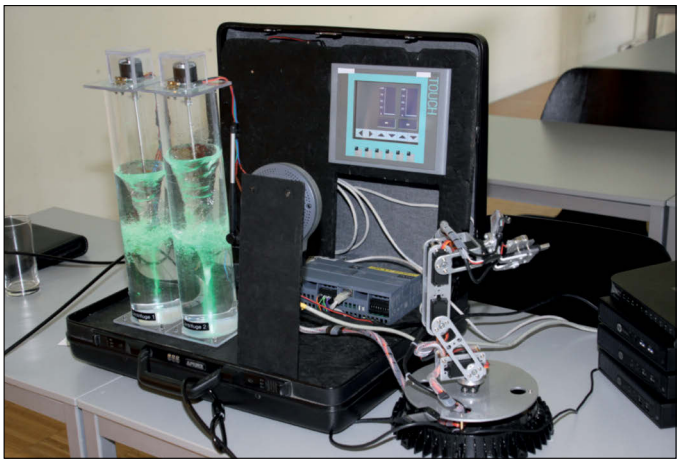
Hacking: Professionelle Angriffe zielen auf Berechtigungen ab, um damit tiefer in die Netzwerke einzudringen.



***Stuxnet*-Nachbau: Der Computerwurm war auf ein Überwachungs- und Steuerungssystem zugeschnitten.**

Neue Gefahren aus dem Web

Wie Angriffe aus dem Internet erfolgen und wie sie abgewehrt werden können, waren die Schwerpunkte des Security-Forums an der Fachhochschule Hagenberg in Oberösterreich.

Ein Schadprogramm auf den eigenen IT-Anlagen zu entdecken, hat 2011 durchschnittlich 416 Tage gedauert, 2014 waren es 205 Tage, und 2015 146 Tage“, sagte Martin Krumböck, *Mendiant Company (www.mandiant.com)* beim Security-Forum am 20. und 21. April 2016 an der Fachhochschule Hagenberg in Oberösterreich. Das Ziel müsse sein, jeden derartigen Vorfall in weniger als zehn Minuten zu erkennen und darauf zu reagieren.

Professionelle Angriffe zielen auf die Berechtigungen ab, um damit immer tiefer in die Netzwerke einzudringen, bis man Administratorrechte erlangt. Deutlich macht sich bei den Angreifern ein „Nine-to-Five-Job“ bemerkbar – die hinter den Angriffen stehenden kriminellen Organisationen sind Unternehmen mit fixen Bürozeiten. Aus der Uhrzeit, zu der Angriffe gehäuft erfolgen, lässt sich abschätzen, aus welcher Weltregion sie kommen.

Bei einer zielgerichteten Attacke gelangt der Täter zunächst über Phishing, Social Engineering, USB-Sticks mit Malware, in das Netzwerk eines Unternehmens, baut sich Hintertüren ein, verschafft sich einen Überblick und verstärkt seine Position. Durch Erlangen immer höherer Rechte gelingt es ihm, die gewünschten Informationen abzuziehen und seine Tätigkeit auf andere Server auszuweiten. Zur Abwehr genügt es nicht, bloß Compliance-Regeln einzuhalten. Vielmehr sollte durch ein Security-Operation-Center ein zentrales Monitoring erfolgen, das selbst kleine Unregelmäßigkeiten erkennt. Neben dem Aufdecken eines Angriffs und dessen Abwehr ist auch zu hinterfragen, was das eigentliche Ziel des Angreifers war.

Intelligence. Angreifer holen sich auf der Suche nach dem schwächsten Glied Informationen über das Angriffsobjekt, schilderte Lukas Reiter, *Hackner Security Intelligence (www.hackner-security.com)*. Die Informationen können öffentlich sein, wie Zeitungsberichte, Suchmaschinen im Internet wie *Google* und öffentliche Dateien (Firmenbuch; *www.firmenmonitor.at)*. Es hilft weiter, Namen, Adressen, Telefon-Nummern, Geburtsdaten von Vorständen, Geschäftsführern, zu kennen. Die *Open Source Intelligence (OSINT)* ist im privaten Umfeld die verbreitetste Methode, sich über jemanden zu informieren. Man kann sich passiv nur auf diese öffentlichen Daten beschränken, sodass beim Zielobjekt die Nachforschungen nicht bemerkt werden, allerdings mit dem Nachteil, dass die Daten nicht unbedingt aktuell sind. Bei semi-passiver Vorgangsweise wird mit dem auszuspähenden System bereits in Verbindung getreten. Bei aktiver *OSINT* werden öffentlich zugängliche Daten heruntergeladen.

