Zunehmend verletzlich

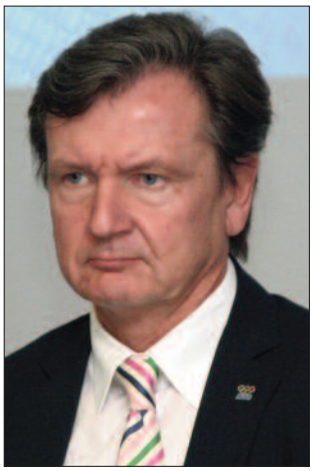
Bei der IT-Sicherheitsmesse „it-sa 2015“ in Nürnberg wurden Lösungen vorgestellt, wie der immer größer werdenden Verletzlichkeit der digitalen Welt begegnet werden kann.

Schon jetzt gibt es mehr als 250 Millionen Varianten von Schadprogrammen, täglich kommen Tausende neue dazu“, sagte Klaus Vitt, seit 1. Oktober 2015 Staatssekretär für Informationstechnik und Verwaltungsmodernisierung im deutschen Bundesministerium des Innern und Beauftragter der Bundesregierung für Informationstechnik, bei der Eröffnung der IT-Sicherheitsmesse *it-sa* in Nürnberg am 6. Oktober 2015.

Identitätsdiebstahl sei zu einem alltäglichen Phänomen geworden und erleichtere Angriffe. Obwohl das Vertrauen in das Internet nachgelassen habe, würden konkrete Schutzmaßnahmen nur geringfügig häufiger eingesetzt. Durch Smartphones und Tablets verbreitere sich die Basis der Verwundbarkeiten; diese Geräte seien eine „Goldgrube für illegale Machenschaften“. Digitale Verwundbarkeit treffe auf digitale Sorglosigkeit, wobei die Verwundbarkeiten – Stichwort selbst fahrende Autos – in den nächsten Jahren weiter steigen würden. Im Internet habe der Staat Schutz- und Gewährleistungsfunktion. IT-Sicherheit sei Teil der Daseinsvorsorge, und zudem ein Standortfaktor.

Das am 25. Juli 2015 in Deutschland in Kraft getretene IT-Sicherheitsgesetz legt den Schwerpunkt auf die Sicherheit kritischer Infrastruktur. Die entsprechenden Unternehmen werden verpflichtet, Mindest-Standards bei der IT-Sicherheit einzuhalten. Relevante Sicherheitsvorfälle sind von den Unternehmen dem *Bundesamt für Sicherheit in der Informationstechnik (BSI)* zu melden. Diese Behörde wertet die Meldungen aus und gibt die Erkenntnisse an alle anderen Betreiber kritischer Infrastruktur weiter, damit diese Gegenmaßnahmen ergreifen können, ehe sie selbst zum Opfer werden. Die Kompetenzen des *BSI* werden im Bereich der Bundesverwaltung gestärkt und erweitert.

Klaus Vitt: „Smartphones und Tablets sind eine Goldgrube für illegale Machenschaften.“



Winfried Holz: „500 von 1.000 Unternehmen wurden in den letzten zwei Jahren Opfer von Datendiebstahl.“

Die Umsetzung des Gesetzes erfolgt durch Rechtsverordnungen, an denen derzeit gearbeitet wird. Die Verordnungen für die Bereiche Energie, Wasser, Ernährung und IKT sollen im Frühjahr 2016 fertiggestellt sein, jene für die restlichen Bereiche Transport und Verkehr, Gesundheit sowie Finanz und Rechnungswesen bis Ende 2016. Unter Einrechnung einer Umstellungsfrist von etwa zwei Jahren wird die Umsetzung des IT-Sicherheitsgesetzes 2018 abgeschlossen sein.

