Unsichtbare Gegner

Angriffe können auch die Informations- und Kommunikationstechnologie betreffen oder über sie geführt werden. Ein Seminar des Abwehramts des BMLVS hat dies deutlich gemacht.

In den letzten Jahren hat sich gezeigt, dass Konflikte zwischen Staaten auch über den Cyberspace ausgetragen werden und in die Informations- und Kommunikationstechnologie des Gegners eingegriffen oder diese beeinflusst wird“, berichteten Experten des Abwehramts des Bundesheeres beim 8. IKT-Sicherheitsseminar, das am 30. September und 1. Oktober 2009 im *Tech-Gate-Tower* in der *Donau-City* in Wien stattfand. Technisch ähnlich hochstehende Angriffe sind auch von der organisierten Kriminalität und auf dem Gebiet der Wirtschaftsspionage zu erwarten; die Abwehr entwickelt sich zu einer gesamtstaatlichen Aufgabe. Der *Computer Network Exploitation,* dem Aufspüren von Schwachstellen in staatlichen Netzen, wird die *Computer Network Defense (CND)* entgegengesetzt.

Ziel des Seminars war es, für die Thematik zu sensibilisieren. IKT-Sicherheit muss zu einem Thema des Managements werden. Eine besondere Gefahrenquelle sind Handys, mobile Datenspeicher und letztlich der Mensch selbst.

Ein Handy kann etwa 120 Funktionen erfüllen, nur einige davon werden genützt. Wenn es jemandem gelingt, Zugriff auf ein Handy zu haben, ist die Manipulation seiner Software bei einem Smartphone eine Sache weniger Minuten, bei einem iPhone dauert es bis zu etwa 20 Minuten. Dann steht einem Auslesen der SMS nichts mehr im Weg, Kontaktinformationen werden weitertransportiert, die Funktion des Silent Calls kann zu einer vom Benutzer unbemerkten Raumüberwachung umfunktioniert werden. Die Konferenzschaltung kann dazu benützt werden, als Man-in-the-Middle-Gespräche unbemerkt mitzuhören.

Darauf, dass das Handy durch die PIN geschützt ist, kann man sich nicht verlassen: Nur die SIM-Karte ist in diesem Fall gesperrt, nicht jedoch der Zugriff auf weitere Informationen, wie etwa auf abgelegte E-Mails oder Kontaktdaten. Demgemäß gilt, ein Handy niemals unbeaufsichtigt liegen zu lassen, sich mit der Bedienungsanleitung vertraut zu machen und die Sicherheitsfeatures zu nützen.

Markus Klemen: „Mit Social Engineering am schnellsten zu Informationen.“

Josef Pichlmayr: „Gefahr in steigender Komplexität und Intelligenz der IT-Angriffe.“

Mobile Datenspeicher. Abgesehen davon, dass auch Handys mobile Datenspeicher sind, gibt es eine Vielzahl anderer, die auf kleinstem Raum enorme Datenmengen speichern können, wie etwa Notebooks. USB-Sticks haben ein Speichervolumen bis zu 256 GB und Festplatten bis zu 1,5 TB. Rechnet man für ein durchschnittliches Word-Dokument einen Datenumfang von 100 KB, können auf einem gebräuchlichen USB-Stick von 8 GB etwa 80.000 Dokumente untergebracht werden. Die Gefahr des Verlustes eines kleinen Datenspeichers ist groß. Am schwerwiegendsten ist der Schaden, der durch den Verlust der darauf gespeicherten Informationen entsteht. Besondere Vorsicht ist bei der Mitnahme von Laptops auf Reisen ins außereuropäische Ausland geboten. Wegen der Einschau- und Durchsuchungsrechte, die sich manche Staaten bei Einreisenden vorbehalten haben, sollten Daten und mobile Geräte nur im unbedingt nötigen Ausmaß mitgenommen und nicht unbeaufsichtigt gelassen werden, nicht einmal in Hotels oder in Konferenzräumen.

