BERICHT INTERNET-SICHERHEIT ÖSTERREICH 2012

GovCERT AUSTRIA

CERT.at

VORWORT

Staatssekretär
Dr. Josef Ostermayer

Das Internet ist längst ein fixer Bestandteil des täglichen Lebens der Österreicherinnen und Österreicher geworden und hat in alle Lebensbereiche Einzug gehalten. In den mehr als 20 Jahren, in denen Österreich nun bereits online ist, hat sich das Kommunikationsverhalten massiv gewandelt und das Funktionieren unserer Gesellschaft grundlegend verändert. Der Austausch von Informationen ist heute schneller und einfacher als je zuvor und Wissen von nahezu überall elektronisch abrufbar. Zusätzlich nutzen Bürgerinnen und Bürger immer stärker das elektronische Leistungsangebot der österreichischen Verwaltung und profitieren somit auch auf persönlicher Ebene von den Innovationen im Informations- und Kommunikationsbereich der letzten Jahre.

Doch die umfangreiche Vernetzung offenbart zunehmend auch ihre Schattenseiten. Bedrohungen und Angriffe über das Internet steigen rasant an und stellen Zivilgesellschaften weltweit vor eine Reihe neuer Herausforderungen und Fragen. Fragen, auf die es nicht nur nationale, sondern vor allem auch gemeinsame internationale Antworten braucht. Denn, wenn es um den Schutz von Grundrechten und Eigentum im Internet, die Eindämmung von kriminellen Handlungen oder die gezielte Abwehr von virtuellen Angriffen und Bedrohungen geht, stoßen bestehende Regelungen und Ansätze oftmals an ihre Grenzen und es bedarf einer stark aufeinander abgestimmten internationalen Zusammenarbeit.

Österreich ist sich dieser Herausforderungen bewusst und arbeitet daher auf nationaler wie auch auf internationaler Ebene intensiv an der Gestaltung von Cyber Security Strategien, die auf das sich ändernde Umfeld Bezug nehmen und langfristig Bestand haben sollen. So wird im Zuge der Stärkung der Europäischen Agentur für Netz- und Informationspolitik ENISA unter anderem die Zusammenarbeit der nationalen Behörden verbessert und ein länderübergreifendes System zur Erfassung von Cyberangriffen aufgesetzt, das auch von Österreich unterstützt wird.

Eine wichtige Rolle im Kampf gegen die „unsichtbaren Feinde“ aus dem Netz nehmen in Österreich das Computer Emergency Response Team (CERT) sowie das GovCERT Austria für den öffentlichen Bereich ein. Die Entwicklung von CERT.at und GovCERT.gv.at ist 4 Jahre nach deren Gründung eine höchst erfreuliche, denn die Organisationen sind in ihrem Tätigkeitsbereich erfolgreich und bestens etabliert.

Seit Herausgabe des ersten CERT Sicherheitsberichtes 2010 hat sich das Themenfeld entlang potenzieller Bedrohungsfelder stark erweitert und gewandelt. Neben dem klassischen Umfeld im Informations- und Kommunikationsbereich stehen heute verstärkt auch andere Sektoren wie Energie, Verkehr oder die Finanzwelt im Fokus. Der überarbeitete Sicherheitsbericht nimmt daher verstärkt auch darauf Bezug und unterstreicht die Leistungen und Pläne Österreichs, wie das Internet auch in Zukunft ein möglichst sicherer Teil des öffentlichen und privaten Lebens werden soll.

CYBER SECURITY HAT VIELE FACETTEN

Robert Schischka,
Leiter von CERT.at

Längst ist das Internet ein wichtiges Aktionsfeld zur Verbreitung von Bedrohungen und Gefahren geworden. Durch den Einsatz und die Nutzung von Informationstechnologien im Alltag wird auch das Thema Cyber Security hierzulande immer wichtiger. Von der zunehmenden Kriminalität im Netz sind mittlerweile potenziell alle betroffen – Einzelpersonen gleichermaßen wie Behörden, Unternehmen oder Regierungen. Zudem nimmt Kriminalität im Internet auf keinerlei Grenzen Rücksicht und entwickelt sich mehr und mehr zu einem internationalen, grenzüberschreitenden Phänomen mit lokalen Auswirkungen. Auch verschmelzen die virtuelle und reale Welt immer stärker miteinander. Ein Umstand, der den Kampf gegen Cyber Bedrohungen neu definiert.

Nationalstaaten kommt in dieser Hinsicht eine immer bedeutendere Rolle zuteil, ist doch das Themenfeld Cyber Security vielfältig und durch ständige Änderungen gezeichnet. Daher ist das Thema in Österreich eine wichtige Querschnittsmaterie. Mit dem CERT (Computer Emergency Response Team) für den Unternehmens- und Privatbereich und dem GovCERT Austria für den Behördenbereich hat Österreich nunmehr seit 2007 zwei etablierte Organisationen, die eine aktive Rolle im Kampf gegen Bedrohungen aus dem Internet einnehmen. CERT.at und GovCERT.gv.at fungieren hierbei gemeinsam als Drehscheibe für Internetsicherheit im Allgemeinen und als Frühwarnsystem und Koordinierungsstelle für den Schutz kritischer Infrastrukturen im Besonderen. So zählt zu den Kernaufgaben neben der Schaffung rechtzeitiger Vorsorgemaßnahmen auch die Förderung der Bewusstseinsbildung für gezielte Schutzmaßnahmen. Dazu setzen CERT.at und GovCERT.gv.at auf intensive Kooperation mit öffentlichen Stellen und der Privatwirtschaft.

Der vorliegende CERT Sicherheitsreport 2012 gibt einen Überblick über die Rolle Österreichs im Kampf gegen Cyber Bedrohungen und beleuchtet die Leistungen von CERT.at und GovCERT.gv.at. Wir freuen uns diesbezüglich auch über Feedback, um gemeinsam Österreich bestmöglich gegen Gefahren abzusichern und auf die Zukunft vorzubereiten.

© HBF

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

INHALT

© eva serrabassa - iStockphoto.com

IMPRESSUM: Medieninhaber und Verleger: 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:** peritia communications (Michael Höfler, Markus Gruber) **Grafik:** creativedirector.cc lachmair gmbh. **Verlags- und Herstellungsort:** Wien. Juni 2012

CYBER SECURITY STRATEGIEN – EIN INTERNATIONALER VERGLEICH

Cyber Sicherheit wird zu einer zentralen Herausforderung für Staat, Wirtschaft und Gesellschaft im nationalen und internationalen Kontext. Angriffe auf kritische Infrastrukturanlagen sind zahlreicher geworden, haben an Komplexität zugenommen und sind durch zunehmende Professionalisierung gekennzeichnet. Daher zählt die Entwicklung von Cyber Security Strategien für viele Länder weltweit zu einem wichtigen Anliegen im sicherheitspolitischen Kontext.

Ein Ziel – viele Ansätze

Doch so einheitlich die im Wesentlichen gleichbleibende Problemstellung erscheint, so unterschiedlich gestaltet sich die Umsetzung. Betrachtet man die Entwicklungen von nationalen Cyber Security Strategien, so zeichnet sich ein durchwegs unterschiedliches Bild. Zahlreiche Länder, wie beispielsweise die USA, Deutschland oder Skandinavien, verfolgen einen eher Top-down getriebenen Ansatz und setzen verstärkt auf Vorgaben und die Schaffung von verbindlichen Regelwerken.

Beispiel Österreich

Andere Strömungen hingegen – zu denen sich auch Österreich zählen lässt – gehen einen anderen Weg und propagieren einen Bottom-up Approach. Dabei werden zumeist relevante Stakeholder identifiziert, Abhängigkeiten aufgezeigt und analysiert sowie in kooperativer Weise mit allen Beteiligten gemeinsam Ansätze und Strategien entwickelt, die in Form eines mehrstufigen Prozesses verdichtet werden. Nicht zuletzt auch aufgrund der historisch in Österreich sehr stark ausgeprägten konsensorientierten Kultur unterscheidet sich der heimische Ansatz im internationalen Vergleich. Österreich baut dazu stark auf einer qualitativen Zusammenarbeit auf breiter Vertrauensbasis auf. Nähere Details zu den Hintergründen der Entwicklung einer österreichischen Cyber Security Strategie lesen Sie auf den Seiten 6 und 7.

Beispiel Deutschland

Unter Cyber Security versteht Deutschland, die Risiken des Internets auf ein tragbares Maß zu reduzieren. Ein Maß, dass das Internet trotz der rasanten Weiterentwicklung und Verbreitung nicht unsicherer erscheinen lässt, als andere Lebensbereiche auch. In diesem Zusammenhang sieht sich Deutschland auch in einer Vorreiterrolle in Europa sowie weltweit und verweist auf bereits zahlreiche Aktivitäten auf diesem Gebiet. 2011 hat Deutschland eine neue Cyber Sicherheitsstrategie beschlossen. Ziel der Strategie ist, Cyber Sicherheit in Deutschland auf einem hohen Niveau zu

gewährleisten – ohne dabei die Chancen und den Nutzen des Cyber-Raums zu beeinträchtigen. So wurde ein nationales Cyber Abwehrzentrum errichtet, dessen Aufgabe darin besteht, Lageinformationen zwischen allen beteiligten Behörden auszutauschen. Es ermöglicht so, schnell und abgestimmt alle Informationen zu Schwachstellen in IT-Produkten oder IT-Vorfällen zu vernetzen, diese zu analysieren und Empfehlungen zum Schutz der IT-Systeme zur Verfügung zu stellen bzw. auszusprechen. Koordiniert wird die Arbeit im Rahmen der Cyber Sicherheitsstrategie durch einen neu eingerichteten Cyber Sicherheitsrat. Zusätzlich beschäftigt sich Deutschland intensiv mit verschiedenen Angriffsszenarien und Analysen bereits erfolgter Vorfälle und sieht das Thema als gemeinsame Herausforderung für Staat, Wirtschaft und Bürger.

