet CERT.at alle eingehenden Meldungen über sicherheitsrelevante Vorkommnisse und entscheidet anlassbezogen über die weitere Vorgehensweise.

> *„CERT.at und GovCERT.gv.at sind Feuerwehr, und nicht die Polizei im Internet."*

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

GovCERT.gv.at – die SpezialistInnen im Behördenbereich

GovCERT.gv.at ist das österreichische Government Computer Emergency Response Team. Es fungiert als Schnittstelle zwischen öffentlicher Verwaltung und kritischen Infrastrukturen und übt dabei eine koordinierende als auch operative Funktion aus. GovCERT.gv.at ist sowohl nationale Informationsdrehscheibe als auch Point of Contact für die internationale Vernetzung. Zu den wichtigsten Aufgaben gehören

die Bündelung der sicherheitstechnischen Expertise für den Bereich der öffentlichen Verwaltung, Präventivmaßnahmen, die Sammlung und Bewertung von sicherheitstechnischen Vorfällen sowie bei Bedarf auch Unterstützungsleistung vor Ort. In der Umsetzung arbeitet GovCERT.gv.at eng mit CERT.at zusammen. Laufende Schulungen, die Koordination von themenspezifischen Arbeitsgruppen, aber auch permanente Defacement-Checks von .gv.at Domains sowie regelmäßige Awareness-Maßnahmen zählen zu den wichtigsten Aktivitäten von GovCERT.gv.at Eine zentrale Rolle spielt GovCERT.gv.at auch beim Auf- und Ausbau des nationalen CERT-Verbunds sowie bei der Koordination und Teilnahme an nationalen und internationalen Cyber Exercises.

GovCERT AUSTRIA

Wichtige Player der Österreichischen Strategie für Cyber Sicherheit (ÖSCS)

Eine effektive Cyber Sicherheitsstrategie bedarf eines dichten und qualitativ hochwertigen Netzwerkes aller Cyber Security Stakeholder und Strukturen. Dazu gehört auch die Einrichtung eines starken und umfassenden Cyber Security Krisenmanagements. Im Rahmen der ÖSCS agieren CERT.at und GovCERT.gv.at als relevante Krisenmanagementstellen, 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, Energie, öffentlicher Verkehr).

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 Security Incidents nur koordinierend und beratend aktiv werden. Das bedeutet auch, dass CERT.at keine Daten mitlesen kann.

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 Fall des Falles eingreift und in enger Abstimmung mit anderen Beteiligten den österreichischen Teil des Internets von Problemen befreit – auf Basis eines freiwilligen Angebots.

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 Internet-Sicherheit in Gesellschaft und Politik.

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.gv.at und des BMLVS ein österreichischer CERT-Verbund ins Leben gerufen. Im Mittelpunkt der Zusammenarbeit stehen der Schutz von IKT-Infrastrukturen, der Informationsaustausch und die rasche Reaktion auf Bedrohungen. Im Rahmen einer Kooperation arbeiten öffentliche Verwaltung und Privatwirtschaft eng zusammen, um eine ganzheitliche Sichtweise im Kampf gegen Cyber Bedrohungen zu entwickeln. Mitglieder des CERT-Verbunds sind neben GovCERT.gv.at und CERT.at unter anderem das ACOnet CERT, das Raiffeisen-IT CERT, das Bundesrechenzentrum, das WienCERT, das BMLVS und das A1-CERT. Durch die Zusammenarbeit soll nicht nur die Qualität der Services steigen, sondern auch ein für den möglichen Ernstfall relevanter Wissensvorsprung aufgebaut werden.

IM DETAIL: ZAHLEN, DATEN UND FAKTEN ZUR INTERNET-SICHERHEIT ÖSTERREICHS

Die Internet-Feuerwehr ist nicht nur dann zur Stelle, wenn IT-sicherheitstechnisch Feuer am Dach ist. Neben Soforthilfe bei Angriffen aus dem Netz leisten CERT.at und GovCERT.gv.at zusätzlich auch wichtige Aufklärungs- und Präventionsarbeit. Eine Leistungsübersicht.

Die Fakten sprechen eine deutliche Sprache. Jeden Tag sind weltweit etwa 150.000 Computerviren im Umlauf und rund 148.000 Computer werden täglich neu infiziert. Der neueste Security Intelligence Report (SIRv15) von Microsoft zeigt auf, dass im Schnitt 17% aller Computer weltweit im ersten Halbjahr 2013 von Malware befallen waren. In Österreich sind zwischen Jänner und Juli 2013 2,1% von 1.000 gescannten Computern infiziert gewesen. Nach Angaben des Weltwirtschaftsforums besteht eine 10-prozentige Wahrscheinlichkeit, dass es im kommenden Jahrzehnt zu einem großen Ausfall kritischer Informationsinfrastrukturen kommt, der Schäden in Höhe von 250 Milliarden US-Dollar verursachen könnte.

Besonders Windows XP-NutzerInnen leben gefährlich. Sie sind aufgrund der veralteten Sicherheitsstruktur des Betriebssystems mittlerweile einer 6-fach höheren Gefahr ausgesetzt, mit Schadsoftware infiziert zu werden, als dies bei aktuellen Betriebssystemen der Fall ist.

Cyber Kriminalität hinterlässt spürbare Folgen

Die zunehmende Berichterstattung über Cyber Angriffe und dessen Auswirkungen bleibt nicht ohne Folgen. So hat eine Eurobarometer-Umfrage zur Cyber Kriminalität 2012 ergeben, dass 38% der Internet-NutzerInnen in der EU infolge von Sicherheitsbedenken ihr Verhalten geändert haben. 18% haben Vorbehalte, Waren online zu kaufen und 15% scheuen sich davor, beispielsweise ihre Bankgeschäfte online abzuwickeln. Rund drei Viertel der Befragten (74%) sind der Ansicht, dass das Risiko, Opfer einer Straftat zu werden, in den letzten Jahren gestiegen ist. Eine Erfahrung, die 12% bereits kennen, da sie selbst bereits einmal Ziel von Online-Betrügern gewesen sind. Immerhin: 89% haben angegeben zu vermeiden, online persönliche Daten preiszugeben.

