Kritische Infrastruktur: Staaten hängen von ihrer Infrastruktur ab und diese ist von der IKT-Sicherheit abhängig.

Gefährdete Infrastruktur

Sicherheit in der Informations- und Kommunikationstechnik (IKT) betrifft jeden und ist eine gesamtstaatliche, bis in die umfassende Landesverteidigung reichende Aufgabe. Das wurde in den Referaten und Workshops beim 9. IKT-Sicherheitsseminar in Wien bewusst gemacht.

Im Internet bestehen Lücken, Information fließt ab und Daten werden anderswo zu einem Bild zusammenfügt, ohne dass dies dem Anwender bewusst wird. Über diese und andere Probleme der IKT-Sicherheit referierten Experten beim 9. IKT-Sicherheitsseminar des Abwehramts am 10. und 11. November 2010 in Wien. Gespeichert werden Daten über das Einkaufsverhalten, welche Webseiten man besucht oder nach welchen Büchern man im Internet sucht. „Noch nie hat es Unternehmen gegeben, die so viel über einen Einzelnen gewusst haben; über Suchmaschinen ergibt sich ein Profil“, betonte Rechtsanwalt Dr. Albrecht Haller. Dazu komme, dass rechtliche Ansprüche kaum wirksam geltend gemacht werden könnten, weil sich die für den Inhalt verantwortlichen Rechtsträger in anderen Rechtsbereichen befinden. „Recht haben und Recht bekommen sind gerade hier zwei verschiedene Dinge.“ Es müsse dafür gesorgt werden, dass keine Vollzugsdefizite entstehen.

Spuren im Internet. Kaum bekannt ist, in welchem Ausmaß man im Internet Spuren hinterlässt. DI Markus Zeilinger, hauptberuflicher Lektor für Kommunikationssicherheit an der FH Hagenberg, hat damit einhergehende Probleme dargestellt. Es beginnt damit, dass Computer zunächst Daten über sich selbst, ihre Betriebssysteme und den verwendeten Browser austauschen, um miteinander kommunizieren zu können. Wichtig sind die IP-Adressen, die einen Computer weltweit eindeutig identifizieren. Nähere Informationen zu den IP-Adressen, die zu dem beteiligten Computer führen, können beispielsweise über *www.ripe.net* abgerufen werden. Über *www.maxmind.com* kann dessen Standort mit den entsprechenden Koordinaten ermittelt werden, die es ermöglichen, etwa über *www.maps.google.com* die Position auf der Landkarte zu bestimmen und sich einen optischen Eindruck vom Standort des Servers zu machen.

Nach Umsetzung der EU-RL 2006/24/EG über die Vorratsdatenspeicherung müssen die Verkehrsdaten vom Provider mindestens sechs Monate lang gespeichert werden. Die Verkehrsdaten zeigen, welcher Computer mit welchem anderen wann und wie lange in Verbindung war. Keine Aussage kann allerdings darüber getroffen werden, welche Person den Computer zu diesen Zeiten benützt hat – das muss mit anderen Methoden ermittelt werden.

Fotos: Joujou, Michael-Grabscheit, Tobias-Kunze/Pixelio • Collage: Herbert Saurugg

Einmal im Internet ist gleichzusetzen mit *immer* im Internet. Es hilft nicht, eine Website zu löschen. Wayback-Maschinen wie *www.archive.org* speichern Websites periodisch ab, sodass auch frühere Versionen aufgerufen werden können. Suchmaschinen machen Informationen relativ leicht auffindbar. Veröffentlichungen über eine Person durch Dritte können kaum gesteuert werden.

Eine andere Art von Spuren sind Cookies, kleine Textdateien, die vom Betreiber einer Website auf den Computer des diese Site Aufsuchenden geschickt werden. Sie haben den Zweck, dem Nutzer bei neuerlichen Anfragen ein schnelleres Aufsuchen bestimmter Fundstellen zu ermöglichen, ergeben aber in Summe ein Persönlichkeitsprofil etwa über Einkaufsverhalten oder persönliche Vorlieben. Das ermöglicht gezielte Werbung und ist eine vergleichsweise harmlose Auswertung. Zwar besteht die Möglichkeit, den eigenen Rechner für Cookies zu sperren, doch lassen Betreiber von Internetshops oder von sozialen Netzwerken einen Zugriff auf ihre Sites zumeist nur zu, wenn sie Cookies platzieren können. Sinnvoller ist es, Cookies in kurzen Abständen zu löschen.

Besuchte Websites, Texte und Bilder werden am eigenen Computer im Browser gespeichert. Zweck ist auch hier, besuchte Seiten leichter wieder zu finden. Im Lauf der Zeit ergibt sich eine Auflistung *(Browser History),* die ebenfalls Rückschlüsse auf die Person des Users zulässt. Gelingt es Dritten, sich in den Besitz dieser Auflistung zu setzen *(Browser History Stealing),* lässt sich ein Persönlichkeitsprofil ableiten. Eine Gegenmaßnahme besteht darin, die History zu deaktivieren oder in kurzen Zeitabständen zu löschen.