Beispiel Schweiz

Das Funktionieren der Schweiz hängt von einer steigenden Zahl miteinander vernetzter Informations- und Kommunikationseinrichtungen ab. Diese Infrastrukturen sind verwundbar und Angriffe können zu erheblichen Beeinträchtigungen von technischen, wirtschaftlichen und administrativen Leistungen der Schweiz führen. Der Schutz der Informations- und Kommunikationsinfrastruktur liegt daher im nationalen Interesse der Schweiz. Was die Cyber-Risiken betrifft, so ist die Schweiz mit denselben Risiken konfrontiert, die in ähnlicher Weise für alle Länder aktuell ein Sicherheitsproblem darstellen. Jedoch gelten Bereiche, in denen die Schweiz eine dominante Marktposition hat, als besonders gefährdet. Das gilt u.a. für das Finanzwesen (wichtiger Finanzplatz) und die Energieversorgung (25% der europäischen Elektrizität wird über die Schweiz transportiert). Der Bundesrat misst daher dem Schutz der Informatik-Infrastruktur eine hohe sicherheitspolitische Bedeutung zu.

Beispiel USA

Die USA sehen Cyber Security als eine zentrale Herausforderung für sich und die Welt. Im Rahmen der im Mai 2011 vorgestellten Cyber-Sicherheitsstrategie nehmen die USA intensiv darauf Bezug. Der Schutz und die Sicherheit von strategisch wichtigen Kommunikations- und Infrastruktursystemen werden unmittelbar mit der Sicherung von „Wohlstand, Sicherheit und Offenheit in einer vernetzten Welt“ assoziiert. Cyber Security wird nicht als Selbstzweck, sondern vielmehr als Verpflichtung angesehen, dass Innovationen weiterhin gedeihen können, die Wirtschaft vorankommt und sich die Lebensqualität verbessert. Dazu wird auch verstärkt auf internationale Kooperation gesetzt. Besonderes Augenmerk der neuen Strategie liegt auf den Bereichen Strom- und Wasserversorgung, Kommunikation sowie Handels- und Regierungsnetzwerken. Dabei wird insbesondere auch auf die Bedrohung durch feindliche Staaten oder terroristische Organisationen Bezug genommen. Die USA wollen künftig stärker international kooperieren und streben u.a. den Aufbau eines weltweit operierenden Frühwarnsystems an. Auch gesetzliche Regelungen stehen im Mittelpunkt der Pläne. So sollen vorhandene Gesetze und Vorschriften stärker als zuvor an die Gegebenheiten im Cyberspace angepasst und entsprechend erweitert werden. Hinzu kommt die Intensivierung der Zusammenarbeit mit Ermittlungsbehörden anderer Länder. In aller Deutlichkeit sprechen sich die USA außerdem dafür aus, auf Cyber Angriffe unter Umständen auch auf „konventionellem Wege“ diplomatisch, ökonomisch oder auch militärisch zu reagieren – im Sinne des Rechtes auf Selbstverteidigung eines Staates.

Die ausgewählten Beispiele zeigen, dass Motive und Beweggründe für die Entwicklung eigener Cyber Security Strategien größtenteils ähnlichen Ursprung haben. Unterschiede in Entwicklung und Ausgestaltung eigener Strategien ergeben sich hingegen aufgrund des jeweiligen Selbstverständnisses und der geopolitischen Rolle eines Landes.

ÖSTERREICHS WEG ZU EINER NATIONALEN CYBER SECURITY STRATEGIE

© Huebi - Fotolia.com

Bedrohungen aus dem Internet sind vielfältig und haben sich in jüngster Vergangenheit um eine weitere Dimension erweitert. Bekannt gewordene Fälle von Cyber Spionage und gezielte Angriffe auf Industrieanlagen oder andere Infrastruktursysteme haben dazu geführt, dass sich die Problematik längst zu einem übergeordneten Bedrohungsfeld entwickelt hat. Maßnahmen und Ansätze zum Schutz gegen Bedrohungen aus dem Internet zählen daher für viele Nationalstaaten zu dem Top-Sicherheitsthema schlechthin. Experten weltweit arbeiten an der Entwicklung von adäquaten und vor allem zukunftsfähigen Strategien, um für den Kampf gegen Cyber Bedrohungen gerüstet zu sein.

Strategieentwicklung mit vielen Facetten

Die zunehmende Verbreitung bzw. Nutzung von Informationstechnologien im Alltag zeigt neben allen Vorteilen und Verbesserungen aber auch ihre Schattenseiten. Und: Die Abhängigkeit der Gesellschaft von Informations- und Kommunikationstechnologien steigt weiter. Daher werden auch Themen wie Cyber Strategien immer wichtiger und schlagen auf zahlreichen Ebenen auf. Auch in Österreich hat das Thema Cyber Security, nicht zuletzt aufgrund von Aktionen von Anonymous und LulzSec in den vergangenen Monaten stark an Bedeutung gewonnen, seitdem die eigene Verwundbarkeit durch gezielte Angriffe sichtbar wurde. Im Rahmen der Regierungsklausur im Mai 2011 hat die österreichische Bundesregierung daher die Entwicklung einer österreichweiten Strategie zur Cyber Security beschlossen.

Gemeinsame Strategieentwicklung auf breiter Basis

Sicherheit und Vertrauen in die weltweite Vernetzung sind wesentliche Faktoren für Unternehmen, Behörden und Bürgerinnen und Bürger. Diese engmaschige Vernetzung gilt es nachhaltig zu schützen. Das Bundeskanzleramt (BKA) nimmt diese wichtige Aufgabe gemeinsam mit dem Bundesministerium für Landesverteidigung und Sport und dem Bundesministerium für Inneres wahr und koordiniert die nationale Cyber Security Strategie. Die Ergebnisse sind ein wichtiger Bestandteil der nationalen Aktivitäten im Bereich Cyber Security und haben das Ziel, Österreich auch im Internet sicherer zu machen – jetzt und für die Zukunft.

Unter Federführung des Bundeskanzleramts arbeiten Experten in unterschiedlichen Arbeitsgruppen auf allen Ebenen an der Entwicklung einer gemeinsamen Strategie, die bis Ende 2012 finalisiert und anschließend von der gesamten Politik umgesetzt und getragen werden soll.

Der erste Baustein, die „Nationale IKT-Sicherheitsstrategie“

Monatelang arbeiteten über 130 Fachleute an einer nationalen IKT-Sicherheitsstrategie mit dem Ziel, ein proaktives Konzept zum Schutz des Cyber-Raums und der Menschen im virtuellen Raum zu schaffen. Im Juni 2012 wurde sie nun fertiggestellt und im feierlichen Rahmen veröffentlicht. Die IKT-Sicherheitsstrategie ist damit der zentrale Baustein für die Erstellung der nationalen Cyber Security Strategie.
Die neue Strategie dient zum einen der Bewusstseinsbildung, zum anderen sieht sie konkrete Aktivitäten für Cyber Vorfälle vor. Die im Rahmen der IKT-Sicherheitsstrategie behandelten Aspekte reichen von Bildung, Forschung, Sensibilisierung und Judikatur über technische und organisatorische Belange österreichischer Unternehmen bis hin zur Absicherung strategisch bedeutender Einrichtungen Österreichs.

Weiterführende Informationen finden Sie im Bericht „Nationale IKT-Sicherheitsstrategie Österreich“ auf www.digitales.oesterreich.gv.at

Um eine nachhaltige und ganzheitliche Strategie zu entwerfen, wurde bei der Ausarbeitung eine Bottom-Up Herangehensweise mit einem breiten Ansatz gewählt, der alle relevanten Akteurinnen und Akteure in Österreich integriert. Die strategischen Zielsetzungen wurden aus der Perspektive von fünf Kernbereichen, die gleichzeitig die Arbeitsgruppen bildeten, festgelegt. Dabei handelt es sich um die Bereiche „Stakeholder und Strukturen“, „Kritische Infrastruktur“, „Risikomanagement und Lagebild“, „Bildung und Forschung“ sowie „Awareness“.

Wie geht es weiter

Die Nationale IKT-Sicherheitsstrategie soll nun mit Cyber Aktivitäten von anderen Ministerien abgestimmt werden und zu einer gemeinsamen Umsetzung führen. Insbesondere sollen die Aspekte von Cyber Crime und Cyber Defense, aber auch sonstige Cyberinitiativen in Österreich berücksichtigt werden. Als von allen Stakeholdern verabschiedetes umfassendes Cyberkonzept für Österreich soll die Cyber Security Strategie Ende 2012 fertiggestellt werden.

ÖSTERREICH IN ZEITEN AKTUELLER BEDROHUNGEN AUS DEM INTERNET

Arbeitsschwerpunkte des Computer Emergency Response Team im Kampf gegen Cyber Security Bedrohungen.

Enormer Wirtschaftsfaktor

750 Milliarden Euro. So hoch wird der Schaden geschätzt, der weltweit jährlich aufgrund von Internetangriffen entsteht – Tendenz steigend. Alleine in Österreich wurde 2010 durch Internetbetrug ein Schaden von 5,7 Millionen Euro gemeldet. Doch die Dunkelziffer dürfte weit darüber liegen, denn vielfach ist den Betroffenen gar nicht bzw. noch nicht bewusst, dass sie Opfer von Attacken geworden sind. Pro Tag wird rund eine Million Menschen Opfer von Cyber Angriffen – in den allermeisten Fällen völlig unbemerkt.[1]

Keine Insel der Seligen

Die Abwehr von Angriffen und der Schutz heimischer IT-Systeme werden als zentrale Herausforderungen für die Zukunft gesehen. Betrachtet man die Sicherheitslage Österreichs im weltweiten Vergleich, so ist auch Österreich in der Vergangenheit keineswegs verschont geblieben. Malware, Trojaner, Viren und andere Bedrohungsformen sind auch längst hierzulande „heimisch“ geworden. Wie auch allgemein in den letzten Jahren Infektionsraten weltweit deutlich zugenommen haben.