Österreich – keine Insel der Seligen

Wer nun denkt, Österreich sei im internationalen Gewässer der Cyber Kriminalität eine Insel der Seligen, der irrt. Die österreichischen CERTs erleben im Rahmen ihrer täglichen Arbeit ein anderes Bild. Denn Internet-Kriminalität kennt keine Ländergrenzen und macht auch vor Österreich nicht halt. Nachfolgend haben wir die bedeutsamsten „Highlights“ der jüngsten Cyber Sicherheitsvergangenheit kurz zusammengefasst.

Alle zwei Sekunden ein neues Schadprogramm

Die verwendeten Techniken und Schadprogramme von Internet-Kriminellen sind vielfältig und komplex – und entwickeln sich mit rasender Geschwindigkeit weiter. Branchen-

schätzungen zufolge entsteht alle zwei Sekunden eine neue Variante eines Schadprogrammes. Das breite Spektrum der Schadsoftware wird unter dem Begriff „Malware“ zusammengefasst und umfasst eine Fülle an verschiedenen Bedrohungsformen. Dazu gehören Computerviren und -würmer, Trojaner, Spyware, Bot (-Clients), Ransomware und viele mehr.

CERT.at beobachtet intensiv die Entwicklung von Malware und anderen Bedrohungsformen im Internet und gibt im Anlassfall proaktiv Sicherheitswarnungen heraus. Zusätzlich unterstützt die Internet-Feuerwehr IT-Verantwortliche durch die Weitergabe von Know-how und leistet auch wichtige Präventions- und Aufklärungsarbeit in der Öffentlichkeit. Dadurch tragen CERT.at und GovCERT.gv.at bei, das Internet in Österreich sicherer zu machen.

Die Internet-Sicherheitslage in Österreich

CERT.at und GovCERT.gv.at führen umfangreiche Statistiken, mit denen sich ein aussagekräftiges und stets aktuelles Lagebild der Internet-Sicherheit in Österreich geben lässt. Wichtige Kennzahlen dafür sind Reports, Incidents und Investigations.

„Reports“ sind Meldungen an CERT.at, die durch sicherheitsrelevante Inhalte gekennzeichnet sind. Bei diesen Sicherheitsmeldungen kann es sich beispielsweise um Anfragen oder um Defacement-, Cross-Site-Scripting-, Phishing-, Malware- oder etwa um Google-Conditional-Hack-Meldungen handeln. Als „Incidents“ werden jene Fälle und Anfragen eingestuft, die tatsächlich ein Sicherheitsrisiko darstellen und von CERT.at behandelt werden. Im Zuge von Incidents kommuniziert CERT.at Informationen an die betroffenen Unternehmen, Organisationen oder PrivatanwenderInnen, die helfen, das Problem zu lösen. Diese Kommunikation wird als „Investigation“ bezeichnet.

2012 verzeichnet CERT.at rund 12.900 Reports, von denen knapp 4.300 als ernstzunehmende Incidents eingestuft wurden. Im Jahr 2013 gibt es sowohl bei Investigations wie auch bei Incidents einen Anstieg zu verzeichnen. Die Gründe dafür liegen nicht nur in der tatsächlichen Zunahme an Bedrohungen, sondern vor allem in der immer besseren Sensorik, mit der eine größere Zahl von Angriffen entdeckt werden kann.

Immer noch wirkungsvoll: Denial of Service-Attacken

„Denial of Service“ (DoS)-Attacken zählen zum Standard-Repertoire der Angreifer – und kommen selbst nach langer Zeit nicht aus der