BSI-Präsident Michael Hange wies darauf hin, dass vom IT-Sicherheitsgesetz zwischen 1.400 und 2.000 Unternehmen in Deutschland betroffen seien – das sei bei drei Millionen mittelständischer Unternehmen ein geringer Prozentsatz. „Angriffe lassen sich nicht verhindern“, sagte Hange; demnach sei Incident Handling erforderlich. Die Oberfläche für die Angriffe nehme zu und auch deren Qualität. Beunruhigend sei die starke Zunahme zielgerichteter, mit großem Aufwand durchgeführter Angriffe *(Advanced Persistent Threats, APTs)*.

Winfried Holz, Mitglied des *Bitkom*-Präsidiums, berichtete über eine Studie des *Bitkom (www.bitkom.org)* zum Thema Wirtschaftsschutz im digitalen Zeitalter. 51 Prozent der befragten 1.000 Unternehmen wurden in den vergangenen zwei Jahren Opfer von Datendiebstahl, digitaler Wirtschaftsspionage oder Sabotage. Der Mittelstand war mit 61 Prozent stärker betroffen; zum einen wegen seiner innovativen Produkte und zum anderen wegen der Integration in die Lieferketten der Großkonzerne. Ein Eindringen in die schwächer abgesicherten digitalen Systeme eines Zulieferers könnte zu Angriffen auf die Großkonzerne genützt werden. Die Studie beziffert den durch die angeführten Delikte bei deutschen Unternehmen angerichteten Schaden mit rund 51 Milliarden Euro pro Jahr.

Ein Viertel dieser Summe geht auf Umsatzeinbußen durch Plagiate zurück, gefolgt von Patentrechtsverletzungen und Umsatzeinbußen durch den Verlust von Wettbewerbsvorteilen. Täter sind in 52 Prozent der Fälle aktuelle oder ehemalige Mitarbeiter und in 39 Prozent befinden sie sich im unternehmerischen Umfeld (Wettbewerber, Lieferanten, Dienstleister). 17 Prozent der befragten Unternehmen nannten Hobby-Hacker als Täter; 11 Prozent gaben an, Opfer organisierter Kriminalität geworden zu sein.

Das IT-Sicherheitsgesetz werde laut Holz eine große Nachfrage nach IT-Sicherheitsexperten nach sich ziehen, die es derzeit auf dem Arbeitsmarkt nicht gebe.

APT-Angriffe. Stefan Strobel, Geschäftsführer des IT-Sicherheitsunternehmens *cirosec GmbH (www.cirosec.de)*, erläuterte die Probleme bei der Bekämpfung heutiger Schadsoftware. Virenscanner erkennen üblicherweise bekannte Schadprogramme. Diese können jedoch so gestaltet sein, dass sich ihre Strukturen mehrmals täglich ändern. Dem können die Scanner nicht mehr folgen. Im Darknet sind Toolkits erhältlich, mit denen man für jeden Anwendungsfall ein neues Stück Schadcode einfügen kann. So wie Wildtie-