Welcher Anteil der PCs in Österreich mit Schadsoftware infiziert ist, lässt sich nicht direkt messen. Jedoch bekommt man anhand einiger Faktoren Anhaltspunkte dafür und kann Vergleiche aufstellen. Werden Botnetze analysiert, so findet man dort meist einen Anteil an IP-Adressen aus Österreich, der grob der Größe unseres Landes entspricht. Die heimischen Infektionsraten liegen dabei im Rahmen des in Mitteleuropa üblichen. Auch melden Installationen von Anti-Viren-Software an den Hersteller statistische Daten über die gefundene Schadsoftware. Darauf aufbauend publiziert etwa Microsoft den Security Intelligence Report (SIR), dem „Computers cleaned per Mille (CCM)“ zugrunde liegen. So sind Microsoft zufolge weltweit neun von tausend gescannten Systemen befallen, in Österreich sind es drei von tausend. Das alleine sagt jedoch nur wenig darüber aus, wie viele infizierte PCs es insgesamt gibt. Relevant ist auch der Anteil an PCs, die laufend aktualisiert und daher gescannt werden. Gerade das ist häufig bei infizierten PCs nicht der Fall, da sie oft mit veralteter Software betrieben werden oder Malware automatische Updates verhindert.

Neben Viren stellen vor allem aber auch Botnetze noch immer – trotz ihrer intensiven weltweiten Bekämpfung – ein Problem dar, wenn auch in etwas geringerem Ausmaß.

CERT.at – die österreichische Internet-Feuerwehr

Betrachtet man das Handlungsumfeld von CERT.at, so lassen sich neben routinemäßigen Eingriffen auch einige größere Phänomene erkennen. Die CERT-Leistungen sind dabei sehr vielfältig und abwechslungsreich, behandeln aber immer aktuelle Sicherheitsbedrohungen im Internet.

Dazu setzt CERT.at sehr stark auf die Zusammenarbeit und Abstimmung mit internationalen CERTs. Zusätzlich vertraut man auf

1: Quelle: Norton Cybercrime Report 2011; BM.I Büro für Kriminalstrategie

die eigens entwickelte Sensorik, mit der proaktiv das österreichische Internet auf potenzielle und tatsächliche Bedrohungen hin untersucht wird. Im Falle konkreter Bedrohungen ist es CERT.at, das entsprechende Warnungen veröffentlicht und Reports zur Behebung des Sicherheitsproblems herausgibt.

Aktiv wird das CERT-Team in erster Linie, wenn es die Ereignisse erfordern. Dies kann aufgrund von Alarmierung bzw. Verständigung durch Partnerorganisationen der Fall sein oder auch auf eigene Initiative erfolgen. CERT.at bearbeitet akribisch alle eingehenden Meldungen über sicherheitsrelevante Vorkommnisse und entscheidet anlassbezogen über die weitere Vorgehensweise. Handelt es sich tatsächlich um Bedrohungen, die ein akutes Eingreifen notwendig machen, so liegt die Hauptarbeit von CERT.at in weiterer Folge darin, Informationen darüber unmittelbar an die jeweiligen Internet Service Provider (ISPs) bzw. Domaineigentümer weiterzugeben. 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 hingegen kann letztlich nur durch die Betroffenen selbst erfolgen.

Ergänzt wird das vorhin genannte Aufgabenspektrum auch durch projektbezogene Arbeit, wie aktuell etwa im Rahmen der Entwicklung einer österreichischen Cyber Security Strategie. Hinzu kommen zahlreiche Vorträge zur Bewusstseinsbildung und Information oder etwa die laufende Kontaktpflege mit nationalen und internationalen Ansprechpartnern.

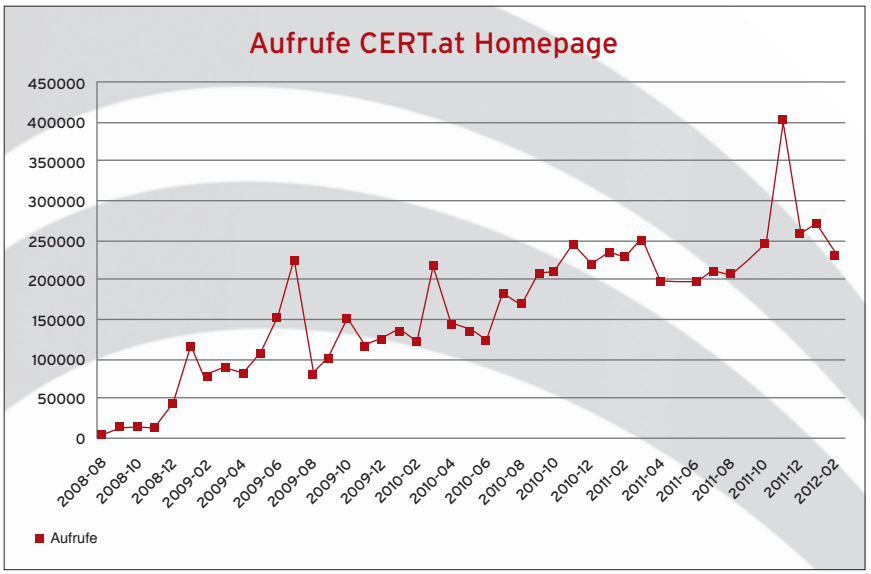


Abbildung 1: Die ansteigenden Zugriffe auf die CERT.at Homepage veranschaulichen die Bedeutung von CERT.at.

GovCERT.gv.at stellt sich vor

GovCERT.gv.at ist das Government Computer Emergency Response Team für die öffentliche Verwaltung und die kritische Informations-Infrastruktur (KII) in Österreich. Seit April 2008 betreibt das Bundeskanzleramt diese Einrichtung in Kooperation mit CERT.at zur Behandlung bzw. Verhinderung von Sicherheitsvorfällen im Bereich der Informations- und Kommunikationstechnologien (IKT). Dabei erfüllt GovCERT.gv.at auf nationaler Ebene eine Koordinationsfunktion zwischen den einzelnen Stellen der öffentlichen Verwaltung und den Betreibern kritischer Infrastruktur. Auf internationaler Ebene agiert GovCERT.gv.at 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 Interessenten weiter.

AUSGEWÄHLTE CERT-THEMEN IN DER RETROSPEKTIVE

CERT-Verbund für mehr Datensicherheit

Die Hackerangriffe in jüngster Zeit haben gezeigt, dass Informations- und Kommunikationssysteme verletzbar sind. Um diese für das tägliche Leben relevanten Systeme sicherer zu machen, wurde Ende 2011 auf Initiative des österreichischen GovCERT.gv.at und des BMLVS ein Österreichischer CERT-

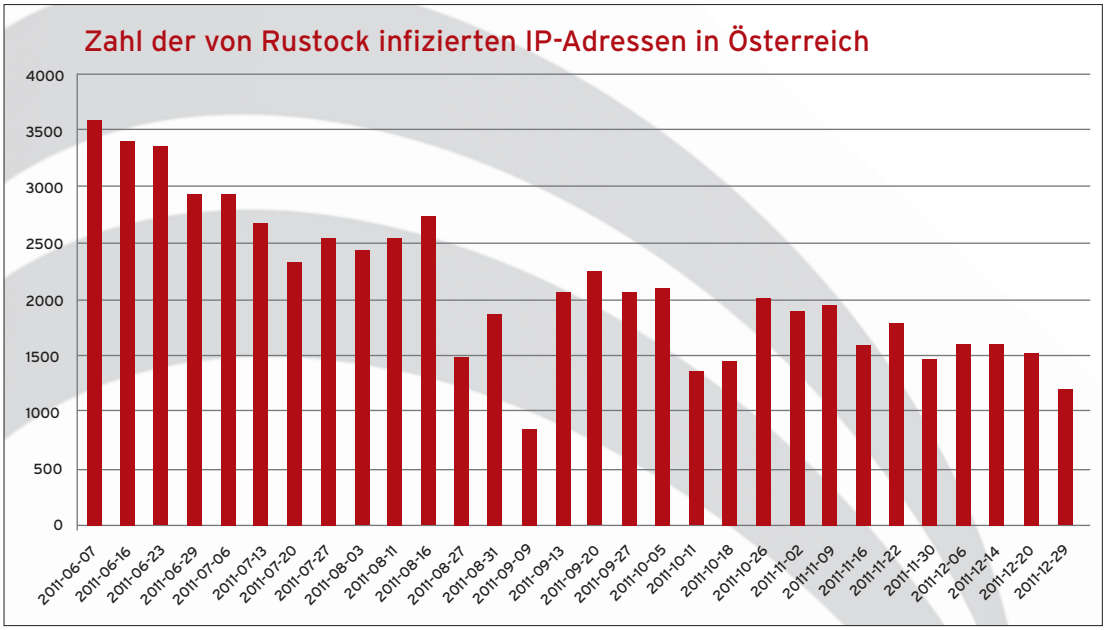


Abbildung 2: Erste Erfolge in der Zurückdrängung von Rustock in Österreich – doch der Kampf dauert weiter an.

Verbund ins Leben gerufen. Im Mittelpunkt der Zusammenarbeit stehen der Schutz von IKT-Infrastrukturen, der Informationsaustausch und die rasche Reaktion auf Bedrohungen. In Form 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/CERT.at unter anderem das ACOnet CERT, Raiffeisen-IT CERT, das Bundesrechenzentrum, WienCERT und das BMLVS. Durch die Zusammenarbeit soll nicht nur die Qualität der Services steigen, sondern auch ein für den möglichen Ernstfall relevanter Wissensvorsprung aufgebaut werden.

