Chancen und Risiken

Chancen und Risiken der Informationstechnologie sowie Strategien zur Bewältigung von IT-Problemen waren Schwerpunkte beim 24. Symposium Sicherheit der Erste Group in Wien.

Unter dem Leitthema „Wir können den Wind nicht ändern, aber die Segel anders setzen“, einem Zitat von Aristoteles, fand vom 16. bis 18. Oktober 2017 im *Erste-Campus* in Wien das *24. Symposium Sicherheit* der *Erste Group* statt.

Joe Pichlmayr, geschäftsführender Gesellschafter des in Wien ansässigen Virenschutz-Unternehmens *Ikarus (www.ikarussecurity.com),* gab einen Überblick über Ransomware, die Art der derzeit am häufigsten auftretenden Schadprogramme. Von den rund 350 aktiven Ransom-Familien sind *CryptoWall 4.0, Locky, TeslaCrypt* und *Goldeneye* die bedeutendsten. Als Lockerware (37 %) versperren sie dem Opfer den Zugriff auf seine Dateien, als Cryptoware (63 %) verschlüsseln sie seine Dateien. In beiden Fällen wird Lösegeld (Ransom) verlangt, um die Maßnahmen rückgängig zu machen. Das Lösegeld liegt zwischen 300 bis 8.000 Euro, je nach Zielgruppe, zahlbar in *Bitcoins*.

Wenn die Algorithmen sauber programmiert wurden, kann die hochwertige Verschlüsselung nicht „geknackt“ werden. Allenfalls eröffnen Fehler in der Programmierung Möglichkeiten dazu. Ferner wird psychologischer Druck aufgebaut: Ein ablaufender Sekundenticker zeigt an, wie viel Zeit zur Lösegeldzahlung noch zur Verfügung steht, bis die Dateien unwiederbringlich gelöscht oder verschlüsselt werden. Oder es wird schrittweise Datei um Datei gelöscht und dies angezeigt. Ob bei Zahlung des geforderten Lösegeldes der *Key* zur Entschlüsselung übermittelt wird, bleibt fraglich.

Symposium Sicherheit Erste Group: Schematischer Aufbau einer Anlage zum Schutz von Bankomaten vor Gassprengung.

Neuerdings werden auch „Soft Targets“ wie Krankenhäuser oder Webhoster angegriffen. Hinter der Entwicklung dieser Schadsoftware stecken arbeitsteilig organisierte Unternehmen, die ihre Produkte im *Darknet* von billiger Massenware bis zur teuren Maßanfertigung anbieten und die Versendung von Ransomware auch als Dienstleistung übernehmen *(Ransomware as a Service – RaaS)*. Die meisten Angreifer sind Trittbrettfahrer, die bereits bewährte Schadcodes einsetzen.

Verbreitungswege sind hauptsächlich E-Mails mit Anhängen, die unachtsam geöffnet werden. Mittlerweile kommen auch soziale Medien, Foren, mobile Browser und USB-Sticks als Infektionsquelle in Betracht. Das im Mai 2017 aufgetretene Schadprogramm *WannaCry,* mit dem erstmals Wurm-Technologie mit Ransomware verknüpft wurde, nutzte ohne weitere Interaktion eine Schwachstelle aus und infizierte 230.000 Computer in 150 Ländern. Etwa zwei Monate später rollte mit *Petya* eine zweite Ransom-Welle um den halben Globus.

Abhilfe gegen diese Art von Erpressung bieten regelmäßige Datensicherungen in nicht zu langen Abständen. Wegen der Gefahr der Infektion auch der Back-ups sollten die hiefür verwendeten Medien nach der Datensicherung vom System getrennt werden. Mit laufenden Sicherheitsupdates sind die Betriebssysteme und Browser am letzten Stand zu halten. Firewalls, Intrusion-Detection-Systeme, Virenscanner und Spamfilter sind nach wie vor unverzichtbar.

Wirtschaftsspionage.

„Heute lassen sich aus den weltweit zur Verfügung stehenden Quellen Informationen gewinnen, die früher nur über Agenten zu beschaffen waren“, sagte Kurt Leichtfried vom Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT). Wirtschaftsspionage und Unternehmensspionage hätten gemeinsam, dass Geschäfts- und Betriebsgeheimnisse inländischer Unternehmen und Forschungseinrichtungen gezielt ausgeforscht würden. Nur die Akteure seien andere, nämlich bei Wirtschaftsspionage ausländische Nachrichtendienste zur Stärkung der Wirtschaft des jeweiligen Staates. Unternehmensspionage hingegen erfolge durch Wirtschaftsunternehmen mit zivilen Akteuren und zu Zwecken des unlauteren Wettbewerbs.