Mobile Datenträger bieten auch jede Menge Platz für Schadprogramme, für die sich, durch die leichte Auswechselbarkeit, Infektionswege eröffnen. Beispielsweise wurde das Ende 2008 aufgetretene Schadprogramm Conficker, von dem weltweit zehn Millionen Rechner betroffen waren und dessen Hintergrund der Aufbau eines Botnetzes für kriminelle Zwecke war, sogar in nach außen gut abgesicherte Netze (Krankenhäuser in Kärnten) über USB-Sticks eingeschleppt.

Das BMLVS hat für den sicheren Umgang mit mobilen Datenspeichern und zu anderen die IKT-Sicherheit betreffenden Themen ein Informationsblatt aufgelegt, das Hinweise und Verhaltensregeln enthält.

„Layer 8“. Die technischen Sicherheitsschichten (Layer), die rund um einen Rechner, vom Kern her beginnend, aufgebaut sind, werden von eins bis sieben nummeriert. Layer 8 ist der Mensch, und eine eigene, 31 Seiten starke Broschüre aus dieser Serie von Informationsmaterial ist allein ihm, dem User, gewidmet – zum Thema „Social Engineering“. Außer Betracht bleibt dabei, was von ihm (von Ausfällen durch höhere Gewalt oder Versagen technischer Komponenten ganz abgesehen) sonst noch an Gefahren durch Unwissenheit, Leichtsinn oder Fahrlässigkeit für die IKT-Sicherheit ausgeht oder an Bedrohungen durch vorsätzliche geführte Angriffe entsteht.

Social Engineering ist eine Gesprächs- und Verhandlungstechnik, mit der sich jemand in das Vertrauen eines anderen einschleicht und ihn dadurch zur Preisgabe von Informationen veranlasst, ohne dass sich der Betreffende dessen bewusst wird. Naivität, Hilfsbereitschaft oder auch Eitelkeit werden ausgenützt. Beliebt ist das Auskundschaften von Passwörtern, indem dringende Arbeiten, Zeitdruck oder ein Auftrag einer höheren Stelle vorgetäuscht wird.

Unternehmen können, ähnlich wie bei Penetrationstests, spezialisierten Anbietern den Auftrag erteilen, die Verletzlichkeit ihres Unternehmens gegen Angriffe zu testen, die über Social Engineering durchgeführt werden.

Über die Planung und Durchführung solcher Tests berichtete Mag. Markus Klemen, Geschäftsführer von *Secure*

FOTOS: KURT HICKISCH

Business Austria (SBA) (www.sba-research.org). Im Vorfeld werden persönliche Daten gesammelt (z. B. über soziale Netzwerke) und dann wird generalstabsmäßig vorgegangen.

In einem Fall bestand der Auftrag darin, zu überprüfen, ob es gelingt, zumindest 15 Minuten lang einen unbeaufsichtigten Aufenthalt im Rechenzentrum zu erhalten. Der die Zutrittskontrolle ausübende Portier wurde von Personen verunsichert, die sich als Prüfer ausgaben und entsprechend energisch auftraten; letzte Zweifel wurden durch eine gleichzeitig einlangende E-Mail der, so hatte es den Anschein, Unternehmensleitung ausgeräumt. In Begleitung des Systemadministrators gelang der Zutritt in das Herz des Rechenzentrums und in das Ausweichrechenzentrum; der Auftrag war erfüllt.

In einem anderen Fall sollte die Resistenz der Mitarbeiter gegenüber Phishing überprüft werden. Als Aufhänger wurde ein angebliches Gewinnspiel anlässlich einer Filialeröffnung gewählt. In der E-Mail wurde nach Usernamen und Passwort gefragt. Von 1.500 Mitarbeitern reagierten rund 700, davon 30 Prozent innerhalb der ersten 10 Minuten. Nicht geprüft wurde, ob die angegebenen Passwörter auch korrekt waren.

Um das Bewusstein der Mitarbeiter im Umgang mit mobilen Datenträgern zu testen, wurden an zehn von ihnen per Post USB-Sticks mit dem Logo einer Firma und einer angeblich auf dem Stick befindlichen Firmenpräsentation versendet. Tatsächlich hat sich ein Programm darauf befunden, das die Aktivierung des Sticks gemeldet hat. Alle zehn Sticks wurden angesteckt, auch an Privatgeräte und ein Teil auch von Nicht-Zielpersonen, möglicherweise aus der Posteinlaufstelle.