Langwieriger Kampf gegen Botnetze

Botnetze sind immer noch ein weit verbreitetes Problem, obwohl der international koordinierte Kampf bereits über Jahre andauert. Bei Botnetzen handelt es sich um versteckte Netzwerke von „Zombie-Rechnern“. Organisierte Internetkriminelle nutzen – zumeist völlig unbemerkt – die Netzanbindung und die Rechenkraft von tausenden von infizierten Computern weltweit für den Versand von E-Mail-Spams, Phishing, Identitätsdiebstahl, Klickbetrug und anderen kriminellen Handlungen. Manche Botnetze existieren schon seit Jahren und kontrollieren Hunderttausende Rechner weltweit. Gesteuert werden sie meist über einige wenige Kommando- und Kontrollserver. Das Botnetz Rustock zählt zu dieser Kategorie. Es wurde erstmals 2006 entdeckt und begann über Jahre hinweg immer stärker aufzutreten. Mitte 2010 zählte es zu den am weitesten verbreiteten Bedrohungen von Computern weltweit. Nachdem Microsoft Mitte 2011 selbst Kontrolle über Kontrollserver erlangen konnte, gelang es Rustock sukzessive zurückzudrängen. Eine weitere Folge war, dass nun erstmals mitprotokolliert werden konnte, von welchen IP-Adressen aus sich Mitglieder des Botnetzes gemeldet haben. Microsoft gibt diese Informationen an die nationalen CERTs weiter. Auch CERT.at bekommt seither laufend Informationen über infizierte österreichische IP-Adressen und unterstützt bei der Bereinigung. Die von CERT.at in Kooperation mit den ISPs gesetzten Maßnahmen sind erfolgreich: So konnte binnen 6 Monaten die Anzahl der infizierten IP-Adressen von Rustock in Österreich halbiert werden. Parallel erhält CERT.at auch laufend Feeds mit österreichspezifischen Informationen zu anderen Botnetzen und informiert im Bedarfsfall ISPs oder die Domaininhaber.

Conficker – totgeglaubte Würmer leben länger

Anfang 2009 tauchte Conficker zum ersten Mal im Web auf und suchte nach einem bestimmten Schlupfloch im Betriebssystem Windows. Zwar hatte Microsoft bereits Ende 2008 für diesen Fehler einen Patch bereitgestellt und veröffentlicht, trotzdem konnte sich der Wurm millionenfach im Internet und in Firmennetzen verbreiten, da Updates von

vielen Benutzern nicht eingespielt und auf aktuelle Schutzsoftware verzichtet wurde. In Österreich erlangte der Wurm Berühmtheit, als er Anfang 2009 ca. 3.000 Rechner der Kärntner Landesregierung lahm legte und sich auch in der Krankenversorgung ausbreitete. Selbst heute ist Conficker noch immer ein Problem. Trotz intensiver Bemühungen im Kampf gegen den Wurm in all seinen Variationen sieht CERT.at den generellen Trend, dass Infektionen nur sehr langsam abnehmen. Auch hier liegt die Verantwortung letztlich bei den PC-Usern dafür zu sorgen, dass ihre Systeme am aktuellen Stand und mit Schutzsoftware ausgestattet sind.

Google Conditional Hacks

Mit einem relativ neuartigen Problem befasst sich CERT.at seit Mitte 2011, den sog. Google Conditional Hacks. Dabei werden bestehende Websites gehackt und schädlicher PHP-Code eingeschleust. Dieser manipuliert den Inhalt der Webseite abhängig davon, wer sie besucht. Ist es der Webcrawler von Google (GoogleBot), 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 nach einer solchen Suche auf der Webseite, dann schickt der PHP-Code des Einbrechers den Besucher auf einen passenden Webshop. Es wird also das Google-Ranking der legitimen Seite ausgenutzt, um dubiose Pillenshops als Top-Treffer bei Google zu platzieren. Der Webseitenbetreiber merkt davon oft nichts und seine Kunden sehen keine Veränderungen, nur der Google-Cache zeigt die manipulierte Seite an. CERT.at durchforstet daher auch laufend österreichische Webseiten auf diese Manipulationen und warnt gegebenenfalls die Betreiber.

Anonymous-Attacken

In den vergangenen Jahren erlebten wir die Entwicklung vom Ego-Hacker der alten Schule hin zu arbeitsteilig arbeitenden Kriminellen und professionell agierenden Spionen, die beide das Internet als Betätigungsfeld gefunden haben. In letzter Zeit hat sich noch eine weitere Motivation für Hacker herausgebildet: Hacktivism. Hierbei geht es um die Übertragung von Aktivismus in die Online-Welt. Anstelle von Demonstrationen, Blockaden und anderen Störaktionen im realen Leben wird jetzt auch im Internet mit teilweise klar illegalen Methoden versucht, Medienaufmerksamkeit für Themen zu finden, und so die Gesellschaft zu verändern.
Unter dem Namen „Anonymous“ hat sich eine Bewegung gebildet, die global mittels Einbrüchen, Denial-of-Service Angriffen und dem Veröffentlichen von geheimen Daten gezielt Firmen und Regierungen angegriffen hat. Die Motivationen dafür reichten von simplem „Spaß“ („for the Lulz“), über die „Bestrafung“ von Firmen (Sony, Paypal etc.) bis hin zu politischen Protesten (ACTA). Auch in Österreich kam es zu Vorfällen, die einer lokalen Splittergruppe („AnonAustria“) der Bewegung zuzurechnen sind. Diese Gruppen sind sehr lose organisiert, haben keine Kommandostrukturen und nutzen diverse Onlinedienste um anonym im Internet zu agieren.

Erste prominente Opfer waren in Österreich im Juli 2011 die Webseiten einiger Parteien sowie die GIS. In allen Fällen wurden Startseiten verändert, sensible Daten kopiert und zum Teil veröffentlicht. Es folgten noch weitere Vorfälle (Polizistendaten, Sozialversicherungsdaten aus Tirol, WKÖ etc.) sowie einige Denial-of-Service Angriffe.

Die Teams von CERT.at und GovCERT.gv.at waren bei mehreren Fällen aktiv bei der Vorfallsbehandlung im Einsatz: So etwa wurde vor Ort Hilfe bei der Forensik, der Absicherung und der Medienarbeit geleistet sowie der Prozess der dauerhaften Korrektur begleitet. In den anderen Fällen agierte CERT (sowohl CERT.at, als auch GovCERT.gv.at) als Koordinator im Hintergrund, um Erfahrungswerte zusammenzufassen und an Betroffene weiterzugeben.

INTERNATIONALE ÜBUNGEN IM KAMPF GEGEN CYBER BEDROHUNGEN

Cyber Bedrohungen sind selten auf einzelne Staaten beschränkt. Die globale und grenzenlose Natur des Internets führt dazu, dass es für die Bewältigung von Krisen eine internationale Vernetzung der Sicherheitsteams braucht. Aus diesem Grund haben GovCERT.gv.at und CERT.at in jüngster Vergangenheit an mehreren internationalen Übungen teilgenommen, bei denen die länderübergreifende Zusammenarbeit getestet wurde.

Zielsetzungen

Technische Hintergründe und Szenarien standen dabei nicht im Vordergrund. Es ging darum, Strukturen in anderen Staaten und Kontaktmöglichkeiten kennenzulernen bzw. zu testen sowie Vertrauen aufzubauen. So wird die gemeinsame Problemlösungskompetenz und Zusammenarbeit geübt und verbessert. Die verwendeten Szenarien waren ein fiktiver Vorwand, um Prozesse zu testen und zu optimieren. Bei den bisherigen Übungen handelte es sich daher nicht um Drill-Übungen, sondern um offene Übungsszenarien um herauszufinden, wie die Kommunikation und Zusammenarbeit im Falle des Falles tatsächlich ablaufen könnte.

Bei internationalen Vorfällen ist die rasche und effektive Zusammenarbeit zwischen Staaten essenziell. Dies funktioniert nur, wenn sich die beteiligten Teams kennen und vertrauen. Auch sollten die Teilnehmer ihr Verständnis verbessern, wie konkrete Vorfälle in einem internationalen Kontext und auf Landesebene behandelt werden. Daher wurden Kommunikation und Koordination nicht nur länderübergreifend, sondern auch innerhalb eines Staates getestet.

Unterschiedliche Szenarien

Auch wenn die tatsächliche Übungsdauer meist nur bei einigen Stunden liegt, so erstreckt sich die Vorbereitung oft über mehrere Monate bis hin zu einem Jahr – unter Einbindung vieler internationaler Beteiligter. Die Übungsszenarien sind unterschiedlich bzw. bauen aufeinander auf.

GovCERT.gv.at und CERT.at haben bislang aktiv an folgenden Übungen teilgenommen:

- CyberEurope 2010
- EuroCybex 2011
- CyberAtlantic 2011

Auf europäischer Ebene gab es mit der CyberEurope 2010 bislang die bedeutendste Übung. Zur Vorbereitung gab es Workshops, in denen Szenarien und Übungsannahmen vereinbart wurden. Getestet wurde nicht die technische Kompetenz der Teilnehmer, sondern deren Umgang mit Krisensituationen. Die Realitätsnähe war für den Übungsverlauf unerheblich.

Lessons learned & Ausblick

Die Analyse der Übungsergebnisse hat gezeigt, dass es in Europa kein einheitliches Modell gibt, wie mit konkreten Gefahrensituationen umgegangen wird. CERTs sind vielerorts unterschiedlich strukturell und organisatorisch verankert. Auch ist die internationale Zusammenarbeit für europäische Verhältnisse relativ neu. Es gibt Potenzial, den gemeinsamen Kampf gegen Cyber Bedrohungen auf europäischer und internationaler Ebene zu intensivieren. Mit den bislang durchgeführten Übungen wurden erste, wichtige Schritte in diese Richtung gesetzt. Auch der persönliche Kontakt der Beteiligten und das gegenseitige Aufbauen von Arbeitsbeziehungen sind von entscheidender Bedeutung für den Erfolg. In Österreich kommen GovCERT.gv.at und CERT.at wichtige Rollen im Krisenmanagement zuteil. Die nächste pan-europäische Übung CyberEurope 2012 findet im Oktober 2012 statt – GovCERT.gv.at ist erstmalig im Planungsteam vertreten.

Pilotprojekt Softwareverteilung mittels DVB-T

GovCERT.gv.at und CERT.at arbeiten abseits der laufenden Tätigkeit parallel auch immer wieder an verschiedenen Projekten. Die „Emergency Software Distribution mittels DVB-T“ ist ein solches. Hintergrund ist die Fragestellung, wie in einer Notfallsituation (zB großflächiger Ausfall des Internets und anderer Kommunikationsformen) Patches, Updates oder andere Softwarepakete an kritische Infrastrukturbetreiber oder lokale Behörden verteilt werden können.

