Angriffe aus dem Cyber-Space

Angriffe auf IKT-Systeme und Gegenmaßnahmen waren Schwerpunkte beim 9. Security Forum am 6. und 7. April 2011 in Hagenberg, Oberösterreich.

Unerlässliche Ausgaben oder Geldvernichtung?“ – diese Frage stellte Mag. Peter Gridling, Direktor des Bundesamtes für Verfassungsschutz und Terrorismusbekämpfung (BVT), beim Security Forum 2011 des Hagenberger Kreises in den Raum, wenn es bei Unternehmen um Ausgaben für IKT-Sicherheit geht. Er bezog sich dabei auf eine Studie des Campus Wien über Wirtschaftsspionage des Innenministeriums, der Wirtschaftskammer und der Industriellenvereinigung.

Für diese Studie wurden Fragebögen an 9.200 Unternehmen versendet. Knapp 300 Unternehmen antworteten, 220 davon ausführlich. Bei 34 Unternehmen, die geantwortet haben, lag der Umsatz unter 200.000 Euro pro Jahr, bei 36 zwischen 200.000 und 500.000, bei 40 zwischen 500.000 und zwei Millionen, bei 43 bis zu 10 Millionen, bei 18 zwischen 10 und 15 Millionen, bei 17 zwischen 50 und 200 Millionen und bei sieben über 500 Millionen.

Die Frage, wie hoch sie das Risiko durch Konkurrenz- und Wirtschaftsspionage einschätzen, wurde nur von 9 Prozent dahingehend beantwortet, darin kein Risiko zu sehen. 50 Prozent stuften das Risiko als eher niedrig ein, 33 Prozent als mittel und 8 Prozent als hoch. 133 Unternehmen waren von Schadensfällen betroffen. Das größte Problem waren abgewanderte Mitarbeiter, die ihre Kenntnisse in anderen Bereichen umgesetzt hatten. 29 Prozent der Unternehmen wurden laut Umfrage durch inländische

Peter Gridling: „Angriffe werden komplexer und auf höherem technischen Niveau durchgeführt.“

Konkurrenz ausgespäht, 20 Prozent durch ausländische Konkurrenz. Als hohes Risiko wurde auch der untreue Geschäftspartner (Lieferant) genannt. Acht Prozent führten den erlittenen Schaden konkret auf Mitarbeiter zurück.

Die Aufwendungen für bauliche Sicherheitsmaßnahmen lagen bei 70 Prozent der Unternehmen unter 10.000 Euro pro Jahr, bei 11 Prozent zwischen 10.000 und 20.000, bei 7 Prozent zwischen 20.000 und 50.000, bei 4 Prozent zwischen 50.000 und 100.000 und in nächstfolgenden Bereichen jeweils nur mehr bei einem Prozent.

Für spezielle IT-Sicherheit gaben 45 Prozent der Unternehmen im Durchschnitt weniger als 10.000 Euro pro Jahr aus, 21 Prozent zwischen 10.000 und 20.0000, 15 Prozent bis zu 50.000 Euro, und in weiteren Stufen jeweils etwa 2,5 Prozent. Drei Prozent wendeten immerhin mehr als eine Million Euro pro Jahr für IT-Sicherheit auf.

„Die Ausgaben werden steigen müssen“, betonte

Walter Unger: „Angriffe auf die IKT können zu einem politisch verwertbaren Ergebnis führen.“

Gridling. Es gebe mehr Angriffe; sie würden komplexer und auf höherem technischen Niveau durchgeführt. Eher unbedeutend sei dabei der Hacker, der sich durch Eindringen in fremde Computersysteme selbst bestätigen will. Gefährlicher seien Saboteure und Datendiebe, deren Treiben sich über Jahre hinziehen kann.

Es geht nicht nur um den finanziellen Schaden, der durch eine Versicherung abgedeckt werden kann. Der Vertrauensverlust und der Schaden an der Reputation kommen dazu. Datenbeschädigung, -diebstahl und -verlust können die Existenz eines Unternehmens bedrohen. Stellt man mögliche Schäden und die Ausgaben zu deren Verhinderung einander gegenüber, ergibt sich eine Unterschätzung des Risikos, sagte Gridling. Kostendruck verhindere eine wirksame Vorbeugung. „Wir brauchen IT-Experten.“

Infrastruktur. Unternehmen und die staatliche Infrastruktur sind durch Angriffe auf die IKT-Sicherheit gefährdet, sagte Oberst Mag. Walter Unger, Leiter der IKT-Sicherheit des Verteidigungsministeriums.

Erst jüngst habe sich herausgestellt, dass der folgenschwere Stromausfall am 14. August 2003 in weiten Teilen der USA und Kanadas statt auf Blitzschlag mit dem zwei Tage zuvor erfolgten Auftreten des „Blaster“-Wurms in Zusammenhang zu bringen ist. Der Stromausfall, der als „Domino-Day“ in die Geschichte eingegangen ist, führte zu einem Zusammenbruch des öffentlichen Verkehrs, der Wasserversorgung und zum Ausfall der Telekommunikationsverbindungen; 50 Millionen Menschen waren betroffen.

