Fachhochschule Hagenberg: 10. Security Forum.

Verwehrter Zugang

Einige spektakuläre Fälle des Eindringens in Datenbanken waren für das 10. Security Forum des Hagenberger Kreises Anlass, damit zusammenhängende Fragen und Maßnahmen zu erörtern.

Welche Lehren kann man daraus ziehen, dass Daten von Versicherten, von Rundfunkteilnehmern oder von Polizeibeamten gehackt wurden? Christian Mock von „CoreTEC“ und Robert Waldner von „CERT.at“ referierten beim 10. *Security Forum* des Hagenberger Kreises am 18. April 2012 in der Fachhochschule Hagenberg zu diesem Thema und wiesen auf häufige Fehler hin: „Alles, was wir erzählen, steht in Lehrbüchern, ergibt sich aus Standards oder dem Grundschutzhandbuch des BSI. Nur sieht die Praxis anders aus.“ Es sollte nicht davon ausgegangen werden, dass Security-Verantwortlichkeiten stillschweigend übernommen werden. Die Zuständigkeiten auch für gehostete Services sind festzulegen. Es sollte überlegt werden, wo überall sich Daten des Unternehmens befinden, und es sollten Kontrollrechte über diese Daten gesichert werden, unter Vorschreibung von Mindeststandards und regelmäßiger Überprüfung. In der öffentlichen Wahrnehmung könnten Fehler anderer IT-Dienstleister auf das eigene Unternehmen zurückfallen.

Ein Einfallstor für Angriffe stellen alte, vergessene Projekte oder frühere Marketingaktionen dar. Hochsensible Daten sollten auf anderen Servern laufen als unkritische oder öffentliche Daten. Features von Programmen wären zu überprüfen, ob man sie wirklich braucht, oder ob sie nur „Eye-Candys“ sind. Nicht benutzte Features werden erfahrungsgemäß nicht mehr gepflegt. Regeln für die Datensicherung sollten aufgestellt und Restores geübt werden. Die IT-Security sollte sich als wichtige Organisationseinheit in Unternehmen als Stabsstelle auf Vorstandsebene befinden und nicht wie so oft innerhalb der technischen Abteilung. Durch Beobachtung von News-Diensten, sozialen Netzwerken und einschlägigen Foren lassen sich Angriffsszenarien erkennen. Checklisten sollten für einen tatsächlich eintretenden Fall vorbereitet sein, die auch das Auftreten gegenüber der Öffentlichkeit mit einschließen.

Wirtschaftsspionage. Auf das Problem von „Datenhalden“ wies Friedrich Wimmer in seinem Referat über „Wirtschaftsspionage und Intelligence Gathering“ hin. Auf das Entstehen von Datenhalden haben Unternehmen keinen Einfluss, sie können bei sinnvoller Verknüpfung Aufschluss geben. Durch den internationalen Warenverkehr entstehen Daten, durch den Kapitalverkehr ebenso. Wenn diese Daten miteinander verknüpft werden, lassen sich Geschäftsverbindungen ermitteln, Preise und Konditionen. „Trade Intelligence“ ermöglicht Informationsvorsprünge, die

Foto: Kurt Hickisch

Referenten beim „Security Forum 2012“ in Hagenberg: Christian Mock, Jörg Asma, Robert Waldner, Thomas Unterleitner, Lukas Fellner und Friedrich Wimmer.

im Wettbewerb von Bedeutung sind. Entwicklungen an den Börsen früh zu erkennen, kann das große Geld bringen. Den wahren Wert eines Unternehmens zu kennen, ist bei der Übernahme von Unternehmen von Bedeutung. Da Manager wegen der Gefahr des Abgehörtwerdens wieder mehr auf persönliche Kontakte zurückgreifen, gewinnen Bewegungsprofile an Bedeutung, wie sie sich aus einer Verknüpfung von Flug- und Mobilfunkdaten ergeben.

Friedrich Wimmer und Alexander Tsolkas haben zum Thema „Wirtschaftsspionage und Intelligence Gathering“ ein Sachbuch verfasst, das in Kürze erscheinen wird.

Strafrecht. Dr. Lukas Fellner von der Wolf Theiss Rechtsanwälte GmbH referierte über den strafrechtlichen Bereich bei einem Eindringen in IKT-Systeme. Täter, die es beispielsweise auf Kreditkartendaten abgesehen haben, sind der organisierten Kriminalität zuzurechnen, da ein organisiertes Zusammenwirken erforderlich ist, um aus den gewonnenen Daten zu Geld zu kommen. „Hacktivists“ dringen aus politischen Gründen in Datenbanken ein oder verfälschen Webauftritte. Unzufriedene Mitarbeiter löschen Daten oder wechseln mit diesen zur Konkurrenz. Eine ständige Bedrohung stellt Industriespionage dar.