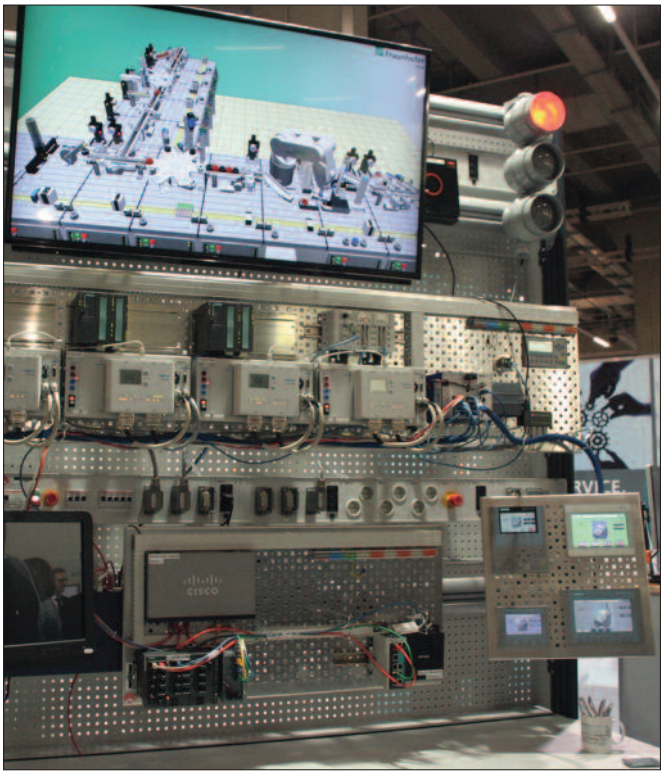
FOTOS: KURT HICKISCH

re zur Tränke ziehen und dort zur leichten Beute für Löwen werden, platzieren *Watering Hole Attacks* Schadprogramme auf vielbesuchte Webseiten. Beim Abrufen dieser Seiten übertragen sich diese Programme auf die Rechner der Abrufenden.

Je nach dem Personenkreis, den der Angreifer treffen will, werden Webseiten infiziert, die bevorzugt von Nutzern einer Zielgruppe (Finanz- und Wirtschaftsfachleute, Wissenschaftler, Unternehmer) besucht werden. Noch weiter geht die Personalisierung von Angriffen, wenn beispielsweise Schadcode in Bewerbungsunterlagen verpackt wird, die an die Personalabteilung eines Unternehmens gesendet werden.

Allen diesen Angriffen ist gemeinsam, dass sie immer häufiger mit fortschrittlicher (advanced) Technik erfolgen, zum Unterschied von bloßem Zufalls-Hacking zielgerichtet und, nicht als Einzelattacke, sondern als Kampagne mit Beharrlichkeit (persistent) durchgeführt werden, im Bestreben, möglichst lange unentdeckt zu bleiben, um an die wertvollsten Zielobjekte zu gelangen.

Diesen Angriffen, denen gegenüber ein Anwender kaum eine Chance hat, müssen neue Techniken entgegengesetzt werden. In diesem Kontext hat sich der Begriff der Threat Intelligence entwickelt. Kommerzielle Anbieter beobachten, von welcher Seite her welche Angriffe erfolgen. Dadurch können Listen von zu sperrenden URLs entwickelt werden. Oder es wird versucht, proaktiv aus den Untergrundforen jener Spezialisten, die derart technisch hochstehende Schadprogramme entwickeln, Informationen zu erhalten, um frühzeitig die Absichten des Gegners erkennen und Abwehrmaßnahmen treffen zu können. Beispielsweise hat das Unternehmen *iSight Partners (www.isightpartners.com)* 300 Experten in 16 Ländern unter Vertrag. Die von diesem Unternehmen herausgegebenen Reports beschreiben für die jeweiligen Auftraggeber (Konzerne, Automobilindustrie, Energiewirtschaft) die zu erwartende Bedrohungslage.



***it-sa* in Nürnberg: Veranschaulichung des Zusammenspiels verschiedener Komponenten im „Internet der Dinge“.**

Götz Bundschuh von der Wirtschaftsprüfungsgesellschaft *EY (www.de.ey.com)* brachte ein Fallbeispiel über die Vorgangsweise bei APT-Angriffen. Die Anunak-Gruppe ist seit 2013 im osteuropäischen Raum aktiv, mit verteilten Teams in der Ukraine, Belarus und der Russischen Föderation. Mit der Methode, die Software von Geldautomaten zu kompromittieren, sodass unautorisierte Geldabhebungen möglich wurden, wurde 2013 und 2014 ein Gesamtschaden von ca. 200 Millionen Euro verursacht. Betroffen waren 50 Banken und fünf Interbank-Clearing-Häuser. Zwei Banken verloren ihre Lizenz und wurden geschlossen. 2015 sind erste Fälle in den USA und Westeuropa aufgetreten.