Ein möglicher Lösungsansatz hierbei ist der Einsatz von DVB-T (Digital Video Broadcasting). Durch Nutzung freier Kapazitäten von Fernsehkanälen lassen sich in der Theorie auch Daten verschicken. Im Zuge eines gemeinsamen Pilotprojekts von GovCERT.gv.at, dem ORS und Global Communication & Services GmbH wurde erprobt, ob sich dieser Ansatz in die Praxis umsetzen lässt. Im Zuge verschiedener Testreihen und –szenarien gelang es, erfolgreich Softwarepakete über das Trägermedium DVB-T zu übermitteln. Zum Einsatz kamen dabei Mini-PCs mit DVB-T Empfangskarten als Empfänger, ein zentraler Encoder beim ORS und die Mitnutzung eines der Transponder am Sender Kahlenberg. Durch den erfolgreichen Abschluss der Evaluierungsphase wurde die Machbarkeit der Idee bewiesen und in diesem Zusammenhang die innovative Rolle Österreichs unterstrichen. Ob die Projektidee weiter verfolgt und ausgebaut wird ist abhängig von rechtlichen und finanziellen Rahmenbedingungen und daher derzeit noch nicht endgültig geklärt.

© Luftbildfotograf - Fotolia.com

GovIX – das österreichische Behördennetz

© frank peters - Fotolia.com

Das Datenaufkommen steigt ständig und so haben auch Einrichtungen der öffentlichen Verwaltung in Österreich einen steigenden Bedarf an leistungsfähiger und betriebssicherer Informations- und Telekommunikationsinfrastruktur. Mit dem GovIX (Government Internet eXchange) steht Österreichs Behörden dabei ein leistungsfähiges, gemeinsam nutzbares und vor allem komplementäres Netz zur Verfügung.
Über den GovIX wird die IT-Kommunikation zwischen Einrichtungen der öffentlichen Verwaltung vom öffentlichen Internet unabhängig. Zahlreiche öffentliche Stellen nutzen das österreichische Wissenschaftsnetz ACOnet als Anbindung an das Internet. Das gibt ihnen auch die Möglichkeit, am GovIX teilzunehmen und so eine direkte Kommunikation untereinander nutzen zu können. Genutzt wird GovIX unter anderem vom Bundeskanzleramt, dem BRZ, verschiedenen Ministerien, dem Magistrat Wien, der Präsidentschaftskanzlei oder etwa auch den Ländern Oberösterreich und Steiermark.

Ein wesentlicher Vorteil von GovIX ist der autonome Betrieb, unabhängig vom offenen Internet. Dadurch lassen sich Verkehrsströme optimieren und Kosten sparen sowie im Falle von Störungen der Internetverbindung die Behördenkommunikation aufrechterhalten. Damit dieser Betrieb zuverlässig und sicher gewährleistet werden kann, stellt das GovCERT.gv.at Nameserver und DNS-Services zur Verfügung (Nameserver für die DNS-Root, „.at“ und „.gv.at“, sowie secondares für alle Teilnehmer). Wie sinnvoll der Einsatz von GovIX ist, hat sich bereits bei einem Ausfall der Internet-Anbindung des Landes Steiermark gezeigt: Durch das komplementäre System konnte die Kommunikation der Behörden aufrechterhalten werden.

SICHERUNG KRITISCHER INFRASTRUKTUREN:

Das österreichische Programm CIP (Austrian Critical Infrastructure Protection)

Gastkommentar von MR Mag. Alexander Pschikal, Abteilung sicherheitspolitische Angelegenheiten im Bundeskanzleramt

Der Schutz kritischer Infrastrukturen ist seit Jahren fixer Bestandteil des sicherheitspolitischen Diskurses. Doch was verstehen wir darunter? Kritische Infrastrukturen sind jene Infrastrukturen oder Teile davon, die eine wesentliche Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen haben. Ihre Störung oder Zerstörung hat schwerwiegende Auswirkungen auf die Gesundheit, Sicherheit, das wirtschaftliche und soziale Wohl der Bevölkerung oder die effektive Funktionsweise der privaten Wirtschaft und/oder von staatlichen Einrichtungen.

Das österreichische Programm zur Sicherung kritischer strategischer Infrastrukturen

Die Entwicklung des österreichischen Programms zum Schutz kritischer Infrastrukturen (APCIP) begann 2005 und baute auf den Erfahrungen der EU auf. Ziel ist, Organisationen und Unternehmen von strategischer, das heißt nationaler Bedeutung, zu identifizieren und durch präventive Maßnahmen und Maßnahmen zur Schadensbehebung vor Störung und Zerstörung zu bewahren. Dieser ‚all-hazard approach' umfasst nicht nur terroristische Bedrohung, organisatorische, rechtliche, technische und intentionale Risiken inklusive der Markt- und Naturrisiken, sondern auch Risiken, die sich aus der Anwendung der IKT ergeben.

Die Risikofelder sind vielfältig:

- Sie umfassen alle Natur-, Umwelt- und Technologiekatastrophen inklusive humaner und veterinärer Epidemien.
- Liegen in der Art der Organisation der Unternehmen selbst.
- Reichen von fahrlässiger Arbeit bis zu kriminellen Handlungen inklusive organisierter Kriminalität und terroristischer Anschläge.
- Wachsen durch die Abhängigkeit von der Informations- und Kommunikations-Technologie und deren Komplexität, Vernetzung und Mobilität.
- Verstärken sich noch durch Wechselwirkungen und Dominoeffekte einer hoch differenzierten Gesellschaft und Wirtschaft.

Fokus auf kritischer Infrastruktur

Das österreichische Programm unterstützt deshalb den Aufbau eines integrierten und umfassenden Risiko- und Krisenmanagements in jenen Unternehmen, die Leistungen der „strategisch wichtigen" Infrastruktur erbringen. Risikomanagement ist Prävention und versteht sich als Verringern von Eintrittswahrscheinlichkeit und Verwundbarkeit durch Vermeiden, Vermindern und Überwälzen von Risiken. Krisenmanagement versucht hingegen den bereits eingetretenen Schaden zu minimieren.

Bis in die 80iger Jahre waren viele Infrastrukturen, die heute als „kritisch" angesehen werden, im Eigentum der öffentlichen Hand. Teile der Energieversorgung und des Transportsystems, Gesundheits- und Sozialeinrichtungen, die Wasserversorgung und Bildungseinrichtungen sind es unter dem Begriff „Daseinsvorsorge" in Österreich heute noch. Mit dem Rückzug des Staates aus privatwirtschaftlichen Aktivitäten sind die Ansprechpartner und Hauptakteure zum Schutz kritischer Infrastrukturen zweifels-

ohne Unternehmen geworden, die strategische Funktionen erfüllen. Der Staat kann diese letztlich nur unterstützen, die Verantwortung liegt bei der Unternehmensleitung und den Eigentümern.

Derzeit wird eine Liste kritischer Infrastrukturen auf Bundesebene fertig gestellt, die ca. 400 Organisationen und Unternehmen umfasst. Die Einrichtungen der Verwaltung, insbesondere die Bundesministerien wurden ebenfalls als strategisch eingestuft, da deren Tätigkeit von keiner anderen Organisation wahrgenommen werden kann. Die öffentliche Hand kann nur Hilfestellungen geben, mit welchen Gefahren und Risiken ein Unternehmen intern und extern konfrontiert sein kann. Deshalb wurde vom Bundeskanzleramt das Handbuch „Sicherheit in Unternehmen mit strategischer Bedeutung für Österreich“ erstellt, das eine Selbstevaluation in Form eines umfassenden Fragebogens ermöglicht, mit dem die eigene strategische Position erkannt werden kann. Die Bestellung eines „Sicherheitsbeauftragten“ im Unternehmen unterstützt darüber hinaus auch die Kommunikation nach außen.

Die meisten Unternehmen, die bisher identifiziert wurden, haben Risiko- und Krisenmanagementinstrumente an Hand von nationalen und internationalen Normen großteils eingeführt. Auf diesen wird im österreichischen Programm aufgebaut. Die öffentliche Hand will Unterstützung dafür geben, dass Präventions- und Vorsorgemaßnahmen möglichst das ganze Spektrum an Risiken und Gefahren abdecken. Denn das schwächste Glied einer Kette definiert bekanntlich deren Gesamtbelastungsfähigkeit.

Erfolgsmodell Austrian Trust Circles

Ein Informationsmanagement ist derzeit im Aufbau, das die Entwicklung von Partnerschaften in der Form von Public-Private-Partnerships unterstützen soll. Hier bekommen Risikomanager die Möglichkeit, einerseits Informationen untereinander auszutauschen und andererseits gemeinsam Gegenstrategien zu entwickeln. Diese Vorgangsweise wird im CERT.at und in den Austrian Trust Circles bereits erfolgreich umgesetzt. In regelmäßigen Treffen diskutieren und beraten Unternehmens- und Behördenvertreter dort über Strategien und Ansätze, wie kritische Systeme geschützt werden können und tauschen gegenseitige Erfahrungen aus.

Letztlich sollen das Programm zur Sicherung kritischer Infrastrukturen, eine IKT Sicherheitsstrategie (Cyber Security Strategie) und die Austrian Trust Circles dazu beitragen, das Bewusstsein für vorhandene Risiken auf allen Ebenen zu stärken und damit die Attraktivität des Wirtschaftsstandorts Österreich und die Daseinsvorsorge für die Bevölkerung weiterhin abzusichern und auszubauen.