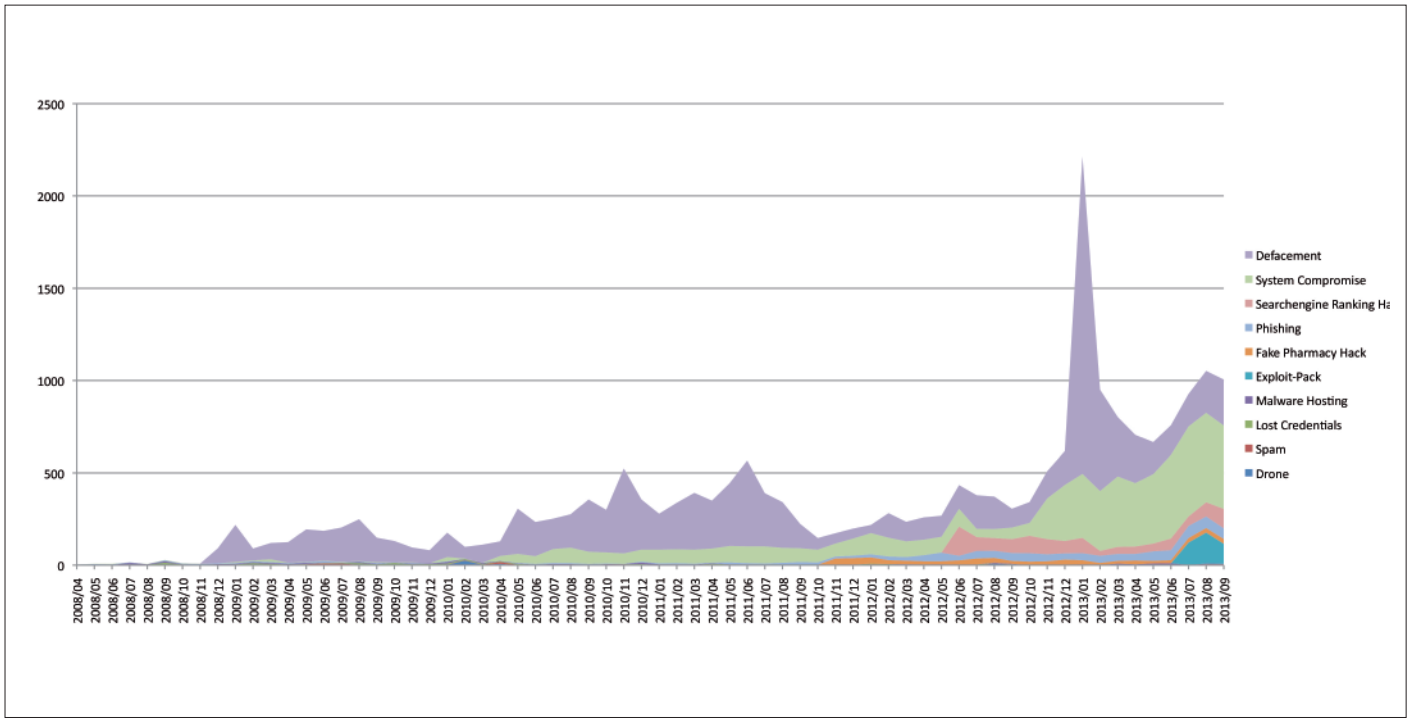


Abb. 1: Incidents pro Monat im Zeitverlauf

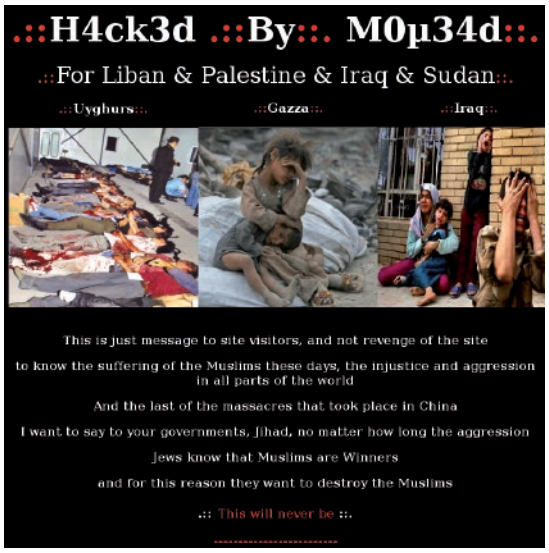
Mode. Bei diesen versendet ein infizierter Computer eine Flut von Anfragen an Server, um diese teilweise oder gänzlich zu blockieren. Ein solcher DoS-Angriff sorgte zuletzt auch in Österreich für Aufsehen. In der zweiten Märzhälfte 2013 kam es zu einer Serie von heftigen DoS-Angriffen auf Spamhaus, einen Anbieter von Anti-Spam-Blocklisten. In einigen Medien wurden die Auswirkungen dieses Angriffs mit einer Verlangsamung des gesamten Internets beschrieben. Die Angriffsmethode und Größenordnung dieser Attacke waren weder neu noch sonderlich innovativ – und deckten dennoch bestehende Angriffsmöglichkeiten schonungslos auf.

Website-Defacements als Massenproblem

Auch die Manipulation und Veränderung von Webseiten, so genannte **Defacements,** haben sich in den letzten Jahren zu einem ernstzunehmenden Problem entwickelt. Besonders Anfang 2013 wurde ein massiver Anstieg an Website-Defacements in Österreich beobachtet, mit teilweise mehr als tausend Vorfällen pro Monat.

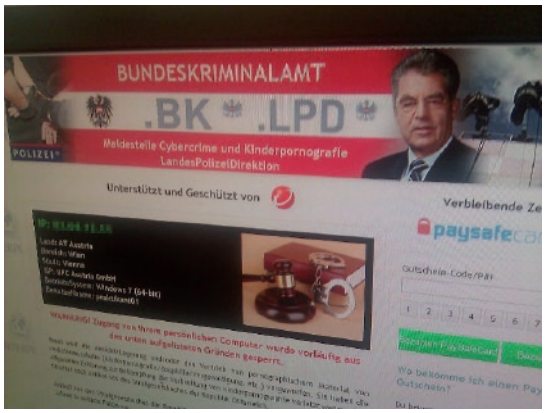
Website-Defacements sind für gewöhnlich technisch nicht besonders aufwändige Angriffe, die jedoch aufgrund ihrer Verbreitung zu einem massiven Problem werden können. Bekannt geworden ist diese Angriffsform in Österreich vor allem durch das gezielte Manipulieren von fremden Webseiten mit zumeist politischen Statements – ohne dabei weiteren Schaden anzurichten. Im aus Anwendersicht ungünstigsten Fall können hingegen Exploit Packs in die Website eingebaut werden, und so die Browser der BesucherInnen angegriffen und infiziert werden. Auch PHP-Skripte werden häufig eingesetzt, wobei beispielsweise gehackte Webserver Teile von Bot-Netzen werden, die wiederum für DoS-Angriffe genutzt werden können.

Stoßen die Experten von CERT.at im Internet auf betroffene Webseiten, informieren sie umgehend die BetreiberInnen. In den meisten Fällen ist Abhilfe schnell möglich. Der Grund für den sprunghaften Anstieg von Defacements zu Jahresbeginn 2013 war ein Fehler in einer veralteten Version eines Plugins für Joomla (ein weit verbreitetes Content Management System). Neben regelmäßigen Updates empfiehlt CERT.at auch, nicht mehr benötigte Plugins und solche, für die es keine (Sicherheits-)Updates mehr gibt, zu deinstallieren, um weitere Einfallsmöglichkeiten für Angreifer zu schließen.



Ransomware, Pishing und andere Dauerbrenner

Es gibt Fälle, bei denen PCs gesperrt oder die Festplatte durch Schadsoftware verschlüsselt und dann "Lösegeld" für die Freigabe verlangt wird. Diese Form ist als Ransomware bekannt. Als einer der prominentesten Vertreter dieser Gattung ist der Polizei- oder BKA (Bundeskriminalamt)-Trojaner zu nennen. Er erhielt diesen Namen, da der vermeintliche Absender der Meldung am PC-Schirm das Bundeskriminalamt oder die Polizei ist. Kriminelle bedienen sich dabei vor allem starker psychologischer Tricks. So wird den Betroffenen häufig der Besitz von Kinderpornographie unterstellt oder durch Auslesen von Bildern über die eigene Webcam Angst gemacht. CERT.at rät, regelmäßige Backups der eigenen Daten zu erstellen, um diese im Notfall wieder rasch herstellen zu können.