Um die Tastatur des Mitarbeiters eines anderen Unternehmens durch eine solche mit einem Keylogger auszutauschen und am Ende des Tages wieder rückzutauschen, wurde für den erforderlichen Zutritt zu den Räumlichkeiten die Zeit des Kantinenzulaufs zur Mittagszeit gewählt. Der Überprüfungsauftrag – der im Ernstfall bedeutet hätte, dass alles, was auf dieser Tastatur geschrieben wurde, unverschlüsselt abgespeichert worden wäre – konnte problemlos abgewickelt werden.

Nachhaltigen Erfolg hatte eine Aktion zur Einhaltung der Clean-Desk-Policy: Nach Dienstschluss wurden auf ungesperrte Rechner, am Tisch liegende Dokumente oder auf Tastaturen, unter die Passwörter geklebt waren, Post-it-Sticker geklebt, in denen auf die Mängel hingewiesen und auf die bestehenden Richtlinien verwiesen wurde. Ein gleicher Test vier Wochen später ergab kaum noch Beanstandungen, doch derartige Aktionen werden wiederholt werden müssen.

Stand der Fachhochschule Hagenberg: Funktionstüchtiges Verschlüsselungsgerät.

„Social Engineering ist immer noch der schnellste Weg, um an geschützte Informationen heranzukommen“, betonte Klemen. „Awareness-Ausbildung ist und bleibt ein aktuelles Thema.“

Über ein in diesem Zusammenhang interessantes soziologisches Experiment informierte Josef Pichlmayr von der *Ikarus Security Software GmbH*. Auf der Website des Unternehmens *(www.ikarus.at)* war vom 7. bis zum 14. Oktober 2008 der Vermerk: „Bitte hier nicht klicken“ zu sehen. Von 31.862 Besuchern der Website konnten 1.074 (3,37 %) der Versuchung nicht widerstehen. Sie erhielten als Reaktion die Antwort: „vielen dank für ihre unterstützung im projekt ‚klicken leute wirklich auf jeden link‘“, verbunden mit einem Bild der Slapstick-Komiker Stan Laurel und Oliver Hardy, die beide, zu Verschwiegenheit und Vorsicht mahnend, beschwörend den Finger auf die Lippen legzen.

Die der IKT-Sicherheit drohende Gefahr sieht Pichlmayr vornehmlich in der steigenden Komplexität und „Intelligenz“ der Angriffe bei relativ sinkendem Systemverständnis.

Weitere Referate befassten sich mit Bedrohungsszenarien in Sprach- und Datennetzen sowie im mobilen Netzwerk und Lösungsmöglichkeiten. Über Datenschutz und Kommunikationsgeheimnis im Lichte des Militärbefugnisgesetzes referierte Rechtsanwalt Dr. Christian Hadeyer, Linz

Malware. Philipp Winter von der Fachhochschule Hagenberg berichtete über Malicious Software (Malware). Auch ohne großes technisches Verständnis wird es immer leichter, Schadprogramme zu generieren. Schwachstellen (Exploits) werden in einschlägigen Foren veröffentlicht, Malware-Kits und der Quellcode von Malware stehen zur Verfügung. Für unerfahrene Autoren sind die Auswirkungen ihrer Programme mitunter nicht absehbar. In Anbetracht der Vielzahl von Schadprogrammen (Ikarus hat Ende Februar/Anfang März 2009 pro Tag an die 30.000 neue Viren gezählt) wird an der FH Hagenberg an einer automatisierten Analyse von Malware gearbeitet.

Akademischer Sicherheitsexperte. Zu den Studiengängen „Sichere Informationssysteme“ wurde von der Fachhochschule Hagenberg in enger Zusammenarbeit mit dem Abwehramt der Lehrgang „Akademischer Sicherheitsexperte für Informations- und Kommunikationstechnologie (ASICT)“ entwickelt *(www.asict.at)*. Unter den im Foyer ausgestellten Kryptogeräten war eine funktionstüchtige Enigma zu sehen, deren Funktion bei der Verschlüsselung von Texten anhand eines Schnittmusterbogens nachvollzogen werden konnte. *Kurt Hickisch*

FOTO: KURT HICKISCH