Austrian Trust Circle

Der Austrian Trust Circle ist eine Initiative von CERT.at und dem österreichischen Bundeskanzleramt und besteht aus Security Information Exchanges in den einzelnen Bereichen der strategischen Informationsinfrastruktur (CIIP). CERT.at bietet in Kooperation mit GovCERT Austria und dem österreichischen Bundeskanzleramt einen formellen Rahmen für praxisnahen Informationsaustausch und gemeinsame Projekte im Sicherheitsbereich. Neben sektorspezifischen Treffen wurde im Mai 2012 bereits zum 2. Mal erfolgreich das sektorübergreifende 2. Austrian Trust Circle Treffen abgehalten. Hierbei fand Informationsaustausch zwischen Vertretern aus Unternehmen der kritischen Infrastruktur (Gesundheit, Transport, Finanz, Industrie, Energie) statt, als auch Diskussionen mit Vertretern des Bundeskanzleramts, des Bundesministerium für Inneres und des Bundesministerium für Landesverteidigung und Sport.

Ziele des Austrian Trust Circle

- Unterstützung der Selbsthilfe in den Sektoren im Bereich Sicherheit
- Operative Kontakte für CERT.at bei der Information über und Behandlung von Sicherheitsvorfällen in den Organisationen
- Operative Experten für Behörden und Teilnehmer im Krisenfall
- Schaffen einer Vertrauensbasis um im Ernstfall gemeinsam agieren zu können
- Vernetzung und Informationsaustausch in und zwischen den Sektoren der strategischen Infrastruktur

HILFE ZUR SELBSTHILFE

Ratschläge und Hinweise zum Schutz vor Angriffen

Die Gefahr lauert immer und überall

Unternehmen und Privatanwender sind zunehmend Angriffen aus dem Cyberspace ausgesetzt. Um sich bestmöglich davor zu schützen ist es wichtig, neben notwendigen technischen Rahmenbedingungen auch auf entsprechende Meinungsbildung und das individuelle Bewusstsein zu setzen. Denn vielfach ist es der Faktor Mensch, der Angreifern nur allzu leichtes Spiel macht.

Einfache Sicherheitstipps für schnellen Schutz

Bereits durch wenige und einfach umzusetzende Maßnahmen lassen sich mögliche Bedrohungspotenziale vermeiden bzw. stark verringern. Die nachfolgende Aufzählung bietet gute Ansätze, gilt aber als demonstrative Auswahl:

1. Computer auf dem aktuellsten Stand halten

Wird die Software von Computern (vom Smartphone bis zum Server) immer auf dem letzten Stand gehalten, lässt sich bereits ein Großteil der laufend stattfindenden Angriffe abwehren. Durch die Aktualisierung mit Patches, Updates oder sonstigen Softwarekorrekturen kann verhindert werden, dass Angreifer aktuelle Sicherheitslücken ausnutzen können. Zwar schützt die Aktualisierung von Systemen nicht vollständig gegen Angriffe, jedoch wird es Angreifern dadurch wesentlich schwerer gemacht. Was für PCs, Laptops und Server gilt, gilt selbstredend auch für Web-Applikationen, Netzwerkgeräte und mobile Geräte wie Smartphones oder Tablets. In vielen Fällen erleichtern die Systeme selber diese Aufgabe: ein automatisches Update lässt sich bei vielen Programmen konfigurieren. Weiters gibt es Werkzeuge, die nötige Wartungsarbeiten anzeigen.

2. Angriffsflächen minimieren

Software, die nicht installiert ist, kann auch nicht ausgenutzt werden. Manche Angreifer versuchen ihre Opfer mit Tricks dazu zu bringen, dass sie Schadsoftware installieren. Typischer Trick ist das Vorgaukeln einer Infektion mit Hinweis auf „Tools“ zum Beheben (Fake-AV) oder der Hinweis, dass man für ein bestimmtes Video „Codecs“ installieren muss. Die Grundregel hier ist, dass man nur die Software installieren soll, die man selber aktiv gesucht hat. Wenn man Software nicht mehr braucht, sollte diese auch wieder deinstalliert werden.

3. Sicherheitseinstellungen prüfen

Häufig werden vorhandene Sicherheitseinstellungen – meist aus Gründen des Komforts – bewusst zurückgestuft und so ihrer maximal möglichen Wirkung beraubt. Daher sollten Sicherheitseinstellungen am Computer und in Programmen (wie zB Web-Browser) entsprechend ihrer Möglichkeiten auch genutzt werden, damit der größtmögliche Schutz gewährleistet werden kann. In Unternehmensnetzwerken lassen sich Sicherheitsrichtlinien zudem zentral verwalten.

4. Verwendung von Sicherheitssoftware
Studien haben ergeben, dass jeder fünfte Internetnutzer ohne Virenschutz und Firewall surft. Und das, obwohl bereits 70% der Nutzer mindestens einmal negative Erfahrungen im Web gemacht haben.[1] Der Einsatz von Anti-Virenprogrammen und Firewalls bietet weiteren Schutz vor Angriffen aus dem Internet. Zudem sind zahlreiche Programme für Privatanwender auch kostenlos erhältlich und mindern die Gefahr, die von Viren, Trojanern und anderer Malware ausgeht. Doch selbst wenn aktuelle Software am Rechner installiert ist, kann sie ihre volle Wirkung nur dann entfalten, wenn sie auch gestartet wurde und im Hintergrund alle Aktivitäten und Prozesse überwacht. Ein Anti-Virenprogramm ist wie das ABS im Auto: Es kann manche Unfälle verhindern, macht den Fahrer aber nicht unverwundbar und ist somit kein Ersatz für überlegtes Handeln.

5. Mitdenken und eigene Verhaltensweisen hinterfragen
Technische Maßnahmen bieten bereits einen großflächigen Schutz. Der angreifbarste Faktor ist und bleibt hingegen der Mensch. Mitarbeiter in Unternehmen wie auch Privatanwender sind aufgerufen, grundsätzlich verdächtig erscheinende Inhalte erst gar nicht zu öffnen sondern im Zweifelsfall zu löschen. Das gilt für das Öffnen von E-Mails und Anhängen von Absendern, die nicht vertrauenswürdig erscheinen genauso wie auch für die Bekanntgabe von persönlichen Daten. Gesundes Misstrauen hilft. Gerade die Gefahr von Social Engineering – also das Täuschen von Opfern durch Vorspielen falscher Identitäten & Co. – nimmt ständig zu und nutzt die Leichtgläubigkeit vieler Anwender aus.

Unternehmen richtig schützen

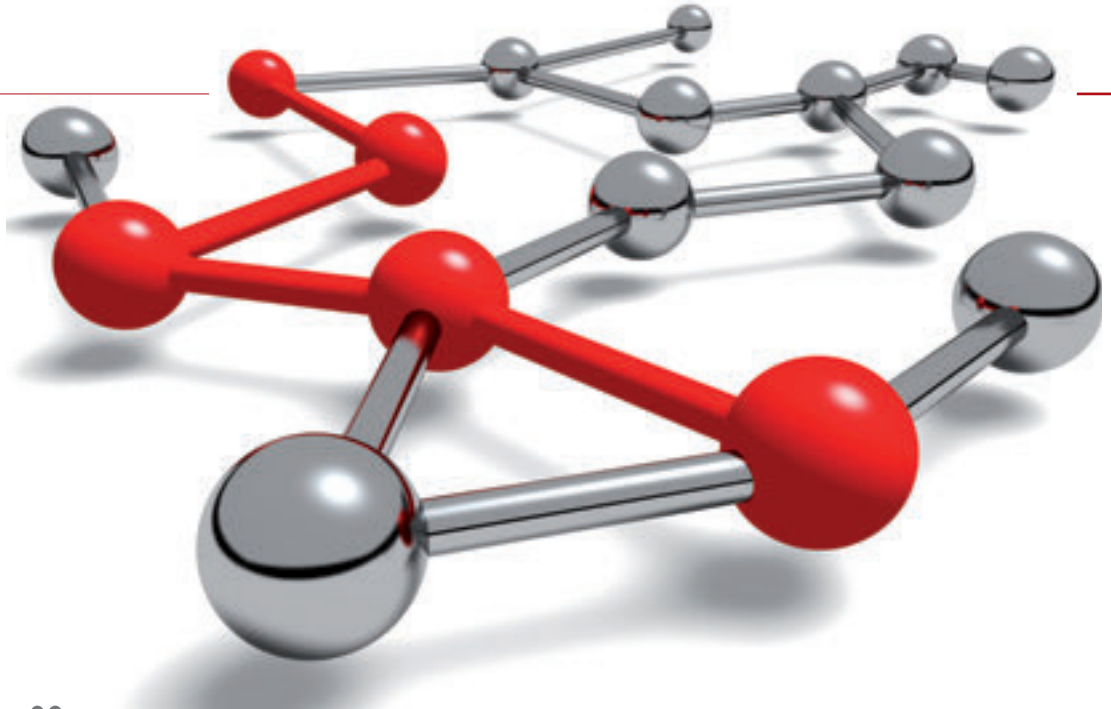
In den letzten Jahren sind verstärkt Unternehmen in den Fokus von Angreifern gerückt. Zahlreiche dokumentierte Fälle von Cyber Spionage verursachten weltweit Schäden in Milliardenhöhe und repräsentieren doch nur die Spitze des Eisberges. Alleine der Schaden von österreichischen Unternehmen aufgrund von Wirtschafts- und Industriespionage wird auf rund 880 Millionen Euro jährlich geschätzt.

Daher bedarf es für Unternehmen eines ganzheitlich durchdachten Sicherheitskonzepts, das sich zu einem Großteil auch mit der IT auseinandersetzt. Es gibt ausführliche Dokumentationen und Leitfäden zum Thema Schutz vor Risiken im IKT-Bereich. So ist es für Unternehmen mittlerweile selbstverständlich, beispielsweise ihre Server in einer Demilitarized Zone (DMZ), geschützt von zumindest einer klassischen Firewall, zu betreiben. Auch der Einsatz von Intrusion Prevention Systemen (IPS), Web Application Firewalls (WAF) und Content-Filtern für Nutzer nehmen immer mehr zu.