Ebenfalls ein Dauerbrenner ist **Phishing,** also das Ausspähen von Zugangsdaten über gefälschte Webseiten und E-Mails. Generell gibt es auch dabei einen Trend zur persönlichen Kontaktaufnahme. Angreifer wählen hierfür

verstärkt den Umweg über Social Media und **Spam.** So verbreiten sich Malware und andere schadhafte Programme mittlerweile auch immer häufiger über beliebte Social Networks wie Facebook und Twitter. Mit **Java** und **PDF** gehören außerdem zwei weit verbreitete Technologien zu den Dauerbrennern im Sicherheitsbereich in Österreich. Vor allem die Vielzahl an Java-Versionen, Inkompatibilitäten und lange Update-Zyklen führen dazu, dass diese häufig nicht aktuell sind – und Angreifer somit leichtes Spiel haben.

Angriffe auf Smartphones im Kommen

Auch die geänderte Mediennutzung macht vor Cyber Kriminellen nicht halt. Daher zielen ihre Angriffe immer stärker auch auf mobile Endgeräte wie Smartphones und Tablets ab. Zwar ist in Österreich bis jetzt noch kein großangelegter Angriff auf mobile Devices bekannt, Attacken wie jene von Hackern auf mehr als zwei Millionen Vodafone-KundInnen in Deutschland im letzten Jahr sind aber ein Alarmsignal. Die Sicherheitsfirma Security Research Labs deckte im Juli 2013 außerdem auf, dass veraltete SIM-Karten als einfaches Einfallstor für Hacker genutzt werden können. Durch eine Sicherheitslücke ist es möglich, dass sich Angreifer unbemerkt Zugang zu fremden Handys verschaffen und anschließend Gespräche oder Nachrichten mithören bzw. mitlesen. Durch das gezielte Anrufen von Mehrwertnummern droht zudem weiterer finanzieller Schaden.

Austrian Trust Circle
Als weiteren Schwerpunkt zur Steigerung der Internet-Sicherheit hat CERT.at gemeinsam mit dem Bundeskanzleramt den Austrian Trust Circle ins Leben gerufen. Dabei handelt es sich um Security Information Exchanges in verschiedenen Bereichen der strategischen Informationsinfrastruktur. Der besondere Rahmen des Austrian Trust Circles erlaubt den praxisnahen und vorbehaltlosen Austausch von führenden VertreterInnen kritischer Infrastrukturen (zB Banken, Energie- oder Telekommunikationsbetreiber) zu aktuellen Sicherheitsthemen – und gilt dadurch auch international als angesehenes Musterbeispiel für mehr Sicherheit.

Nationale und internationale Übungen
CERT.at und GovCERT.gv.at nehmen regelmäßig auch an nationalen wie internationalen Übungen teil. Dabei werden Sicherheitsvorfälle simuliert, Szenarien durchgespielt sowie Kommunikation und Zusammenarbeit in der Praxis geprobt. Im Fokus steht die weitere Verbesserung der Problemlösungskompetenz. Auf europäischer Ebene ist mit Cyber Europe 2014 die nächste länderübergreifende Übung geplant, bei der das BKA unter anderem die österreichische Beteiligung koordiniert. Nach den Cyber Europe Übungen 2010 und 2012 liegen die Schwerpunkte 2014 verstärkt auf technischer, operationeller sowie strategisch-politischer Ebene. Aus nationaler Sicht sind weitere Übungen im Zuge des SCUDO-Projektes, welches vom österreichischen Sicherheitsforschungsprogramm (kurz “KIRAS”) unterstützt wird, sowie im Rahmen der Cyber Exercise seitens des BKA geplant.

IM BESONDEREN: IT-SICHERHEIT ALS INTERNATIONALES THEMA

Cyber Angriffe machen keinen Halt vor territorialen Grenzen. Darum bedarf es länderübergreifender Strategien und Lösungsansätze – ENISA Gastkommentar.

Gastkommentar von
Andrea DUFKOVA
Expert in Computer Incident and Response Handling
Operational Security Unit – CERT relations
ENISA

ROLE OF NATIONAL AND GOVERNMENTAL CERTS IN NATIONAL CYBER COOPERATION

Protecting information online has been a challenging task for many companies, institutions, network providers or individuals due to the extensive growth of businesses and private life going 'online' in the 21st century. Computer Emergency Response Teams (CERTs) are established to support this task by primarily providing necessary response to cyber incidents. Over years the role, tasks and responsibilities of a CERT have developed, especially in the area of national and governmental teams (n/g CERTs) due to information handling expansion into the virtual domain in our daily lives.

Except incident response as core service, there are many other, very important services provided by n/g CERTs. An important task is cooperation with different partners on national and cross-border level. The complexity of procedures, laws, processes and interest of different entities in the cyber world enforce teams to focus and increase their collaboration ambitions and capabilities.

Engagement in activities like supporting the CERT community, saving time and resources e.g. by applying lessons learnt from incident handling, usage and development of tools and information sharing in general or engaging in the (inter)national fight against cybercrime (like cooperation with law enforcement) are not only of benefit for the particular team, but for the community as a whole.

Another example of "new" tasks of n/g CERT's lies in the area of protection of national critical information infrastructure (CIIP). This role varies from country to country and heavily depends on the respective national cyber security strategy (NCSS) and established practices. In some countries the n/g CERT has a more operational role (such as in Estonia or Austria). In other countries they pursue a more advisory role (like in the Czech Republic or Latvia).

How does cooperation work in practice?

There are many examples of successful national cooperation models, among others:

The Netherlands
The National Cyber Security Centre (NCSC) is a government initiative to centralise cyber security related tasks, and the Dutch n/g CERT has an important role to play here. The NCSC defines the integral approach and brings existing initiatives together. Ensuring digital security is the task of various parties and the NCSC acts as the link which binds together the different activities in the country.

Austria
The "Austrian Trust Circle" is an initiative of the national CERT (CERT.at) and the Austrian Federal Chancellery ("Bundeskanzleramt", BKA) and consists of Security Information Exchanges in the individual areas of strategic information infrastructure protection (CIIP). CERT.at offers, in cooperation with the governmental team (GovCERT Austria) and the BKA, a formal framework for practical information exchange and joint projects in the area of security.