Als Informationsquellen dienten offene Quellen, das Eindringen in Informationssysteme sowie Mitarbeiter, die entweder unbewusst „abgeschöpft“ oder aus persönlichen Motiven zu angeworbenen und geführten Innentätern würden. Spuren von Einbrüchen, bei denen aber augenscheinlich nichts entwendet wurde, sollten den Verdacht auf Spionage aufkommen lassen. Es könnten Daten- oder Aktenkopien angefertigt oder Lausch- und Späheinrichtungen angebracht worden sein. Der Schaden durch Wirtschafts- und Industriespionage für österreichische Unternehmen werde auf etwa eine Milliarde Euro pro Jahr geschätzt, bei annähernd 8.400 betroffenen Unternehmen.

Bewusstseinsbildung.

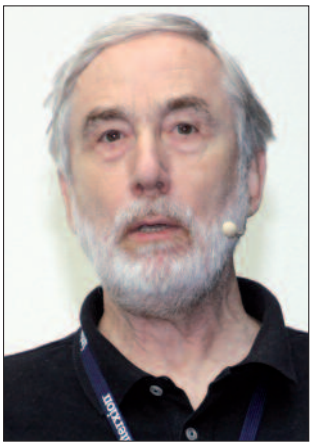
Reinhold Wochner, Group-CSO der *Erste Bank,* berichtete über das *Scrum*-Modell, das gegenüber dem Wasserfallmodell (Planen, Aufbauen, Testen, Überprüfen und dann erst Ausrollen, mit bindenden Vorgaben für die jeweils nächste Phase) schneller und flexibler sei, um beispielsweise Projekte zur Bewusstseinsbildung zu entwickeln. Das *Scrum*-Modell setzt sich funktionell aus dem Product-Owner, dem

FOTO: KURT HICKISCH

Scrum-Master und dem *Scrum*-Team zusammen. Der Product-Owner gibt das zu erreichende Ziel nicht in fest umrissenen Aufgaben, sondern eher als Vision vor. Das aus drei bis neun Personen verschiedener Fachrichtungen besetzte (Entwickler)-Team organisiert sich selbst und produziert in kurzen Abständen („Daily Sprints“) erfolgenden Sitzungen Zwischenergebnisse, die bis zum Erreichen des Ziels immer weiter verbessert werden. Bei Aufsplitterungen entscheidet der Owner, welcher Weg weiterverfolgt werden soll. Bereits in diese Prozesse (und nicht erst beim fertigen Endprodukt) sind Sicherheitsaspekte einzubringen. Der *Scrum*-Master sorgt dafür, dass das Team ungehindert arbeiten kann. Der Vorteil des *Scrum*-Modells liegt in der Anpassungsfähigkeit an komplexe, nicht von Anfang an zur Gänze durchschaubare Strukturen.

Bei der *Kanban*-Methode werden Kärtchen, die in Kurzfassung die zur Erfüllung der Aufgabe notwendigen Anforderungen enthalten, auf einer Pinnwand präsentiert und von dort in wöchentlichen Sitzungen abgearbeitet.

Einmalige Initiativen zur Hebung der Awareness im Sicherheitsbereich würden oft rasch vergessen, an Awareness-Maßnahmen gewöhne man sich, angeordnete Fortbildung werde bloß ertragen, führe aber zu keiner Sicherheitskultur. Spielerische Elemente einzubringen, steigere Motivation und Lernerfolge, erläuterte Dietmar Prantner, Information Risk Manager bei *ING-DiBa Austria*. Spielerisch Erlerntes merke man sich zudem leichter und länger. Spielen stärke auch den Zusammenhalt eines Teams. *Gamification* bestehe darin, bei festgesetzten Regeln im Wettbewerb mit anderen ein klar definiertes Ziel zu erreichen – etwa das Erarbeiten von Lernprogrammen. Der Fortschritt könne durch die Vergabe von Punkten oder Fortschrittsbalken ersichtlich gemacht werden. Freiwilligkeit der Teilnahme sei Voraussetzung. Vollends in eine Spielwelt mit Lernerfolgen eintauchen könne man in gegeneinander antretenden Teams bei Spielen wie *Cyber Resilience Game, Risk Game* oder *Crisis Game*.