Vortragende beim Security-Forum: Georg Beham, Friedrich Wimmer, Peter Panholzer, Lukas Reiter.

Als *Imaginery Intelligence (IMINT)* wird das Sammeln von Daten durch Abfotografieren von Gebieten bezeichnet. *Human Intelligence (HUMINT)* ist die Sammlung von Daten über menschliche Datenquellen durch Observation, Social Engineering. *Signals Intelligence (SIGINT)* als Sammlung von Daten durch Abhören von Signalen oder Kommunikation sowie *Measurements and Signatures Intelligence (MASINT;* Erfassung und Auswertung von Abstrahlungen und Emissionen) sind bereits dem militärischen Bereich zuzuordnen.

Die Arten der Informationsbeschaffung (Intelligence Gathering) reichen

FOTOS: ARTUR MARCINIEC/FOTOLIA, KURT HICKISCH (5)

Cyber-Kriminalität gegen Industrieunternehmen: Angriffsziele sind Entwicklung, Messdaten, Maschineneinstellungen.

Foto: Sven Petersen/Fotolia

von der automatisierten Beschaffung (Level 1) über eine zusätzliche manuelle Analyse bis zu einer vollumfassenden Analyse (Level 3). Diese hat zum Ziel, möglichst viele Informationen zu sammeln und schließt Phishing oder Social Engineering ein.

Dem Bestreben eines Angreifers, möglichst viele Informationen zu erhalten, kann man als Privatperson entgegensetzen, möglichst wenig über sich preiszugeben. Dazu gehört zu überprüfen, welche Datenquellen man mit welchen Informationen versorgt und auch, sich selbst zu checken, was im Internet bereits an Informationen über einen selbst besteht. In sozialen Netzwerken sollte auf restriktive Privacy-/Sicherheits-Einstellungen geachtet und nicht mehr verwendete Accounts sollten gelöscht werden.

Hat sich ein Angreifer so tief in ein System eingegraben, dass ihm alles offensteht, er im Besitz des „Golden Tickets" ist, vergleichbar einem Schlüssel, mit dem in alle Wohnungen einer Stadt eingedrungen werden kann, helfen bloß chirurgische Maßnahmen nicht mehr. Der Angreifer würde einfach ausweichen, sagte Friedrich Wimmer, Leiter IT-Forensik von *Corporate Trust (www.corporate-trust.de)*. Kurzfristige Gegenmaßnahmen bestehen darin, den Angreifer zu behindern und laufende Angriffe schwerer und teurer zu machen. Mittelfristig aber wird, um die Kontrolle über die Systeme wieder zu erlangen, eine Abschaltung aller nicht zwingend benötigten Netzwerkverbindungen erforderlich sein. Dazu gehört es, infizierte Server und Clients neu aufzusetzen, die Passwörter aller Benutzer mit Admin-Rechten und von allen technischen Accounts zu ändern sowie keine Default-Passwörter mehr zu verwenden. Für die „Kronjuwelen" ist in weiterer Folge ein eigener Safe einzurichten. Zugriffe auf diesen unterliegen einem strikten Monitoring.

Alfred Czech, Geschäftsführer von *Corporate Trust* in Österreich, betonte die Eigenverantwortung von Unternehmen hinsichtlich der Vorbereitung auf den Ernstfall und der zeitnahen Reaktion auf Sicherheitsvorfälle. Auffälligkeiten (Einbruchsspuren an der Tür zum Serverraum; Einbrüche, ohne dass etwas weggekommen ist; regelmäßige Überstunden eines Mitarbeiters spätabends) sollten einem Single Point of Contact (SPOC) zugeleitet werden, von dem aus bei Verdichtung der Verdachtslage Maßnahmen zu initiieren wären.