„Hacking“ ist, als widerrechtlicher Zugriff auf ein Computersystem (118a StGB), strafbar – allerdings mit Einschränkungen. Verschafft sich jemand den Zugang zu einem Computersystem (oder einem Teil davon), ist als verschärfte Form des Verschuldens die Absicht (§ 5 Abs. 2 StGB) des Spionierens, des Verwendens der Daten, des Erzielens eines Gewinns oder der Zufügung einer Schädigung erforderlich. Dem Täter muss es darauf ankommen, diese Ziele zu verfolgen. Erfolgen etwa Penetrationstests mit Zustimmung des Berechtigten, wird der Tatbestand des § 118a StGB nicht erfüllt.

Überdies müssen zur Erfüllung des Tatbestands Sicherheitsvorkehrungen im Computersystem überwunden werden. Wird der physische Zugang zu einem in Betrieb befindlichen Computersystem widerrechtlich erlangt (beispielsweise durch Aufbrechen einer versperrten Türe), ist dies keine Überwindung einer Sicherheitsvorkehrung im Computersystem. Gleiches gilt, wenn die Sicherheitsvorkehrung „Mensch“ überwunden wird, etwa durch Social Engineering.

Wird ein Botnetz durch Versenden von Mails mit infizierten Anhängen aufgebaut (und später vermietet), die unachtsam geöffnet wurden, hat der Urheber keine Sicherheitsvorkehrung im System überwunden. Überdies ist der Täter nur mit Ermächtigung des Verletzten zu verfolgen (§ 118a Abs. 2 StGB). Wenn der Geschädigte nicht will, dass Sicherheitslücken seines Computersystems in einem Gerichtsverfahren offenkundig werden, kann er von der Erteilung der Ermächtigung absehen.

Das Verändern von Daten eines Web-Auftritts (Web-Defacement) erfüllt den Tatbestand des § 126a StGB (Datenbeschädigung), allerdings nur dann, wenn ein Schaden entsteht, also etwa ein finanzieller Aufwand getätigt werden muss, um die Daten wiederherzustellen. Gleiches gilt, wenn Daten gelöscht, sonst unbrauchbar gemacht oder unterdrückt werden. Bedingter Vorsatz reicht aus. Zum Verbrechen wird die Tat, wenn ein 50.000 Euro übersteigender Schaden herbeigeführt oder sie von einem Mitglied einer kriminellen Vereinigung begangen wird (§ 126a Abs. 2).

Denial of Service (DoS) Attacks fallen unter § 126b StGB (Störung der Funktionsfähigkeit eines Computersystems), wenn eine schwere Störung des Systems erfolgt. Eine Freiheitsstrafe bis zu zwei Jahren kann die Folge sein, wenn eine längere Zeit andauernde Störung herbeigeführt wird (§ 126b Abs. 2 StGB), wobei eine Störung durch mehrere Tage als für die Erfüllung dieses Tatbestands ausreichend angesehen wird.

§ 51 Datenschutzgesetz 2000 stellt, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, die Verwendung personenbezogener Daten in Gewinn- oder Schädigungsabsicht unter gerichtliche Strafe. Wenn behauptet wird, man habe mit der Veröffentlichung derartiger Daten nur Sicherheitslücken aufdecken wollen, wird dies zu hinterfragen sein.

Im Sinne des § 123 StGB (Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses) verschafft sich jemand Daten, wenn er diese nicht im Gedächtnis hat. Erfolgt dies mit dem Vorsatz, sie zu verwerten, einem anderen (Konkurrenz) zur Verwertung zu überlassen oder der Öffentlichkeit preiszugeben, ist der Tatbestand erfüllt (Privatanklage; § 123 Abs. 2).

Nach § 11 Abs. 1 des Bundesgesetzes gegen den unlauteren Wettbewerb (UWG) kann gerichtlich bestraft werden, wer als Bediensteter eines Unternehmens Geschäfts- oder Betriebsgeheimnisse, die ihm während des Dienstverhältnisses anvertraut oder sonst zugänglich geworden sind, während der Geltungsdauer des Dienstverhältnisses unbefugt anderen zu Zwecken des Wettbewerbes mitteilt. Die Strafdrohung betrifft den „untreuen Insider“. Es handelt sich um ein Privatanklagedelikt.

Bei der Ausforschung eines Täters im IT-Bereich wäre es „Best Case, wenn der Täter bis zu einer österreichischen IP-Adresse zurückverfolgt

Fotos: Kurt Hickisch

Feuchte Mauern?