Germany
In Germany many CERTs of many sectors are assembled in a formal cooperation network, the German "CERT Verbund". Traditionally, there is a close cooperation between the various teams to collect and prepare the necessary information they need for their own work. By the merge of CERT-Verbund this cooperation is provided on a consistent basis. However, the individual response teams in that network remain responsible for their respective target group (constituency). Other topics for collaboration in the CERT-Verbund are ensuring a common approach to the protection of national networks of information technology, and quickly and collectively react to IT Security incidents.

There are other aspects of collaboration which deserve attention: enabling new, freshly installed teams to quickly get up to speed with their services! ENISA plays well-recognised role in this process by collecting good practice from established, mature teams and making it available to newcomers. However, again it needs to be stressed that support on the national level, especially when there are already well-established teams in a country, is absolutely crucial for success!

Some examples of national supporting initiatives are: The national team of the Czech Republic (CSIRT.CZ) helped to establish the governmental CERT (govCERT.CZ) in that country. The (de facto) national CERT in Poland (CERT-Polska) supported the establishment of the governmental team (govCERT.pl).

In general: good practice shows that in many countries the n/g CERT has an indispensable role in the development of national cyber security cooperation processes and operations.

It is one of ENISA's main tasks to support the CERTs and the CERT communities in Europe! It is important to stress that without the engagement of well-established and mature teams, by supporting actively also in day-to-day business, ENISA could not succeed in this! CERT.at, one of the most advanced teams in Europe, plays a crucial role here. Keep up the good work!

Österreichischer Rekord beim Europäischen Monat der Cyber Sicherheit im Oktober 2013

Als Zeichen der europäischen Zusammenarbeit fand im Oktober 2013 der erste European Cyber Security Month (ECSM) statt, unterstützt durch ENISA und die Europäische Kommission. Die wesentlichen Ziele dieser EU-Kampagne sind die prinzipielle Sensibilisierung der BürgerInnen zur sicherheitsbewussten Nutzung der Möglichkeiten der digitalen Informations- und Kommunikationstechnologien, sowie die Bewusstseinsbildung für Netzwerk- und Informationssicherheit als wichtiges Thema.

Fachtagung im Rahmen des Europäischen Sicherheitsmonats im BKA am 8.10.2013

Neben Österreich beteiligten sich 25 weitere Staaten am Europäischen Monat der Cyber Sicherheit. Mit jeweils etwa einem Fünftel (20%) aller Teilnehmerorganisationen (13 von 69) bzw. Einzelaktivitäten und Veranstaltungen (18 von 86) war Österreich – wie auch von der ENISA gewürdigt – das Mitgliedsland mit den mit Abstand meisten Beiträgen zu dieser Kampagne. Die Schwerpunkte in Österreich reichten von Informationen für BürgerInnen über das IKT-Sicherheitsportal www.onlinesicherheit.gv.at über Fachtagungen für KMUs, Vorlesungen und Workshops an Hochschulen bis hin zur Präsentation eines Leitfadens für die Unterstützung kleiner und mittlerer Gemeinden bei der Implementierung von Maßnahmen zur Verbesserung der IKT-Sicherheit.

IN ZUKUNFT:
DIE DIGITALE REVOLUTION UND FOLGEN FÜR DIE CYBER SECURITY

Die Zukunft unserer Gesellschaft ist von zunehmender Mobilität, der Vision eines „Internet of Things“ und der fortschreitenden digitalen Revolution geprägt. Drucker, die eigenständig neue Tintenpatronen nachbestellen, Smart Meter für die elektronische Stromablesung und vernetzte Autos sind dabei erst der Anfang. Der Cyber Raum entwickelt sich unaufhaltsam in Richtung eines vernetzten, digitalen Aktionsraums für Staat, Wirtschaft, Wissenschaft und Gesellschaft. Eine Transformation, die auch Folgen für die Zukunft der Cyber Security hat. Ein Ausblick.

Cyber Raum – unendliche Weiten?

Das Internet bestimmt schon heute das Leben vieler Österreicherinnen und Österreicher. Die Sicherheit aller Menschen, die zugleich auch Akteurinnen und Akteure in einem großen digitalen Raum sind, wird immer bedeutender. Unsere Gesellschaft befindet sich auf dem Weg in eine Zukunft, die von neuen Interaktions- und Kommunikationsmöglichkeiten geprägt sein wird – mit ebenso neuen Chancen und Herausforderungen für die Cyber Sicherheit:

Information und Kommunikation
Das Internet ermöglicht die Verbreitung und Übertragung unterschiedlicher Daten- und Informationsbestände und wächst mit rapider Geschwindigkeit: Laut einer Statistik des Unternehmens Qmee werden pro Minute derzeit rund 204 Millionen E-Mails versandt, über zwei Millionen Suchabfragen bei Google getätigt, sechs Millionen mal Facebook aufgerufen und mehr als 70 neue Domains registriert.

Soziale Interaktion
Das Internet ist ein Interaktionsraum, den die Menschen zur Pflege sozialer Beziehungen nutzen. Weltweit gibt es mehr als zwei Milliarden Internet-NutzerInnen – Tendenz steigend.

Wirtschaft und Handel
In kurzer Zeit hat sich das Internet zu einem Marktplatz von strategischer Bedeutung entwickelt. Schätzungen zufolge könnte sich der Wert des weltweiten E-Commerce-Geschäfts von 572 Milliarden US-Dollar im Jahr 2012 bis 2014 nahezu verdoppeln.

Politische Partizipation
Das Internet beeinflusst auch das Verhältnis zwischen Staat und Gesellschaft. Mit E-Government erreicht der Staat Bürgerinnen und Bürger, und ermöglicht damit vereinfachte Wege zu staatlichen Leistungen. Digitale Formen der Interaktion eröffnen neue Möglichkeiten der politischen Partizipation und der politischen Meinungsäußerung.