Doch Prävention hilft nur so lange, bis sie fehlschlägt. Ein vollständiges Sicherheitskonzept enthält daher auch Maßnahmen, die der möglichst frühzeitigen Erkennung von erfolgreichen Angriffen dienen. Unternehmen stehen in diesem Zusammenhang eine Reihe an Ressourcen zur Verfügung. Exemplarisch zu erwähnen sind das A-SIT Sicherheitshandbuch, IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI), ISO 27000 Standards, Information Security Management Systeme (ISMS) sowie die professionelle Unterstützung von Consultingfirmen und anderen Experten. CERT.at hat zudem seine Erfahrungswerte aus den Webserver-Sicherheitsvorfällen von 2011 in einem eigenen Report zusammengefasst (zu finden unter http://www.cert.at/warnings/specials/20111122.html).

Zuletzt darf aber nicht vergessen werden, dass man mit Anti-Schadsoftware und hoher Aufmerksamkeit aller Beteiligten nicht alle Gefahren komplett ausschließen kann. Hier bleibt neben der erhöhten Aufmerksamkeit der Nutzer nur die ständige Suche nach verdächtigem Verhalten von infizierten PCs als Abwehrstrategie.

1: Studie „IT-Kriminalität in Deutschland" des Bundesverbandes für Informationswirtschaft, Telekommunikation und Neue Medien, Juni 2011



ÜBER CERT.AT

CERT.at und GovCERT.gv.at stellen sich vor

Wie alles begann

Als 1988 der erste Internet-Wurm eine beträchtliche Anzahl an IT-Systemen angegriffen und lahmgelegt hat, wurde der Welt erstmals die Notwendigkeit von organisierten und aufeinander abgestimmten Schutzmaßnahmen schmerzlich vor Augen geführt. Daher wurde kurz darauf das erste Computer Emergency Response Team (CERT) an der Carnegie Mellon University in Pittsburgh in den USA gegründet. Die Thematik hat vier Jahre später auch Europa erfasst, wo 1992 die erste europäische Einrichtung dieser Art in den Niederlanden entstand. Heute zählt die europäische Agentur für Netzsicherheit ENISA (European Network and Information Security Agency) weit über 100 akkreditierte CERTs auf. Die Bezeichnung CERT ist mittlerweile die geläufigste Form, häufig wird aber auch von CSIRT (Computer Security Incident Response Team) oder anderen Abkürzungen wie SERT, CIRT, IRT oder z.B. auch WARP (Warning, Advice and Reporting Point) gesprochen.

CERT.at und GovCERT.gv.at in Österreich

CERT.at und GovCERT.gv.at wurden 2007 als gemeinsame Initiative von Bundeskanzleramt und der Internet Foundation Austria (IPA) gegründet und nahmen im März 2008 ihre operative Arbeit auf. Seither sind sie 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). Im Fokus stehen all jene, die strategisch wichtige und kritische Infrastruktursysteme zur Verfügung stellen bzw. betreiben – sowohl auf öffentlicher als auch privater Seite.

Was CERT.at ist – und was nicht

CERT.at versteht sich als Kontaktpunkt für sicherheitsrelevante IKT-Ereignisse in Österreich und dient als vertrauenswürdige und anerkannte Informationsdrehscheibe. Zu den Aufgaben zählen die Koordination von Security Incidents, die öffentliche Information sowie die Schaffung von Awareness für Sicherheitsanliegen. Zusätzlich – durch die internationale Vernetzung – ist CERT.at auch der „international sichtbare Partner“ für ausländische CERTs. Hingegen ist CERT.at keine Ermittlungsbehörde noch befasst es sich mit

dem Thema der Strafverfolgung im Internet. Auch handelt es sich bei CERT.at um keine Einrichtung, die völlig isoliert arbeiten kann und ebenso wenig über eine „Wunderwaffe“ gegen alle Sicherheitsprobleme verfügt. CERT.at definiert sich daher selbst als die „Österreichische Internet-Feuerwehr“, die im Falle des Falles eingreift und in enger Abstimmung mit anderen Beteiligten den österreichischen Teil des Internets von Problemen befreit – auf Basis eines freiwilligen Angebots.

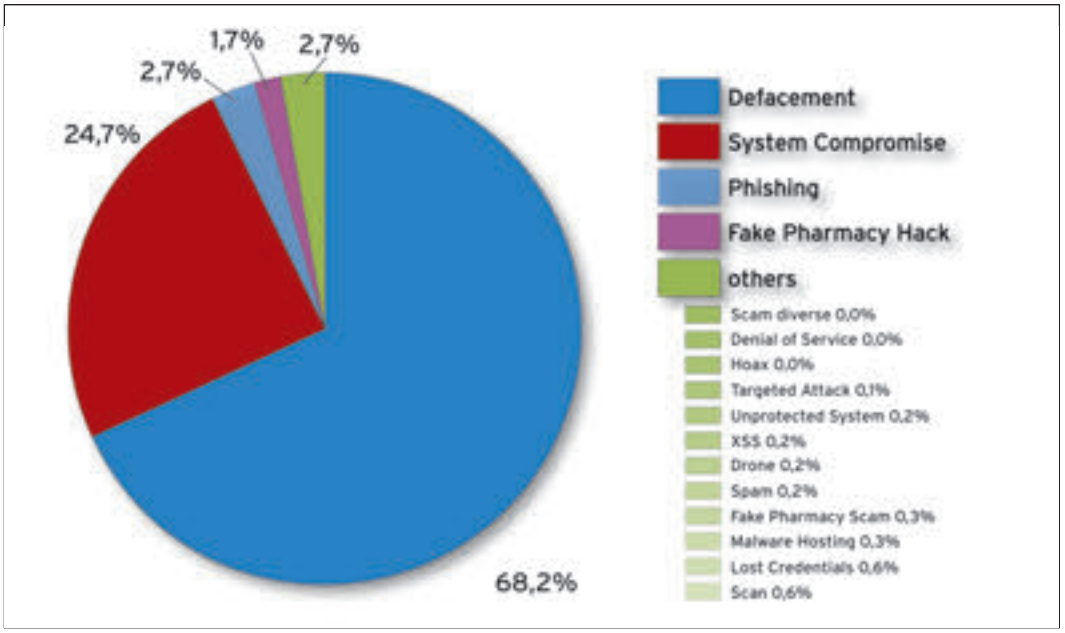


Abbildung 3: Incidents nach Gruppen 2011

Zahlreiche Bedrohungen und ein vielfältiges Handlungsumfeld

Die konkreten CERT.at Leistungen sind dabei sehr vielfältig. Einen Überblick über die wichtigsten Ereignisse und Arbeitsschwerpunkte der jüngsten Vergangenheit finden Sie auf den Seiten 8 bis 15 in diesem Bericht. Im Zentrum der Tätigkeit steht für CERT.at und GovCERT.gv.at immer die akute Sicherheitsbedrohung im Internet. Entweder auf Basis eigener Recherchen oder nach Verständigung durch betroffene Stellen. So arbeitet das österreichische CERT auch intensiv mit ausländischen CERTs zusammen und pflegt einen regen Informations- und Erfahrungsaustausch mit Experten aus aller Welt.

Einen Überblick über das aktuelle Handlungsumfeld von CERT.at gibt die Auswertung der Leistungsstatistik. Diese zeigt auf, mit welchen Anlässen und Themenfeldern sich das CERT-Team im Jahr 2011 beschäftigt hat. So gingen 2011 bei CERT.at insgesamt rund 12.000 Meldungen (sog. „Reports“) über Probleme oder Auffälligkeiten im Internet ein. Diese wurden zu einem Großteil von automatischen Sensoren generiert oder auch selbst ermittelt. CERT.at geht diesen Meldungen nach und schreitet bei tatsächlichen Bedrohungen aktiv ein. So wurde 2011 in über 3.900 Fällen proaktiv die Initiative ergriffen und Probleme mit den jeweils betroffenen Unternehmen, Institutionen oder Privatanwendern gelöst.

Einen Überblick über die am häufigsten vorkommenden Problemfelder (sog. „Incidents“) zeigt die Abbildung oben. Mit einem Anteil von über 2/3 stellen Website Defacements den häufigsten Problemfall dar. Dabei werden Sicherheitslücken ausgenutzt und Websites unberechtigterweise verändert. An zweiter Stelle der Incidents stehen System Compromises, bei denen der eigentliche Besitzer die Kontrolle über ein System verliert. Phishing liegt – bereits mit stark reduzierter Häufigkeit – an dritter Stelle.

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 Botschafter von CERT.at und GovCERT.gv.at und unterstützen damit die Vernetzung des Themas Internetsicherheit in Gesellschaft und Politik

CYBER SECURITY TRENDS

Was bringt die Zukunft?

Wenig überraschend war auch das Jahr 2011 von exponentiellem Wachstum an der Malware-Front gezeichnet. Eine Herausforderung für die Hersteller von Sicherheitssoftware, die mitunter an ihre Grenzen stoßen, alle identifizierten Schädlinge zu erfassen und hinsichtlich Wirkung und Funktionsweise zu analysieren. Insbesondere bei gezielten Angriffen wird es für die Anti-Viren Software schwierig. Wenn die Schadsoftware für einen spezifischen Einsatz programmiert wurde, so finden sich keine passenden Muster in den Signatur-Datenbanken der AV-Industrie. Heuristische und verhaltensbasierte Verfahren helfen zwar noch, sind aber nur eine weitere Stufe im ewigen Katz und Mausspiel.
Denn eines ist sicher: Vollkommene Sicherheit gibt es nicht. Obwohl im internationalen Kampf gegen Cyber Bedrohungen in der Vergangenheit bereits zahlreiche Erfolge erzielt werden konnten, werden Schadprogramme wie Würmer, Viren oder sonstige Malware Anwender auch in Zukunft „begleiten“. Doch neben diesen klassischen Bedrohungsformen haben sich in letzter Zeit neue Felder herauskristallisiert, die laut Experten künftig weitere Ziele potenzieller Angriffe sein werden.