Philipp Schaumann: „Techniker bauen Geräte, die sicher funktionieren, bedenken aber Fragen der IT-Sicherheit nicht.“

Christian Sageder: „Die Drohnenabwehr muss in ganzheitliche Sicherheitskonzepte eingebunden werden.“

Drohnen. Das Aufkommen von Drohnen mache den Luftraum oberhalb von zu schützenden Objekten zu einer Sicherheitslücke, erläuterte DI Christian Sageder vom *Österreichischen Wachdienst (ÖWD)*. „500-Dollar-Drohnen fordern die Sicherheitsindustrie heraus“. Die Zahl der Drohnen in Österreich wird auf 50.000 bis 100.000 geschätzt. Weltweit wurden 2015 mehr als 16 Millionen Hobby-Drohnen ausgeliefert; bis 2021 werden es 67 Millionen sein. Die Drohnenabwehr müsse in ganzheitliche Sicherheitskonzepte eingebunden werden, betonte Sageder. Um Abwehrmaßnahmen ergreifen zu können, müssten Detektionssysteme, wie sie vom *ÖWD* angeboten werden, Drohnen mit möglichst hohem Automatisierungsgrad zunächst erkennen und identifizieren können. Es gehe auch um die Sicherung von Beweisen für Überflüge. Nicht invasive Abwehrmaßnahmen seien, Menschen in Sicherheit zu bringen, die Sicht zu versperren, (Zellen) Türen abzuschließen, das Gelände nach abgeworfenen Objekten abzusuchen, nach dem Piloten zu suchen und den Sicherheitsdienstleister zu verständigen. Invasive Maßnahmen seien das Jammen der Funkverbindung, *Jammen* oder *Spoofen* der GPS-Signale und physische Maßnahmen, wie die Drohne abzuschießen oder eine kontrollierte Landung zu erzwingen.

Prävention. Ewald Kronawitter von der Kriminalprävention des Landeskriminalamts Oberösterreich gab einen Überblick über die Organisation der sicherheitspolizeilichen Beratung in Österreich. In Oberösterreich wurden für Präventionsbeamte Ausbildungsmodule für „Eigentumsschutz und Technik“ entwickelt. Nach Absolvierung der Grundmodule Kriminalprävention im E-Learning folgen vier weitere, jeweils mehrtägige Module, die neben einer technischen Ausbildung im Einbruchsschutz auch Rhetorik und Präsentationstraining umfassen. In jährlichen Follow-ups wird das erworbene Wissen auf dem letzten Stand gehalten. Ziel ist, die fachliche Kompetenz bei Beratungen auf ein Niveau zu heben, das mit dem eines Alarmanlagentechnikers vergleichbar ist – ohne diese Tätigkeit aber auszuüben. Zur Sicherheitsunterweisung für Bankangestellte im Kassenbereich wurde ein Schulungsfilm entwickelt, mit Tipps für das Verhalten vor, während und nach einem Banküberfall. Spezielle Beratungen gibt es auch für weitere Risikobetriebe wie Juweliere, Tankstellen, Trafiken. Die sicherheitspolizeiliche Beratung, an die sich jedermann wenden kann, ist unabhängig, produktneutral und kostenlos.

Felia Brugger, Leiterin des Sicherheitsmanagements im *KHM*-Museumsverband, erläuterte Sicherheitsmaßnahmen, die im *Kunsthistorischen Museum* in Wien und in seinen Außenstellen (Hofburg, Wagenburg, Schloss Ambras) bestehen. Diebstahl- und Vandalismusschutz seien nur ein Teil dieser Maßnahmen. Es gehe auch um Brandschutz, Schutz vor Wasserschäden und um die Sicherheit der jährlich etwa 1,5 Millionen Besucher sowie jener Gäste, die die etwa 400 Veranstaltungen im Jahr besuchen. Jährlich einmal erfolgen bei Vollbetrieb zusammen mit Polizei und Feuerwehr Evakuierungsübungen. Es gibt über die Melder durchschnittlich alle drei Minuten eine Alarmmeldung (jemand kommt einem Objekt zu nahe, eine Tür wird unerlaubterweise geöffnet), die alle abgearbeitet würden. Für Notfälle gründete Brugger 2014 den *Notfallverbund Österreichischer Museen und Bibliotheken*. Die etwa

FOTO: KADMY/FOTOLIA

30 dem Verbund angeschlossenen Institute stellen im Notfall Räumlichkeiten für Evakuierungen von Kunstgegenständen zur Verfügung, und helfen einander mit Personal (Restauratoren) aus.

Krisenmanagement. Das Lukaskrankenhaus in Neuss, einer Stadt am Niederrhein in Nordrhein-Westfalen, hat sich einen Ruf als Vorzeigekrankenhaus der Digitalisierung erworben. Durch eine Cyber-Attacke mit Ransomware wurde es am 10. Februar 2016, Aschermittwoch, ab 9 Uhr unvermittelt wieder in die analoge Welt zurückgeworfen. Zunächst gab es uungewöhnliche Fehlermeldungen und Verzögerungen; Bildschirmfenster ließen sich nicht mehr öffnen. Fünf Tage zuvor war noch eine Warnung vor Computerviren ausgesendet worden, mit der Aufforderung, bei einer verdächtig erscheinenden Mail den Anhang nicht zu öffnen.