Steuerung
Eng mit den zuvor genannten Bereichen verwoben ist auch die Steuerungsrolle des Internets. Künftig wird ein Großteil der Infrastruktur im Verkehrs-, Wirtschafts-, Sicherheits-, sowie im Gesundheits- und Bildungsbereich über das Internet koordiniert werden. Schätzungen zufolge könnten im Jahr 2020 bis zu 50 Milliarden Geräte miteinander kommunizieren – das sogenannte „Internet of Things“ wird Wirklichkeit.

Vorboten für die Zukunft

Aus Perspektive der IT-Sicherheit betrachtet, bieten diese Entwicklungen nicht nur enorme Chancen, sondern auch neue Risiken und Herausforderungen. Aktuelle Trends und Entwicklungen wie etwa Cloud Computing, Bring your own device, Smart Grids und Mobile Security sind dabei nur Vorboten, die in verstärkter Form auch in Zukunft das Verständnis unserer Gesellschaft zu Sicherheitsthemen prägen werden. Daher ist es entscheidend, bereits heute die „richtigen“ Grundlagen für die Sicherheit unserer Kommunikation in der Zukunft zu definieren. Mit den Teams hinter CERT.at und GovCERT.gv.at verfügt Österreich über ExpertInnen, die diese Aufgabe auch in Zukunft professionell und effektiv verfolgen werden.

Awareness von heute ist der Schutz von morgen

Aus Sicht der SicherheitsexpertInnen steht fest, dass zentrale Bereiche unserer Gesellschaft künftig mit mehr IKT-Intelligenz ausgestattet werden. So lässt sich beispielsweise der Wunsch nach Energieoptimierung oder die Vision einer Energiewende nur in Kombination mit Smart Grids, also intelligenten Netzwerken, erreichen. Die Herausforderung liegt darin, dabei eine ausgewogene Balance zwischen Sicherheit, Datenschutz und Optimierung zu finden. Daher steht für CERT.at und GovCERT.gv.at die Awarenessbildung im Mittelpunkt – um der illegalen Verwendung neuer Tools entgegen zu treten.

© burak çakmak - Fotolia.com

IN SICHERHEIT: SO SCHÜTZEN SIE SICH VOR INTERNET-KRIMINALITÄT

Die Gefahr im Internet lauert immer und überall, denn Cyber Kriminalität ist eine boomende Branche. Doch gegen Angreifer aus dem Internet sind Sicherheitstüren oder Alarmanlagen machtlos. Internet-Kriminelle dringen auf völlig andere Weise in unsere Privatsphäre ein und bereichern sich teilweise direkt vor den Augen der AnwenderInnen – und dennoch bemerken es viele erst, wenn es längst zu spät ist.

Die Lage ist keineswegs aussichtslos. Obwohl sich die technischen Möglichkeiten der Cyber Kriminellen rasant weiterentwickeln, können sich Internet-NutzerInnen mit einer Handvoll Tipps und Tricks wirkungsvoll schützen. Aber wie im realen Leben gilt auch im digitalen Raum: absolute Sicherheit gibt es nicht.

Einfache Grundregeln für unmittelbaren Schutz

Bereits durch wenige, einfach umzusetzende, Maßnahmen lassen sich Bedrohungspotenziale verringern oder gänzlich vermeiden. Mit Einhaltung der folgenden Grundregeln haben Internetangreifer künftig kein leichtes Spiel mehr:

1. Software immer auf dem aktuellsten Stand halten

Veraltete und nicht upgedatete Betriebssysteme stellen für Angreifer eine willkommene Einladung dar. Insbesondere Windows XP gilt in diesem Zusammenhang als anfälliges Betriebssystem mit hohem Sicherheitsrisiko. Obwohl schon vor über zehn Jahren auf den Markt gebracht, ist der „Oldtimer“ unter den Betriebssystemen heute noch immer auf rund einem Drittel aller PCs weltweit im Einsatz – und liegt damit nach Windows 7 auf Platz zwei aller eingesetzten Betriebssysteme.

Problematisch an Windows XP ist die Tatsache, dass es sicherheitstechnisch quasi aus der „Steinzeit“ stammt. So macht die stark veraltete Sicherheitsarchitektur Windows XP zu einem enormen Sicherheitsrisiko, sowohl für EndkonsumentInnen wie auch für Unternehmen. AnwenderInnen setzen sich dadurch unbewusst enormen IT-Sicherheitsrisiken aus, die sich jedoch einfach vermeiden lassen – beispielsweise durch den Umstieg auf aktuelle Betriebssysteme von Microsoft oder anderen Anbietern. Hinzu kommt, dass Microsoft am 8. April 2014 den Support für Windows XP end-

gültig einstellt. Das bedeutet, dass es ab diesem Zeitpunkt keinerlei Aktualisierungen, Sicherheitsupdates oder technischen Support mehr von Microsoft für Windows XP geben wird. Den besten Schutz ab diesem Zeitpunkt bietet dann nur mehr das Ziehen des Netzwerkkabels.

Nicht nur Betriebssysteme, sondern jede Art von Software sollte generell immer am aktuellen Stand gehalten werden. Das Aktivieren von automatischen Updates bietet hier für gewöhnlich bereits effektiven Schutz, da Angreifer oft bekannte Sicherheitslücken von alten Versionen ausnutzen. Selbstverständlich gilt dies in immer stärkerem Ausmaß auch für mobile Geräte wie Smartphones und Tablets.

2. Angriffsflächen minimieren

Die nächste Grundregel ist nicht nur trivial, sondern zugleich auch höchst effektiv. Software, die nicht installiert ist, kann auch nicht von Angreifern ausgenützt werden. Cyber Kriminelle sind sehr einfallsreich, wenn es darum geht, Schadsoftware auf fremde PCs einzuschleusen. AnwenderInnen sollten daher nur jene Software tatsächlich installieren, die sie selbst aktiv gesucht haben. Vor Zusatz-Tools aller Art, speziellen Add-ons oder sonstiger Software, die ihre Installation förmlich aufdrängt, sollten AnwenderInnen tunlichst die Hände lassen. Außerdem ist es ratsam, nicht mehr benötigte Software wieder zu deinstallieren.