Cloud Computing

Cloud Computing entwickelt sich zu einem weltweiten Trend. Aber die Vorteile und Annehmlichkeiten des Arbeitens in der Wolke bergen auch zahlreiche neue Risiken. Vor allem, da vielfach sensible Daten in die Hände von Dritten „ausgelagert“ werden, die Rechenzentren in allen Teilen der Welt betreiben. Bislang gab es noch keine bekannten größeren Attacken auf Cloud-Netze, sehr wohl aber schon signifikante Ausfälle inklusive Datenverlust. Jedoch ist Cloud-Computing ein noch relativ junger Zweig und

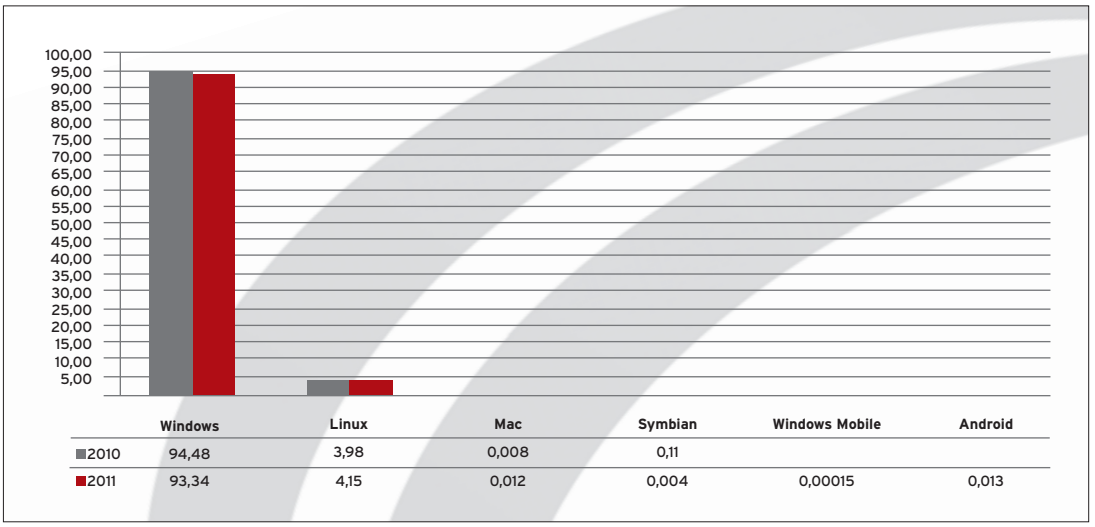
> *„Aus Malware-Sicht stehen wir bei Smartphones und Tablets heute da, wo wir vor 20 Jahren in der PC-Welt gewesen sind. Der Unterschied ist jedoch, dass wir die Entwicklung im mobilen Sektor ungleich exponentieller erleben werden. Es ist davon auszugehen, dass auch im mobilen Segment die Zahl der Malware und auf Malware basierenden Angriffe explosionsartig zunehmen wird.“*
>
> Joe Pichlmayr, IKARUS Security Software

Erfahrungswerte daher Mangelware. Vor allem die zunehmende Vernetzung bietet zahlreiche Möglichkeiten für potenzielle Angreifer und eine Reihe neuer Schnittstellen und Abhängigkeiten erhöhen die Komplexität des Systems. Wie sich das langfristig auf die Sicherheit und Verfügbarkeit dieser Dienste auswirken wird, ist noch unklar. Auch wenn Sicherheit in der Cloud für CERT.at derzeit noch kein unmittelbares Handlungsfeld ist, so werden Entwicklungen diesbezüglich bereits intensiv mitverfolgt und laufend beobachtet.

Zielgerichtete Angriffe im Kommen

Mit Stuxnet wurde 2011 eine neue Dimension von Cyber Angriffen eingeläutet, da der Wurm explizit dafür entwickelt wurde, industrielle Steuerungssysteme im Iran anzugreifen und zu schädigen. Hervorgehoben hat sich Stuxnet vor allem durch den neuen Umstand, dass der Wurm ein bewusster Angriff auf bestehende Systeme war, um diese zielgerichtet zu manipulieren und um zusätzlich reale Auswirkungen zu verursachen. Die Herkunft des Wurms ist bis heute ungeklärt und hat dennoch erstmals weltweit das Gespenst eines möglichen Cyberkrieges heraufbeschworen. Allgemein nehmen Ad-

vanced Persistent Threats (APT) zu. Darunter versteht man zielgerichtete Angriffe (targeted attacks) auf Systeme oder Organisationen, um unerkannt Daten zu exfiltrieren - kurzum Cyber Spionage. Diese Angriffe sind grundsätzlich nicht neu, jedoch durch ihre Folgen ernsthaft bedrohlich. Besonders Regierungen, Behörden oder auch nationale und internationale Hightech-Unternehmen geraten auf diese Weise zunehmend in den Fokus von Angreifern, die beispielsweise hochsensible Informationen stehlen oder Sabotageaktionen durchführen wollen. Eine Entwicklung, die die Sicherheitspolitik weltweit vor neue Herausforderungen stellt. Hinzukommt, dass das alleinige Abwehren von Angriffen dieser Art nicht ausreichen wird. Die relevante Frage ist vielmehr, wie zuverlässig erkannt werden kann, ob sich „ungebetene Gäste" im eigenen System befinden.



	Windows	Linux	Mac	Symbian	Windows Mobile	Android
2010	94,48	3,98	0,008	0,11		
2011	93,34	4,15	0,012	0,004	0,00015	0,013

Quelle: IKARUS

Abbildung 4: Verteilung von Malware nach Betriebssystemen: Mobile Systeme holen künftig stark auf

Mobile Security

Haben sich Angreifer bislang vor allem auf die klassische IT (Server, PCs) fokussiert, so werden mit dem Siegeszug von Smartphones, Tablets und anderen mobilen Geräten diese zunehmend auch für Angriffe interessant. Mobile Geräte sind, was Leistungsumfang und Komplexität betrifft, vollwertige Computer. Sie enthalten zwar alle Sicherheitsmechanismen, deren Wirksamkeit hat sich in der Praxis jedoch als verbesserungswürdig herausgestellt. Insbesondere das Zusammenspiel von persönlichem Umgang und unterstützenden Maßnahmen macht noch Probleme. Mitunter ein Grund, warum Sicherheitsexperten derzeit starke Parallelen zu den Anfangszeiten von PCs sehen, als diese größtenteils noch unsicher betrieben wurden.

Beliebtes Einfallstor bei mobilen Geräten sind vor allem die darauf installierten Apps. Angreifer nutzen die Sorglosigkeit von Anwendern und deren leichtfertigen Umgang mit Programmen aus, um so Zugriff auf fremde Systeme zu erlangen, persönliche Daten zu stehlen oder um sich auf andere Art und Weise zu bereichern. Vor allem der Siegeszug von Googles mobiler Plattform Android, aber auch Apples iOS rücken zunehmend in den Fokus der Angreifer. Das Missbrauchspotenzial von schädlichen Apps, die häufig als vermeintlich nützliche Programme getarnt sind, ist dabei durchwegs groß. Durch das Auslesen von IMEI-Nummern, Adressbüchern oder dem Browserverlauf gelangen Angreifer an höchstpersönliche und eindeutig zuordenbare Daten. Fälle, in denen beispielsweise durch Schadsoftware am Smartphone unbemerkt kostenpflichtige Mehrwert-SMS ins Ausland verschickt wurden, sind bereits bekannt.

Auch sind Smartphones, im Gegensatz zu Computern, meist rund um die Uhr eingeschaltet und ständig mit dem Internet verbunden – das bietet Angreifern hervorragende Bedingungen. Hinzu kommt, dass Smartphones & Co. zunehmend auch als mobile Bezahlsysteme genutzt werden und dieses Anwendungsgebiet bereits heute verstärkt forciert wird. So sind den Herstellern von Sicherheitssoftware derzeit bereits einige Tausend Schädlinge für mobile Geräte bekannt. Auch wenn die Zahl im Vergleich zur Anzahl bekannter PC-Schädlinge noch unbedeutend gering erscheint, so wird ein starker Anstieg schon in unmittelbarer Zukunft prognostiziert.

CERT-GLOSSAR

In a nutshell - die wichtigsten Begriffe kurz erklärt

Austrian Trust Circle

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

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.

DoS-Angriff

Denial of Service (DoS) heißt „Nutzung verhindern“. Bei einem DoS-Angriff wird ein Computer von einer Reihe von anderen Rechnern 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).

Estland- und Georgien-Vorfall

Im Frühjahr 2007 legte eine große Anzahl von DDoS-Angriffen estnische Webseiten von Unternehmen, Banken, Behörden, Polizei und Regierung tagelang lahm. Im Herbst 2008 passierte dasselbe mit georgischen Webseiten. Die Internetauftritte staatlicher Stellen in Georgien waren daraufhin nicht mehr aufrufbar.

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 schädlicher PHP Code eingeschleust. Dieser manipuliert den Inhalt der Webseite abhängig davon, wer sie besucht. Ist es der Webcrawler von Google (GoogleBot), 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 PHP-Code des Einbrechers den Besucher auf einen passenden Webshop. Das Ganze ist also ein Trick, um das Google-Ranking der legitimen Seite auszunutzen, um dubiose Pillenshops als Top-Treffer bei Google zu platzieren. Der Webseitenbetreiber merkt davon oft gar nichts

Lost Credentials

Bei dieser Kategorie von Vorfällen, der direkt übersetzt so viel wie „verlorene Zugangsdaten“ heißt, geht es um publik gewordene Passwörter von Usern. Das kann über Schadsoftware

am PC passiert sein, oder auch durch Einbrüche in Webserver.

mTAN (auch smsTAN)

Mobile TAN (mTAN) oder auch smsTAN wird hauptsächlich im Online-Banking eingesetzt. Um eine Online-Überweisung erfolgreich abzuschließen, erhält der User einen Code via SMS, mit dem er das Bankgeschäft freigeben bzw. abschließen kann.

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 oder Programmen 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 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“.

PHP-Code

PHP eine Skriptsprache mit einer an C und Perl angelehnten Syntax, die hauptsächlich zur Erstellung dynamischer Webseiten oder Webanwendungen verwendet wird.

Social Engineering

Social Engineering meint im Zusammenhang mit dem IT-Security Thema 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 Cyberkriminellen 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-EMails 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 werbliche Inhalte und werden in Massen versendet.

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.

Trojanisches Pferd

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 2012