Cybercrime. Die bei einem Bankraub zu erbeutenden Summen sind wesentlich geringer als bei einem IT-Angriff auf Geldinstitute. Zudem ist das Entdeckungsrisiko bei Zweiterem nicht so groß, sagte Georg Beham, *KPMG Advisory GmbH* Österreich. Cyber-Kriminalität ist lukrativer als der Drogenhandel. Beispielsweise konnten mit dem 2014 entdeckten Schadprogramm *Carbanak* Kriminelle etwa eine Milliarde Dollar von Banken vor allem in Russland, der Ukraine, der EU und in China erbeuten. Aufgedeckt wurden die Angriffe, als ein Bankomat in der Nacht fortwährend Geldscheine ausgab.

Millionen wurden mit CEO-Betrug (Fake President Fraud; s. *„Öffentliche Sicherheit" Nr. 5-6/16, S. 6 – 8*) erbeutet, hinter dem kriminelle Organisationen stehen. Die Täter verschaffen sich Informationen über ein Unternehmen, dessen Strukturen und Hierarchien und über die anweisungsberechtigten Personen. Diese werden unter dem Vorwand besonderer Dringlichkeit und einzuhaltender höchster Geheimhaltung, verbunden mit autoritärem Auftreten, dazu gebracht, bedeutende Beträge auf Konten vornehmlich in Osteuropa oder Asien zu überweisen. Das Geld wird nach Eingang umgehend behoben. Ein Rückruf ist vielfach nicht mehr möglich.

Im Fokus der organisierten Cyber-Kriminalität liegen Finanzinstitute, Industrieunternehmen wie die Autoindustrie und Energieversorger sowie mittelständische Unternehmen. Angriffsziele sind Forschung und Entwicklung, Messdaten, Maschineneinstellungen. Insider werden entweder angeworben, können

aber auch unabsichtlich durch bloße Gedankenlosigkeit (Öffnen des Anhangs einer dubiosen E-Mail; Anstecken eines infizierten Sticks u. a.) zum Mittäter werden.

Tyler Moffitt und Kelvin Murray von der Firma *Webroot (www.webroot.com)* gaben einen Überblick über Schadsoftware, insbesondere solche, die den Inhalt einer Festplatte verschlüsselt. Erst nach Bezahlung eines „Lösegelds" (Ransom) in Bitcoins wird der Code für die Entschlüsselung übermittelt und die Festplatte wieder freigegeben. Zukünftige Angriffe würden sich gegen die Steuerung von (selbstfahrenden) Autos richten. Ein Beispiel dafür war der „Chrysler Car-Hack", der 2015 zum Rückruf von 1,4 Millionen SUVs in den USA geführt hatte.

Einen Einblick in „Russian Cybercrime" gab eine Vertreterin des französischen Start-up-Unternehmens *CybelAngel (www.cybelangel.com)*. Das auf die Aufdeckung von Daten-Lecks und Produktfälschung im Internet spezialisierte Unternehmen ermittelte fünf größere russische Foren, die den Markt mit Hacking-Tools, gestohlenen Kreditkartendaten und Personaldokumenten sowie Malware-Service beliefern. Das „neue Gold" sind persönliche Daten aller Art, die aus dem Internet abgezogen werden. Verbunden mit Daten von Kreditkarten und Bankkonten bilden sie die Basis für hochentwickelte Betrugsszenarien.

Industrielle Systeme. „Vor *Stuxnet* 2010 waren die IT-Anlagen in der Industrie vor Angriffen relativ sicher", sagte Peter Panholzer, *Limes Security (www.limessecurity.com)*. Es wurden proprietäre Software-Systeme verwendet, die physisch nicht mit anderen verbunden waren. Es gab nur wenige bekannt gewordene Sicherheitsvorfälle, etwa den *Maroochy Water-Breach* in Queensland, Australien. Aus Verärgerung, keine Anstellung beim Abwasser-Entsorgungsunternehmen erhalten zu haben, hackte sich ein Mann im März 2000 in das Maschinensystem der Anlage ein und flutete die Stadt mit Abwasser. 2008 brachte in Lodz ein 14-Jähriger einen Straßenbahnzug zum Entgleisen. Er hatte herausgefunden, dass die Weichensteuerung der Straßenbahn über Infrarot erfolgte, und dies mit einer adaptierten TV-Fernbedienung nachgestellt. Der Computerwurm *Stuxnet* war ein professionell entwickeltes, 2010 entdecktes Schadprogramm, das auf ein Überwachungs- und Steuerungssystem *(Supervisory Control and Data Acquisition – SCADA)* zugeschnitten war, speziell auf Zentrifugen, die zur Urananreicherung benützt werden können. Die Umdrehungszahl der Motoren wurde durch das Programm verändert. Dennoch wurden für die Kontrolleinrichtungen die Soll-Werte angezeigt.