MTL

Mauersanierungen GmbH

A-1230 Wien, In der Wiesen 15 B

Telefon + FAX: 01/815 08 68

Email: office@mtl.at Homepage: www.mtl.at

SCHMID ESTRICHE

Alois Lutter Strasse 8
2514 Traiskirchen
www.estrich-schmid.at

Tel.: 02252 / 50 84 60
Fax: 02252 / 50 86 35
office@estrich-schmid.at

UHR Werk

Uhr-Werk Wien 8
Josefstädet Straße 71
1080 Wien
Tel.: 01/409 25 31
Fax: 01/409 25 31

Uhr-Werk Wien 1
Krugerstraße 10
1010 Wien
Tel.: 01/513 55 66
Fax: 01/ 512 56 34

Email: office@uhr-werk.at Internet: www.uhr-werk.at

www.bm-nasko.at

Büro für Bauwesen
Beratung - Planung - Projektmanagement

Hoch- und Tiefbauplanungen
Energieausweisberechnung

klima:aktiv
kompetenzpartner

BAUMEISTER
ING. MICHAEL NASKO
3100 St. Pölten, Handel Mazzetti Str.16
Tel.: +43(0)676 / 40 19 155, E-Mail: **office@bm-nasko.at**
www.bm-nasko.at

STINGL

Garten- und Grünflächenbau
Gartengestaltung

Christian STINGL

1160 Wien, Seitenberggasse 7
Tel.: 0676 / 408 93 50
Mail: office@gartengestaltung-stingl.at
Site: ww.gartengestaltung-stingl.at

MALER
Gneist
Wiener Neustadt

Innenbereich:
Tapetenarbeietn
Raumgestaltung
Farbgestaltung
Spachteltechniken
Wischtechnik
Stuckarbeiten
Möbellackierarbeiten

Außenbereich:
Fassadenrenovierung
Fassadenanstriche inklusive Putzschädenbehandlung
Holzerneuerungsanstriche deckend und Lasuranstriche
Eisenanstriche
Blechanstriche (Dächer/Ablaufrohre/Dachrinnen)

2700 Wr. Neustadt, Zehnergasse 7a
Tel.: 02622 / 241 40, Fax: DW 20
Email: maler-gneist@chello.at

Für unsere Zeitschriften und Broschüren suchen wir seriöse **Anzeigenkontakter** auf Werkvertragsbasis – in allen Bundesländern.

Rufen Sie uns an:
Herr Johann Köchelhuber
Telefon 0664/462 71 34

ARCHITEKTURBÜRO THAJER
ARCHITEKT DI MICHAEL THAJER
STAATLICH BEFUGTER UND BEEIDETER ZIVILTECHNIKER
FORMANEKGASSE 6 | 1190 WIEN | Tel. 01 368 21 08
www.thajer.com | office@thajer.com | Fax. 01 368 21 08 4

THAJER

werden kann“, sagte Feiler. Nach § 18 Abs. 4 E-Commerce-Gesetz (ECG) haben Hosting-Provider Name und Adresse eines Nutzers ihres Dienstes auf Verlangen dritten Personen zu übermitteln, sofern diese ein überwiegendes rechtliches Interesse an der Feststellung der Identität des Nutzers glaubhaft machen. Zu Hosting-Providern zählen Access-Provider (OGH vom 16. März 2004, 4 Ob 7/04i); allerdings nicht bei dynamischen IP-Adressen (OGH vom 14. Juli 2009, 4 Ob 41/09x).

Seit Einführung der Vorratsdatenspeicherung am 1. April 2012 besteht diese Auskunftspflicht Privaten gegenüber nicht mehr (§ 99 Abs. 5 Z 2 TKG idF Z 20 BGBl I 2011/27), sondern nur mehr gegenüber dem Staatsanwalt (§ 76a StPO idF Art 1 BGBl I 2011/33), gegenüber Sicherheitsbehörden nach Maßgabe des § 53 SPG idF Art 2 BGBl I 2011/33. Bei Offizialdelikten kann nach Erstattung einer Anzeige bzw. überdies erteilter Ermächtigung im Fall des § 118a StGB im Wege der Akteneinsicht die Identität des Täters in Erfahrung gebracht und gegen diesen zivilrechtlich vorgegangen werden. Diese Vorgangsweise versagt bei Privatanklagedelikten (zu denen auch jene des § 91 UrhG gehören), da bei strafbaren Handlungen, deren Begehung nur auf Verlangen des Opfers zu verfolgen ist, ein Ermittlungsverfahren nicht stattfindet (§ 71 Abs. 1 letzter Halbsatz StPO).