3. Sicherheitssoftware verwenden

Sicherheit beginnt dort, wo der Komfort endet. Doch wo genau diese Grenze verläuft, ist von AnwenderIn zu AnwenderIn verschieden. Der Einsatz von aktueller Sicherheitssoftware wie Anti-Virenprogrammen und Firewalls bietet auf einfachem Weg einen Basisschutz. Zahlreiche Programme von renommierten Herstellern sind für PrivatanwenderInnen außerdem kostenlos verfügbar. Wie beim ABS im Auto gilt auch hier die Devise: Sicherheitsgewinne gibt es nur, wenn diese Programme auch aktiviert sind, und sich NutzerInnen nicht im Vertrauen auf diese Helfer für unverwundbar halten.

> *Das Böse triumphiert allein dadurch, dass gute Menschen nichts unternehmen.*
> *(Edmund Burke)*

4. Sorgfältiger Umgang mit persönlichen Daten

Mobile Devices wie Smartphones oder Tablets begleiten Internet-AnwenderInnen mittlerweile auf Schritt und Tritt. Besondere Vorsicht ist daher geboten, wenn über öffentliche Zugänge (zB Public WLAN) eine Verbindung mit dem Internet hergestellt wird und Daten ausgetauscht werden. Internet-NutzerInnen sollten sehr sorgfältig darauf achten, wie sie mit ihren persönlichen Daten umgehen und wo sie diese im Internet preisgeben. Denn nichts ist für Cyber Kriminelle einfacher, als personenbezogene Daten oder Passwörter über ein offenes WLAN abzufangen. Auch sollten unterschiedliche Passwörter für unterschiedliche Zugänge gewählt werden. Allgemein gilt bei der Weitergabe eigener Daten sehr zurückhaltend zu agieren – insbesondere auf Social Networks wie Facebook & Co.

5. Nicht alles glauben

Trotz aller technologischen Schutzmechanismen gibt es noch immer eine Hürde, die Internet-Kriminelle nicht ohne weiteres überwinden können: den gesunden Hausverstand. Eine gewisse Grundskepsis im Umgang mit dem Internet sowie die Entwicklung eines „digitalen Bauchgefühls“ sind daher eine wichtige Basis, um Angriffsversuche von Kriminellen abzuwehren. Kindern wird von Anfang an beigebracht, keine Geschenke von Fremden anzunehmen. Solche selbstverständlichen Regeln müssen wir uns auch für den Internet-Umgang aneignen.

Webtipps

IKT-Sicherheitsportal mit zahlreichen weiteren Tipps und Tricks:
www.onlinesicherheit.gv.at

Initiative „Sicher im Internet“:
www.saferinternet.at

Europäisches Verbraucherzentrum Österreich:
www.europakonsument.at

IM ÜBERBLICK: CERT SICHERHEITSGLOSSAR

Informationen und Erläuterungen zu den wichtigsten Fachbegriffen der IT-Sicherheit.

Austrian Trust Circle
Der Austrian Trust Circle (ATC) besteht aus Security Information Exchanges in den einzelnen Sektoren der strategischen Infrastruktur und zwischen diesen. Das Ziel ist es, Vertrauen zwischen den handelnden Personen und Organisationen aufzubauen, um sicherheitsrelevante Erfahrungen austauschen und im Anlassfall rasch gemeinsam agieren zu können. Aktuell sind die Sektoren Energie, Finanz, Gesundheit, Industrie, ISP und Transport adressiert.

Awareness
Bezeichnet das Sicherheitsbewusstsein aller an der Informationssicherheit mitverantwortlichen Personen. Die dauerhafte Einhaltung und Umsetzung von Sicherheitsregeln ist nur durch Verständnis und Motivation zu erreichen.

Bot-Netz
Ein Bot (Abk. für Roboter) ist ein Programm, das auf dem PC eines Users installiert wird, ohne dass dieser es bemerkt. Der Besitzer des Bots kann dann aus der Ferne am fremden PC Anwendungen ausführen. Werden mehrere dieser virtuellen Roboter zusammengeschlossen, spricht man von einem Bot-Netz. Prominente Beispiele für einen solchen Zusammenschluss von Bots sind Rustock oder Conficker.

CERT
CERT ist die Abkürzung für „Computer Emergency Response Team“. CERTs sind Arbeitsgruppen oder Organisationen, die aktive Unterstützung bei IT-Sicherheitsproblemen in ihrem Verantwortungsbereich bieten. Das kann eine einzelne Organisation sein, in der das Team um den IT-Sicherheitsverantwortlichen die CERT-Rolle übernimmt, oder der Staat, wo das nationale CERT als Internet-Feuerwehr des Landes fungiert.

Conficker
Conficker (auch bekannt unter Downup, Downadup, Kido und Worm.Win32/Conficker) ist ein Computerwurm für Microsoft Windows, der im November 2008 erstmals auftauchte und seither in mehreren Versionen aktiv ist. Er schaffte es Anfang 2009, weltweit die Windows-Netzwerke einiger kritischer Infrastrukturen zu infizieren.

Cyber Angriff
Ein Cyber Angriff ist ein Angriff mit Mitteln der IT, der sich gegen einen oder mehrere andere IT-Systeme richtet und zum Ziel hat, die Funktion der IT-Sicherheitssysteme zu stören oder zu umgehen. Dabei werden die Grundlagen der IT-Sicherheit, Vertraulichkeit, Integrität und Verfügbarkeit als Teil oder Ganzes verletzt. Angriffe, die sich gegen die Vertraulichkeit eines IT-Systems richten, werden als Cyber Spionage bezeichnet. Jene gegen die Integrität und Verfügbarkeit eines IT-Systems als Cyber Sabotage.

(D)DoS-Angriff
Denial of Service (DoS) heißt „Nutzung verhindern“. Bei einem DoS-Angriff wird ein Computer mit Netzwerkpaketen oder Anfragen bombardiert. Die Folge: Der Rechner kann die gewaltigen Datenmengen nicht mehr verarbeiten und ist überlastet. Wird von mehreren Quellen her gleichzeitig angegriffen, spricht man von einem DDoS-Angriff (Distributed Denial of Service-Angriff).