Spyware. Der Benutzer kann über Spionage-Software ausgespäht werden. Die entsprechenden Programme (Trojaner, Botnetze) nisten sich unbemerkt auf dem Rechner ein. Ausgespäht werden Zugangsdaten, der Nachrichtenverkehr, Unternehmensgeheimnisse. Der Schutz besteht im Einsatz einer jeweils aktuellen Antiviren-Software sowie darin, beim Surfen im Internet Vorsicht walten zu lassen und beispielsweise nicht jeden reißerisch aufgemachten Link bedenkenlos anzuklicken. Wird keine Verschlüsselung eingesetzt, werden Daten im Internet unverschlüsselt

Kommunikationssicherheitsexperte Markus Zeilinger: „Einmal im Internet – immer im Internet."

übertragen. Das gilt auch für E-Mails. Jeder, der auf den Übermittlungsweg Zugriff hat, kann den Inhalt mitlesen. Hinzu kommt, dass der Absender leicht verfälscht werden kann. Vertrauliche Informationen sollten daher entweder nicht oder verschlüsselt über E-Mail versendet werden.

Datenschutz ist im Internet ein wunder Punkt, der auch soziale Netzwerke betrifft. Bereits im Persönlichkeitsprofil gibt man persönliche Daten preis, stellt Bilder von sich und seinem Umfeld ins Netz, nimmt Kontakt mit anderen Benutzern auf und nimmt an Gruppen und Fan-Gemeinschaften teil. Beispielsweise werden auf die Plattform „Facebook" monatlich drei Milliarden Bilder und zehn Millionen Videos hochgeladen. „Facebook" hat weltweit über 500 Millionen Nutzer, in Österreich sind es 2,2 Millionen.

Aus den Eintragungen lässt sich ein Persönlichkeitsprofil ableiten, das unter anderem von Personalabteilungen in Unternehmen ausgewertet wird, aber auch zum Identitätsdiebstahl verwendet werden kann. Die Plattformen bieten die Basis für Cybermobbing und Cyberstalking. Die Nutzungsrechte für Inhalte wie Bilder werden nach den AGBs zumeist an die Plattformen abgetreten, und selbst beim Löschen des Accounts wird dieser nur als gelöscht markiert, nicht aber entfernt – einmal dabei, immer dabei.

Anonymisierung. Wer angesichts der hinterlassenen Spuren sein Auftreten im Internet verschleiern will, kann das über Anonymisierungsdienste bewerkstelligen. Im einfachsten Fall wird ein Server zwischengeschaltet, sodass die Anfrage nicht direkt vom Sender kommt, sondern vom zwischengeschalteten Proxy. Die Sicherheit dieses Verfahrens hängt von der Vertrauenswürdigkeit des Proxy-Betreibers ab. Wenn dieser die IP-Adresse des Absenders in den „Header" der Anfrage einbaut („X-Forwarded-For Header"), ist die Rückverfolgbarkeit von vornherein gegeben.

Eine andere Methode besteht darin, Kaskaden von Rechnern aufzubauen, von denen jeder nur seinen unmittelbaren Vorgänger und Nachfolger kennt, keiner jedoch die Gesamtkette, die aus den dem Anonymisierungsdienst zur Verfügung stehenden Rechnern nach dem Zufallsprinzip gebildet wird. Nur – der letzte in der Kette kann jener sein, der eine verbotene Aktion (Urheberrechtsverletzungen) setzt, ohne dass dies gewollt gewesen wäre. „Überlegen Sie sich, an wen Sie welche Daten weitergeben, informieren Sie sich darüber, wie diese nach den Datenschutzbestimmungen des Betreibers verwendet und an wen sie weitergegeben werden dürfen, welche Rechte an Texten, Bildern und Videos Sie einem Betreiber einräumen", gab Zeilinger zu bedenken.

FOTO: KURT HICKISCH

ABWEHRAMT

IKT-Sicherheitsseminare

Das 9. IKT-Sicherheitsseminar des Abwehramts des Bundesministeriums für Landesverteidigung und Sport (BMLVS) wurde am 10. und 11. November 2010 im Vortragssaal des *TechGate Vienna* abgehalten. Wegen des großen Teilnehmerinteresses wurde wie im Vorjahr das gleiche Programm an zwei Tagen hintereinander angeboten.

Ursprünglich fand das Seminar in einer Kaserne in Wien statt und war nur Teilnehmern des Bundesheeres zugänglich. Mit der Veranstaltung will das BMLVS das Bewusstsein für die IKT-Sicherheit Führungskräften auch außerhalb des Verteidigungsressorts zugänglich machen – der übrigen Verwaltung und der Wirtschaft.

Das nächste IKT-Sicherheitsseminar wird am 9. und 10. November 2011 stattfinden.