Zunächst wurden E-Mail-Adressen und Telefonnummern von in Betracht kommenden Bankmitarbeitern ermittelt. Diesen wurde mit gefälschter Absender-Adresse eine Mail der russischen Zentralbank gesendet, mit einem passwortgeschützten Anhang mit infiziertem Word-Dokument. Der Mitarbeiter wurde daraufhin angerufen, um ihm das Passwort mitzuteilen und auch sicherzustellen, dass der Anhang geöffnet wird.

Durch das Öffnen erfolgte die Infektion mit einem Trojaner, der einen Fernzugriff auf den PC des Mitarbeiters ermöglichte. Über den Fernzugriff wurde eine

IT-SICHERHEITSMESSE

it-sa 2015

Bei der vom 6. bis 8. Oktober 2015 im Messezentrum Nürnberg abgehaltenen IT-Sicherheitsmesse *it-sa* waren 428 Aussteller (2014: 385) aus 18 Ländern vertreten.

Die jährliche Sicherheitsmesse *it-sa* ist von der Zahl der Aussteller her die größte IT-Fachmesse Europas und eine der weltweit wichtigsten Fachmessen zur IT-Security. Es wurden 9.015 Fachbesucher aus 34 Ländern und drei Kontinenten gezählt (2014: 7.390).

In drei Foren (Auditorium, Forum Blau für Technik, Forum Rot für Management) wurden, zumeist im Viertelstunden-Takt, über 250 Vorträge angeboten, die unter *www.it-sa.de/foren* als Videomitschnitt sowie zum Download der Präsentationen abgerufen werden können. Höhepunkte unter den Vorträgen waren die Live-Hackings.

Sonderflächen zu bestimmten Themen wie etwa das *Data Center Plus* für IT-Systeme und Rechenzentren oder die *IAM-Area* für die Verwaltung digitaler Identitäten erleichterten den Überblick über das Angebot. Zwei Flächen boten Startup-Unternehmen die Möglichkeit, sich zu präsentieren. Die Messe wurde begleitet vom *Congress@it-sa,* bei dem in 13 Vortragsreihen Fragen zur IT-Sicherheit vertieft wurden.

Die nächste *it-sa* findet vom 18. bis 20. Oktober 2016 im Messezentrum Nürnberg statt.

www.it-sa.de

Foto: Kurt Hickisch

***it-sa* in Nürnberg: Stand der auf Datenrettung spezialisierten Firma Attingo aus Wien.**

Administrator-Software installiert, die Passwörter von lokalen Administratoren geknackt und initiale Infektionsspuren entfernt. In weiterer Folge wurde der Mailverkehr überwacht, um weitere Passwörter und vertrauliche Informationen zu erhalten und um erkennen zu können, ob der Kompromittierung auf die Spur gekommen wurde. Die Administrator-Arbeitsplätze wurden überwacht, um Gegenmaßnahmen vorgreifen zu können. Mit Administrator-Accounts wurden Mails versendet, um eventuell verdächtige Handlungen als legitim zu tarnen.

Nach im Durchschnitt sechs Wochen war der Zugriff auf das Bankautomaten-Netz möglich. Es wurde eine modifizierte Wartungs-Software installiert, mit der zunächst die Nummern der Geldkassetten vertauscht wurden. Die 100-Rubel-Kassette wurde durch die 5.000 Rubel-Kassette ersetzt. Im weiteren Ausbau wurde ein Abheben ohne Karte ermöglicht.

Abhörschutz. Die auf Abhörschutzlösungen für Unternehmen und Behörden spezialisierte *Secusmart GmbH (www.secusmart.com)* präsentierte die Ergebnisse einer Befragung von Fach- und Führungskräften aus verschiedenen Branchen der deutschen Wirtschaft und Industrie zur Frage „Wie sicher ist Deutschlands Unternehmenskommunikation?“. Nach dieser Studie befürchten 92 Prozent der Befragten Lauschangriffe auf den Bereich Forschung und Entwicklung.