Fachhochschule Hagenberg, Veranstaltungsort des Security-Forums.

Stuxnet hat gezeigt, dass durch die Manipulation von Softwarekomponenten physischer Schaden angerichtet und die Schnittstelle zwischen verschiedenen Systemen („Air Gap") übersprungen werden kann. Panholzer führte ein Modell einer Zentrifugen-Steuerung vor, an dem man sich über Internet als Hacker versuchen konnte. Die Schnittstelle wurde durch einen Roboter symbolisiert, der einen USB-Stick an den Rechner der Steuerungseinheit anzustecken hatte – was wahrscheinlich auch der Übertragungsweg von *Stuxnet* war.

Die Sicherheit von IT-Komponenten in der Industrie wurde in der Folge durch die Übernahme von bewährten Sicherheitsmethoden aus dem Office-Bereich (Virtual Private Networking, Intrusion Detection Systeme, Virenscanner, Risikoanalysen, Pentests) verbessert, liegt aber, als nicht zum eigentlichen Kerngeschäft der Industrie gehörend, immer noch hinter der herkömmlichen IT-Security zurück. Probleme sind auch veraltete Softwarebestände und ungepatchte Systeme, die Heterogenität von Anlagen und der unbekannte Sicherheitsstatus von über Jahrzehnten gewachsenen Anlagen.

Eine der im Internet am häufigsten verwendeten Suchmaschinen für Industriekomponenten ist *Shodan (www.shodan.io)*. Der Entwickler dieses Systems, John Matherly, bot einen Überblick, was derzeit im Internet der Dinge öffentlich einsehbar ist, Kraftwerke, Tankstellen, Pumpanlagen, Krematorien, Webcams, Verkehrsleiteinrichtungen, Drucker. Die Anzahl dieser Einrichtungen und Geräte wächst von Tag zu Tag, wogegen die Sicherheits- und Kontrollsysteme im Wesentlichen auf dem gleichen Stand bleiben.

Einen Überblick über die am 24. Mai 2016 in Kraft getretene Datenschutz-Grundverordnung der EU (DSGVO) bot Rechtsanwalt Dr. Lukas Feiler von der Wirtschaftskanzlei *Baker & McKenzie*. Er ging insbesondere auf die nach der DSGVO erforderlichen Datensicherheitsmaßnahmen ein; die Meldepflicht bei Sicherheitsverletzungen (Data Breach Notification); die hohen Verwaltungsstrafen und die schadenersatzrechtliche Verantwortlichkeit gegenüber Betroffenen.

Die – unmittelbar anwendbare – Verordnung gilt ab dem 25. Mai 2018. In Anbetracht der Sanktionen (in einigen Fällen sind Geldbußen bis zu 20 Millionen Euro oder bis zu vier Prozent des gesamten weltweiten Jahresumsatzes eines Unternehmens vorgesehen) betonte Feiler die Wichtigkeit, die entsprechenden Vorkehrungen und Maßnahmen zeitgerecht in die Wege zu leiten und noch vor dem Geltungstag abzuschließen.

Kurt Hickisch

FOTO: KURT HICKISCH

HAGENBERGER KREIS

Security-Forum

Der 2002 gegründete Verein „Hagenberger Kreis zur Förderung der digitalen Sicherheit" mit dem Sitz in Hagenberg/Oberösterreich setzt sich zusammen aus Studierenden der Bachelor- und Master-Studiengänge „Sichere Informationssysteme" (SIB, SIM) an der Fachhochschule Hagenberg. Ziel des Vereins ist es, das Sicherheitsbewusstsein in Bezug auf die Informations- und Telekommunikationstechnik sowohl bei Privatpersonen als auch in Unternehmen zu heben.

Der Verein veranstaltet seit 2003 alljährlich an zwei Tagen im April in den Hörsälen der Fachhochschule Hagenberg das Security-Forum, eine IKT-Sicherheitskonferenz. In zwei parallel ablaufendenden Panels halten Fachleute sowohl technische als auch management-orientierte Vorträge.

www.hagenbergerkreis.at
www.securityforum.at