„Wenn Staaten von ihrer kritischen Infrastruktur abhängig sind, und diese heute vom Funktionieren der Informations- und Telekommunikation, ergibt sich zwangsläufig, dass Angriffe auf die IKT zu einem politisch verwertbaren Ergebnis führen können“, hob Unger die Bedeutung des Schutzes vor allem der Verfügbarkeit von Daten hervor, der in diesem Zusammenhang gegenüber Vertraulichkeit und Integrität ein noch höherer Stellenwert zukomme. Man müsse sich nur das Szenario vorstellen, dass Stromversorgung, Telekommunikation, Internet, ORF, Innenministerium und Notfallorganisationen gleichzeitig angegriffen und lahmgelegt werden. Derartige Angriffe können über *Botnetze* erfolgen oder durch Unterbrechung der Datenautobahnen. Beispiele dafür sind Angriffe gegen Estland im Jahr 2007 oder gegen Georgien während des Krieges 2008.

Fotos: Kurt Hickisch

Gefährdete Infrastruktur: Angriffe können über Botnetze erfolgen oder durch Unterbrechung der Datenautobahnen.

Welches Ausmaß Schäden durch Schadprogramme annehmen können, hat das Auftreten des Wurms „Conficker“ in Kärnten vor zwei Jahren kurz nach Silvester gezeigt. Zunächst wurden 3.000 Rechner der Landesverwaltung lahmgelegt, dann nochmals 3.000 in drei Spitälern. Um die Schäden wieder zu beheben, haben 40 Techniker in 60 Stunden die Rechner neu aufgesetzt. Der Arbeitsausfall bei den betroffenen Mitarbeitern hat sieben Personenjahren entsprochen.

Das gezielt gegen Maschinen gerichtete Schadprogramm *Stuxnet* hat in letzter Zeit die Verwundbarkeit kritischer Infrastrukturen erneut vor Augen geführt und die Wichtigkeit des Ausbaus redundanter Netze sowie weiterer organisatorischer Maßnahmen.

SCADA. DI (FH) Thomas Brandstetter, MBA, vom *Siemens CERT (www.siemens.com/cert)* referierte über die technischen Aspekte des Angriffs auf kritische Infrastruktur. In der IT-Welt steht Security an der Spitze, in der Industrie Safety, dass also Menschen durch technische Systeme nicht zu Schaden kommen. Daher unterscheiden sich die Schutzkonzepte. Während in der IT-Welt kurzfristige Ausfälle einzelner Geräte verkraftbar sind, muss das im industriellen Bereich unter allen Umständen verhindert werden. In industrielle Anlagen Patches einzuspielen, ist wegen der hohen Anforderungen an Sicherheit im Sinn von Safety ungleich aufwendiger. Dazu kommt, dass keine Zeitverzögerungen auftreten dürfen. Man braucht nur an eine Lichtschranke zu denken, die einen Arbeitsprozess sofort abzuschalten hat, wenn einem Menschen Gefahr droht. Während in der IT-Welt Computerprogramme schon nach wenigen Jahren durch neue ersetzt werden und der Support für ältere Programme eingestellt wird, müssen Anlagen in der Industrie jahrzehntelang in Betrieb sein – mit ihnen auch die zugehörigen elektronischen Systeme, die im Entwicklungsstand dementsprechend zurückbleiben.

Prozesse in der chemischen Industrie, der Flughafenlogistik, der Energiegewinnung und -verteilung, bei der Wasserversorgung, in Massentransportsystemen laufen in der Regel in einem hierarchischen Informationssystem ab, nämlich von einer Kontrollinstanz über weitere Leitstellen bis letztlich zum Endgerät, mit der Aufgabe zu steuern, zu messen und zu regeln. Diese

Foto: Egon Weissheimer

Systeme werden unter *Supervisory Control and Data Acquisition (SCADA)* zusammengefasst. Sie umfassen Automatisierungsprozesse, die in Echtzeit kontrolliert werden. Durch die lange Laufzeit der Anlagen sind die eingesetzten IT-Technologien alt und auf Vertrauen zueinander aufgebaut. Wenn ein Angreifer einmal in dieses Zellkonzept eingedrungen ist, fällt es ihm leicht, das System selbst zu okkupieren.

Als Beispiele für Angriffe auf SCADA-Systeme nannte Brandstetter den Maroochy Water Incident, bei dem im April 2000 in Queensland, Australien, ein entlassener Mitarbeiter eine Kläranlage zum Überlaufen brachte. In Lodz, Polen, entdeckte im Jänner 2008 ein 14-Jähriger, dass die Weichen der Straßenbahn über Infrarot gesteuert wurden – und stellte diese mit einer Fernbedienung wie bei einer Modelleisenbahn um. Vier Züge entgleisten; andere mussten durch Notbremsung gestoppt werden, dabei wurden zwölf Fahrgäste verletzt.

Der Wurm „Slammer" unterbrach 2003 in einem Kernkraftwerk in Ohio die Kommunikationsverbindung zwischen der Leitstelle und der Reaktortechnik. Und eine Künstlergruppe spielte 2007 in Tschechien während der Wiedergabe der von Kameras gelieferten Bilder von Erholungszentren im Frühstücksfernsehen einen Videoclip mit einer Atombombenexplosion im Riesengebirge ein.