Als die drei größten Sicherheitsrisiken wurden Hackerattacken auf das Firmen/Behördennetzwerk angesehen (66 %), Lücken im IT-Sicherheitsmanagement (50 %) und Lücken in der Smartphone-Kommunikation (47 %). Dass sich die organisierte Kriminalität weltweit mehr auf Abhörangriffe ausweiten wird, befürchteten 61 Prozent der Befragten. Gemeinsam mit Vodafone hat das Unternehmen eine hochsichere Sprachverschlüsselungs-App für Android und *iOS*-Smartphones entwickelt *(Vodafone Secure Call)*. Die Nutzung des Dienstes ist nicht an einen Vodafone-Mobilfunkvertrag gebunden und ist von der genutzten Übertragungstechnologie (EDGE, UMTS, LTE) unabhängig.

Datenrettung. „Große Unternehmen sollten bereits im Vorfeld Überlegungen anstellen, was bei technischen Defekten zu tun ist, die zu Datenverlust führen könnten“, sagte DI Nicolas Ehrschwendner, Geschäftsführer des Wiener Unternehmens *Attingo Datenrettung GmbH (www.attingo.at)*. Im Ernstfall, wenn beispielsweise im Spital der Hauptserver ausfällt oder in der Industrie die Produktion stillsteht, im Branchenverzeichnis hektisch nach Unternehmen zu suchen, die Datenrettung anbieten, könnte zu Briefkastenfirmen führen, die die Datenträger ohne Wissen des Kunden bloß weiterschicken.

Datenrettung wird von den meisten Anbietern als IT-Dienstleistung und somit als freies Gewerbe angesehen. Eine Zertifizierung, die dem Kunden entsprechende Sicherheit bieten würde, hat sich bisher noch nicht durchsetzen können. Vorab sollte man sich über geeignete Unternehmen erkundigen, diese im Firmenbuch überprüfen, sich die Labors zeigen lassen. Datenverlust sei zu 70 Prozent auf Hardwareschäden (zum Beispiel Headcrash bei Festplatten) zurückzuführen und zu 30 Prozent auf Fehler des Anwenders, sagte Ehrschwendner. Attingo hat ein Ersatzteillager mit mehr als 10.000 Festplatten in Wien.

Jedenfalls sollte ein in Panik erfolgendes Ein- und Ausschalten vermieden werden. Durch das wiederholte Hochfahren würde sich bei einem Headcrash der Schaden nur noch verschlimmern, betonte Ehrschwender. Das Unternehmen bietet einen kostenlosen Rund-um-die-Uhr-Anrufservice an, bei dem geschulte Mitarbeiter eingetretene Schäden bereits abschätzen können. Defekte Platten werden abgeholt. In Reinraumlabors in Wien, Hamburg und Amsterdam werden die Daten wieder rekonstruiert.

Wichtig, beispielsweise für die Entsorgung von Computern, kann auch sein, Datenträger unrettbar zu zerstören. Mit einem einfachen, händisch bedienbaren Gerät, das die Firma *ADR AG Advanced Digital Research (www.adr-ag.de)* vorgestellt hat, werden über eine Hebelvorrichtung mit einem konisch zugespitzten Stempel Löcher durch die Festplatte gepresst. Dadurch wird diese so nachhaltig zerstört, dass eine Rekonstruktion der Daten, wenn überhaupt, nur mehr mit unverhältnismäßig großem Aufwand möglich ist.

Am dritten Messetag war Edward Snowden live aus seinem Asyl in Russland zugeschaltet. Er wies darauf hin, dass für Datenschutz und -sicherheit auf politischer und technischer Seite gekämpft werden müsse. So schnell wie möglich sollten flächendeckend Verschlüsselungslösungen eingesetzt werden. *Kurt Hickisch*

FOTO: KURT HICKISCH