Josef Pichlmayr (Ikarus Software Security): „Wir gehen auf Zehenspitzen über ein Minenfeld.“

Rechtsanwalt Albrecht Haller: „Recht haben und Recht bekommen sind zwei verschiedene Dinge.“

Oberst Walter J. Unger (Abwehramt): „Es ist wichtig, redundante Netze getrennt vom Internet aufzubauen.“

Cyber-Kriminalität. „2010 lag die Anzahl bekannter Schadsoftware bei etwa 38 Millionen. 2006 lag dieser Wert noch bei etwa 2,5 Millionen und ist seither exponentiell angestiegen“, berichtete Josef Pichlmayr, geschäftsführender Gesellschafter der österreichischen Softwarefirma *Ikarus Security Software GmbH (www.ikarus.at)*. Werden diese Schadprogramme von der organisierten Cyber-Kriminalität eingesetzt, geht es dabei vor allem um Geld. Nach Schätzungen des US-Finanzministeriums werden durch Cybercrime mehr als 100 Milliarden US-Dollar im Jahr umgesetzt und damit mehr als im illegalen Drogenhandel.

Zu denken geben gezielte Attacken wie etwa die „Operation Aurora“ von Mitte bis Ende 2009, die offenbar zu gezielter Spionage konzipiert war, sowie der im Juni 2010 entdeckte Stuxnet-Trojaner, der darauf angelegt war, industrielle Steuerungssysteme (SCADA-Systeme) zu manipulieren. Dieses allem Anschein nach mit sehr großem Aufwand von Experten ihres Fachs entwickelte Schadprogramm eröffnet neue Dimensionen, was die Gefährlichkeit betrifft.

SCADA-Systeme werden in kritischen Infrastrukturen verwendet, wie Wasserversorgungssystemen, Kraftwerken, Verkehrsleitsystemen, Rundfunk- und Recycling-Systemen, Kontrollsystemen auf Flughäfen. Den Konstrukteuren des Schadprogramms ist es dabei nicht darum gegangen, Maschinen außer Betrieb zu setzen, sondern Mess- und Steuerungsdaten zu verfälschen, was noch gravierendere Auswirkungen hat.

In Stromnetzen ist das „Smart Metering“ im Kommen, das es ermöglicht, elektrische Energie effizient zu nützen, etwa dann, wenn Strom gerade billiger ist. Der Zählerstand kann vom Versorgungsunternehmen über Fernabfrage ausgelesen werden. Über die mit der Inkasso-Funktion verbundene Möglichkeit der Fernabschaltung könnte ein Angreifer den Kunden beispielsweise den Strom abschalten. In einer Simulation waren innerhalb von 24 Stunden 15.000 von 22.000 Haushalte infiziert und damit unter der Kontrolle der Angreifer.

Dem steigenden Grad der Vernetzung, der steigenden Komplexität und Raffiniertheit bei Angriffen stehe laut Pichlmayr ein sinkendes Systemverständnis gegenüber: „Wir gehen auf Zehenspitzen über ein Minenfeld.“

Cybersecurity. „Hoch entwickelte Staaten hängen von ihrer Infrastruktur ab, und diese ist heutzutage von der IKT-Sicherheit abhängig“, sagte der Leiter der Abteilung IKT-Sicherheit des Abwehramts, ObstdG Mag. Walter J. Unger, in seinem Lagebericht zur Cybersecurity. „Man muss sich nur vorstellen, was passieren würde, wenn gleichzeitig die Energie- und Wasserversorgung sowie die Kommunikationsverbindungen, auch jene zu und zwischen Notfallsorganisationen, zusammenbrechen würden.“ Beispiele für umfassende Cyber-Angriffe hat es schon gegeben: 2007 wurde die kritische Infrastruktur Estlands durch Spam- und dDoS-Attacken etwa eine Woche lang gestört.

Eine ähnliche Situation im Jahr 2008 in Georgien war zusätzlich von einem Krieg begleitet. Die militärische, auf zwei Glasfaserleitungen aufgebaute Kommunikation brach zusammen, lediglich eine unabhängig vom Internet betriebene Nachrichtenverbindung blieb intakt.

Der Zeitaufwand für einen solchen Cyberangriff wird auf 18 bis 24 Monate geschätzt, bei Kosten von etwa 10 Millionen Euro. Damit sind diese Angriffe im Verhältnis zu den angerichteten Schäden relativ gering. Die Wahrscheinlichkeit der Entdeckung der Urheberschaft ist gering. Im Verhältnis zur klassischen Kriegsführung sind Vorbereitungen schwer erkennbar, es gibt keine Vorwarnzeit. Die Angriffsziele sind rasch erreichbar, physische Zerstörungen gering und es gibt kaum Verluste an Menschenleben.

Die bisher erfolgten Cyberangriffe auf Staaten zeigen, dass es wichtig ist, redundante Netze getrennt vom Internet aufzubauen, in die die Notfallorganisationen einzubeziehen sind. Zu klären ist, unter welchen Voraussetzungen über den Cyberspace ein Angriff auf die nationale Sicherheit (der nicht notwendigerweise von anderen Staaten ausgehen muss) vorliegt, wer dies feststellt und wer die Abwehr koordiniert.

Kurt Hickisch

Fotos: Kurt Hickisch