Firewall
Eine externe (Netzwerk- oder Hardware-) Firewall stellt eine kontrollierte Verbindung zwischen zwei Netzen her. Dabei überwacht die Firewall den durch sie hindurch laufenden Datenverkehr und entscheidet anhand festgelegter Regeln, ob bestimmte Netzwerkpakete durchgelassen werden oder nicht. Auf diese Weise versucht die Firewall ein Netzwerk oder Netzsegment vor unerlaubten Zugriffen zu schützen.

Google Conditional Hacks
Dabei werden bestehende Websites gehackt und ein schädlicher serverseitiger Code eingeschleust. Dieser manipuliert den Inhalt der Webseite abhängig davon, wer sie besucht. Ist es der Webcrawler von Google (Google-Bot), so baut der Schadcode Schlagwörter wie beispielsweise „Viagra“ in die Seite ein, worauf diese bei einer entsprechenden Google-Suche nach diesen Pillen gefunden wird. Landet ein Besucher auf der Webseite nach einer solchen Suche, dann schickt der Code des Einbrechers den Besucher auf einen passenden Webshop. Das Ganze ist also ein Trick, bei dem das Google-Ranking einer legitimen Seite ausgenutzt wird, um dubiose Pillenshops als Top-Treffer bei Google zu platzieren. Der Webseitenbetreiber merkt davon oft über lange Zeit gar nichts.

Hacker
Bezeichnet Personen, die Sicherheitslücken in fremden IT-Systemen suchen und unter Ausnutzung von Schwachstellen unberechtigt Zugriff auf sonst geschützte Systeme/Daten erlangen. Mit dem Begriff „White-Hat-Hacker“werden gesetzestreue Hacker bezeichnet, die meist im Auftrag der Eigentümer der IKT-Systeme nach Si-

cherheitslücken suchen, um die Sicherheit dieser zu verbessern. Mit dem Begriff „Black-Hat-Hacker“ werden Hacker mit krimineller Energie bezeichnet, die Angriffe auf IT-Systeme ausüben, um sich einen finanziellen Vorteil zu verschaffen oder sonstigen Schaden anzurichten.

Lost Credentials

Bei dieser Kategorie von Vorfällen, die direkt übersetzt so viel wie „verlorene Zugangsdaten“ heißt, geht es um publik gewordene User-Zugangsdaten. Das kann über Schadsoftware am PC passiert sein, oder auch durch Einbrüche in Webserver.

Malware

Als Schadprogramm oder Malware (Zusammensetzung aus engl. malicious, „bösartig“ und Software) bezeichnet man Computerprogramme, die entwickelt wurden, um vom Benutzer unerwünschte und schädliche Funktionen auszuführen. Dieser Begriff bezeichnet keine fehlerhafte Software, auch wenn diese Schaden anrichten kann. Malware wird von Fachleuten der Computersicherheitsbranche als Über-/Sammelbegriff verwendet, um die große Bandbreite an feindseliger, unerwünschter Software zu beschreiben. Als Malware Hosting bezeichnet man das Bereitstellen von Malware auf Webseiten.

Man-In-The-Middle Attacke

Darunter versteht man den Angriff auf den Kommunikationskanal zwischen zwei oder mehreren Computersystemen. Dabei versucht der Angreifer, die Kommunikation unter seine Kontrolle zu bringen, ohne dabei bemerkt zu werden. Ziel ist es, den Informationsfluss einsehen und manipulieren zu können.

Phishing

Der Begriff Phishing setzt sich aus „password“ und „fishing“ zusammen. Mit Phishing bezeichnet man den Versuch, mit Hilfe gefälschter E-Mails/Websiten an vertrauliche Daten zu kommen. Oft funktioniert das über Webseiten, die den Loginseiten von Banken, Webmailservern oder anderen Webdiensten täuschend ähnlich sehen. Phishing ist eine bekannte Variante des „Social Engineering“.

Social Engineering

Social Engineering meint im Zusammenhang mit IT Security eine bestimmte Strategie von Online-Betrügern. Bei Social Engineering versucht der Angreifer, vergleichbar mit Trickbetrug, nicht über technische Tricks oder Programmfehler sein Ziel zu erreichen, sondern sein Opfer so zu täuschen, dass es von sich aus dem Angreifer hilft. Die Cyber Kriminellen adressieren ihre Opfer bei dieser Methode oft individuell und können so immer wieder Treffer landen. Surfgewohnheiten, Namen aus dem persönlichen Umfeld des Opfers etc. werden zuerst ausspioniert, um dann z.B. Phishing-E-Mails persönlich zu gestalten und das Vertrauen der jeweiligen Person gewinnen zu können.

Spam

Als Spam bezeichnet man elektronische Nachrichten, die einem Empfänger unerwünschter Weise zugestellt werden. Diese Nachrichten beinhalten oftmals Werbeinhalte, werden in Massen versendet und können auch zur Verteilung von Malware (Malware-Spreading) verwendet werden.

System Compromise

Durch einen System Compromise verliert der eigentliche Besitzer des Systems die Kontrolle darüber. Dieser Kontrollverlust kann mehrere Gründe haben wie zum Beispiel die lückenhafte Kontrolle von Benutzerkennwörtern oder durchlässige Webapplikationen.

Trojaner

Als Trojanisches Pferd, auch kurz Trojaner genannt, bezeichnet man ein Computerprogramm, das als nützliche Anwendung getarnt ist, im Hintergrund aber ohne Wissen des Anwenders eine andere Funktion erfüllt. Ein Trojanisches Pferd zählt zur Familie unerwünschter bzw. schädlicher Programme, der so genannten Malware.

Website-Defacement

Mit Website-Defacement (oder auch nur Defacement) wird die unberechtigte Veränderung einer Website bezeichnet. Dabei werden Sicherheitslücken ausgenützt oder gestohlene Passwörter benutzt, um das visuelle Erscheinungsbild einer Website zu „entstellen“. Oftmals wird auch eine Botschaft auf der veränderten Website hinterlassen.

MEHR INFORMATIONEN UNTER
WWW.CERT.AT
UND
WWW.GOVCERT.GV.AT

WIEN 2013