Notifikationspflicht. Mittelbar bringt die Verpflichtung, betroffene Personen von der Kompromittierung ihrer personenbezogenen Daten (Data Breach) zu informieren, eine Erhöhung der Daten-Sicherheit mit sich. Unternehmen müssen damit eingestehen, nicht genug für die Sicherheit der bei ihnen bestehenden Daten getan zu haben – die tatsächlich vorhandene IT-Sicherheit wird überschaubarer. Die bestehende „Informations-Asymmetrie“ (Feiler) wird verringert. Sie besteht darin, dass Unternehmen alles über die bei ihnen bestehende Datensicherheit wissen, der Kunde aber nichts. Vornehmlich hat diese aus dem kalifornischen Recht stammende und durch § 24 Abs. 2a DSG 2000 sowie § 95a TKG 2003 in das österreichische Recht eingeführte Einrichtung den Sinn, den Betroffenen reaktive Maßnahmen zu Verlust der Vertraulichkeit, Integrität oder Verfügbarkeit ihrer personenbezogenen Daten zu ermöglichen.

Der Einsatz mobiler Computer birgt Sicherheitsgefahren. Schutz bietet eine aktuelle Sicherheitssoftware.

Foto: Kaperski

Nach dem durch die DSG-Novelle 2010, BGBl I 2009/133, in das DSG eingefügten und seit 1. Jänner 2010 in Kraft stehenden § 24 Abs. 2a DSG besteht die Notifikationspflicht, wenn einem Auftraggeber bekannt wird, dass Daten aus einer seiner Datenanwendungen systematisch und schwerwiegend unrechtmäßig verwendet wurden und den Betroffenen Schaden droht. Diese sind unverzüglich in geeigneter Form zu informieren, außer, die Notifikation würde in Anbetracht eines nur geringfügigen Schadens einen unverhältnismäßigen Aufwand erfordern. Diese Informationspflicht zu verletzen, stellt nach § 52 Abs. 2 Z 4 DSG eine Verwaltungsübertretung dar, die mit Geldstrafe bis zu 10.000 Euro zu ahnden ist.

Nach § 95a TKG, idF BGBl I 2011/102, der am 22. November 2011 in Kraft getreten ist, hat der Betreiber öffentlicher Kommunikationsdienste unverzüglich die Datenschutzkommission von der Verletzung personenbezogener Daten, die im Zusammenhang mit der Diensteerbringung verarbeitet wurden, zu verständigen. Während diese Verständigung zu erfolgen hat, sind die Betroffenen unverzüglich zu informieren, wenn anzunehmen ist, dass durch die Verletzung Personen in ihrer Privatsphäre oder die personenbezogenen Daten selbst beeinträchtigt werden. Von einer Benachrichtigung der Betroffenen kann abgesehen werden, wenn der Datenschutzkommission nachgewiesen wird, dass technische Schutzmaßnahmen getroffen wurden. Die Benachrichtigung nicht durchzuführen wird als Verwaltungsübertretung mit Geldstrafe bis zu 37.000 Euro bestraft (§ 109 Abs. 3 Z 15a TKG).

In beiden Fällen der Notifikationspflicht besteht die Haftung für Vermögensschäden nach dem Zivilrecht. Im Verhältnis von Vertragsparteien zueinander kann die Informationspflicht im Fall des Data Breach präziser geregelt werden. Ohne eine Vereinbarung hat ein Vertragspartner dem anderen die Sicherheitsverletzung zur Kenntnis zu bringen – aus der allgemeinen Verpflichtung, ihn vor Schaden zu schützen (nebenvertragliche Schutzpflicht).

Feiler empfiehlt, sich vor einem Fall des Data Breach einen Ablaufplan über die zu ergreifenden rechtlichen Maßnahmen zurecht zu legen (Emergency Response Plan).

„Bring your own device“: Mitarbeiter arbeiten in einem Unternehmen mit ihren eigenen Geräten und Programmen. Dieses Geschäftsmodell sei nur auf den ersten Blick kostengünstig, sagte Jörg Asma von der *KPMG*. Es ergeben sich Probleme mit der Anpassung an die anderen im Unternehmen verwendeten Geräte und Programme und damit mit der Verfügbarkeit der Daten sowie Lizenzprobleme, die zu einer Haftung des Vorstands führen können. Zudem besteht die Gefahr, dass Sicherheitseinrichtungen umgangen werden, da über die verwendeten Geräte keine Kontrollmöglichkeit besteht.

Kurt Hickisch

www.securityforum.at
www.hagenbergerkreis.at