Gegen SCADA-Systeme, und auch hier nur gegen bestimmte Maschinen, wurde der im Vorjahr aufgetretene Wurm „Stuxnet" entwickelt. Seine Eigenheit besteht darin, nach außen hin ordnungsgemäße Betriebszustände vorzutäuschen, wogegen sie in Wirklichkeit außer Kontrolle geraten sind. Das Schadprogramm umfasst etwa 650 kB bei 60.000 Zeilen Code. Das hat die Analyse schwer gemacht. Die Einschleusung des Wurms ist möglicherweise über mobile Datenträger (USB-Stick) oder über Notebooks bei Wartungsarbeiten erfolgt.

Fachhochschule Hagenberg in Oberösterreich: Veranstaltungsort des 9. Security Forums.

Bewusstseinsbildung für IT-Sicherheit allein ist zu wenig; die Menschen müssen diese im Sinne einer gelebten Sicherheitskultur verinnerlichen" forderte Prof. Steven Furnell (Universität Plymouth) und erläuterte, warum es Menschen leid ist oder verleidet wird, Sicherheitsbestimmungen zu beachten. Mitarbeitern kann durchaus bewusst sein, dass sie Anhänge zu E-Mails unbekannter Absender nicht öffnen, keine schwachen Passwörter verwenden, Systemwarnungen nicht ignorieren oder Sicherheitskopien ihrer Daten anlegen sollen. Aber es kann beispielsweise zunehmend beschwerlicher werden, sich immer neue und noch kompliziertere Passwörter auszudenken und zu merken. Trotz vorhandenen Sicherheits-Bewusstseins können Sicherheitsbestimmungen ignoriert werden – bis zur Gleichgültigkeit, was sich bis zu Widerstand und offene Ablehnung steigern kann. Da macht es keinen Sinn mehr, für alle immer aufs Neue Sicherheitsbestimmungen zu wiederholen und zu trainieren. Es muss, der jeweiligen Zielgruppe Hilfe und Unterstützung geboten werden, um letztlich innerliche Akzeptanz zu erreichen. „Technik allein kann das Sicherheitsproblem nicht lösen".

Dass Gebäude und Anlagen physisch abgesichert sein müssen, erscheint selbstverständlich. Doch immer wieder zeigen sich hier Schwachstellen. Durch Gedankenlosigkeit oder Nachlässigkeit werden physische Sicherheitseinrichtungen unterlaufen, erläuterte Sicherheitsexperte Thomas Hackner, MSc, *(www.hackner-security.com)*.

Datenschutzrecht.
Rechtsanwalt Marcel Keienborg (*adMERITia GmbH, Langenfeld/Rhld)* hat das deutsche (BDSG) und österreichische (DSG) Datenschutzgesetz miteinander verglichen. Bemerkenswert ist, dass der Datenschutz nicht im deutschen Grundgesetz verankert ist, sondern vom Bundesverfassungsgericht aus dem Grundsatz der Unantastbarkeit der Würde des Menschen (Art. 1 Abs. 1 GG) abgeleitet wurde. Er bezieht sich in Deutschland nur auf natürliche Personen, wenngleich die Gerichte in ihrer Rechtsprechung den Datenschutz zum Teil auch auf juristische Personen ausdehnen. Dagegen kennt das deutsche Recht die Einrichtung des betrieblichen Datenschutzbeauftragten, der in Unternehmen auf die Einhaltung datenschutzrechtlicher Vorgaben hinzuweisen und der Geschäftsleitung zu berichten hat. Er hat ein Verzeichnis automatisierter Datenverarbeitungen zu führen, das jedermann zugänglich gemacht werden muss. Der nach dem deutschen Telemediengesetz (TMG) für das Auftreten im Internet erforderlichen Datenschutzerklärung entsprechen im österreichischen Recht die Verpflichtungen nach dem E-Commerce-Gesetz (ECG). Im Grunde aber sind wesentlich mehr Gemeinsamkeiten als Unterschiede in den datenschutzrechtlichen Bestimmungen zwischen Österreich und Deutschland festzustellen, wobei Keienborg das österreichische DSG als „handwerklich besser" bezeichnete. *Kurt Hickisch*

FOTO: FH HAGENBERG

SECURITY FORUM

Hagenberger Kreis

Der „Hagenberger Kreis *(www.hagenbergerkreis.at)* zur Förderung der digitalen Sicherheit" wurde 2002 von Studierenden des Fachhochschullehrgangs Computer und Mediensicherheit an der FH Hagenberg, Oberösterreich, als Verein gegründet und hält seit 2003 alljährlich im April das „Security Forum" ab. Dem Vortragszyklus am ersten Tag, mit Themen der IKT-Sicherheit, folgen jeweils Workshops am darauffolgenden Tag. Das 9. Security Forum, das am 6. und 7. April 2011 in Hagenberg stattgefunden hat, wurde von etwa 160 Teilnehmern besucht.

www.securityforum.at