Der Krisenstab habe sich für ein Herunterfahren der Systeme entschieden, um eine Weiterverbreitung des Virus zu verhindern und Patientendaten zu schützen, berichtete Dipl.-Kfm. Dr. Nicolas Krämer, Geschäftsführer des Krankenhauses. Es wurde auf „Handbetrieb“ umgeschaltet. Papier wurde wieder zum Datenträger. Die Folge: keine elektronischen Verwaltungsprogramme, keine elektronische Befundübermittlung, kein Zugriff auf Kontaktdaten, auf OP-Pläne und Terminkalender; kein Internet und keine E-Mails.

Von Anfang an wurde auf enge Zusammenarbeit mit Polizei, Staatsanwaltschaft und BSI gesetzt sowie auf Transparenz gegenüber den Mitarbeitern, den Patienten und der Öffentlichkeit. Wegen eines gleichartigen Angriffs auf das *Hollywood Presbyterian Medical Center* in Kalifornien ergab sich auch eine Zusammenarbeit mit dem FBI. Beschlossen wurde, kein Lösegeld zu bezahlen. In drei Schichten wurde rund um die Uhr an einer Wiederherstellung der IT-Systeme gearbeitet. Am Sonntag, 14. Februar, konnte erste Entwarnung gegeben werden. Am nächsten Tag wurde, nach Prioritäten gestaffelt, begonnen, die Systeme wieder hochzufahren. Ab dem 25. Februar wurden, nach dem Motto Sicherheit vor Funktionalität, die Systeme revitalisiert. Am 18. März erfolgte eine Abschlusskonferenz. Hinweise auf Kompromittierung von Patientendaten ergaben sich nicht.

Dem Krankenhaus entstand durch zusätzliche Kosten ein Schaden von etwa einer Million Euro, es gab aber keinen nennenswerten Ausfall bei den Einnahmen. Auch war kein Vertrauensverlust festzustellen.

Nach der Amokfahrt eines Autofahrers am 20. Juni 2015 in Graz mit drei Toten und 36 Verletzten waren nicht nur die Rettungs- und sonstigen Einsatzkräfte gefordert, sondern es musste auch das weltweite Medieninteresse bewältigt werden. Darüber berichtete der Magistratsdirektor der Stadt Graz, Dr. Martin Haidvogl. Am Tag der Amokfahrt wurden vom Krisenstab Pressekonferenzen veranstaltet und es wurde über *graz.at* und *Facebook* informiert. Um die Trauer und das Mitgefühl der Menschen behutsam in Bahnen zu lenken, wurde am Portal der Stadtpfarrkirche ein zentraler Gedenkort errichtet, zu dem die mittlerweile an den einzelnen Tatorten aufgestellten Kerzen und abgelegten Blumen zusammengetragen wurden.

Die Gedenkstätte wurde durch den päpstlichen Nuntius gesegnet. Noch am Abend wurde ein Kondolenzbuch aufgelegt und ein solches auch im Internet eingerichtet. Während der anschließenden Trauerwoche wurde im Rathaus ein Kriseninterventionsteam mit 140 ehrenamtlichen Mitarbeitern eingerichtet, die bei 500 Einsätzen insgesamt 7.440 Stunden leisteten. Die Straßen wurden gereinigt, ein Spendenkonto eingerichtet, Veranstaltungen abgesagt, Hochzeiten verlegt. Mit einem Gedenkmarsch am 28. Juni 2015 mit 12.000 Teilnehmern, darunter fast die gesamte Bundesregierung, wurde die Trauer offiziell für beendet erklärt.

„Rituale und Symbole sind wichtig, auch, mit Bildern zu sprechen“, betonte Haidvogl. Wichtig sei, wieder den Übergang zur Normalität zu finden. Gezeigt habe sich ein enormer Zusammenhalt der Bevölkerung.

Symposium Sicherheit: Der Österreichische Wachdienst präsentierte Detektionssysteme zur Drohnenabwehr.

Ausblicke. Im *Internet of Things* sind alle Geräte miteinander vernetzt, und in alle kann eingegriffen werden. Die Ursache dafür sah Dipl.-Phys. Philipp Schaumann in aus der Elektrotechnik kommenden Entwicklern, die Geräte zum sicheren Funktionieren bringen (Safety), aber Fragen der IT-Sicherheit (Security) nicht bedenken würden.

„Wenn Sie Ihr Garagentor mit der Fernbedienung bedienen können, können das andere auch.“ Dabei gebe es für IT-Sicherheitsprobleme längst Lösungen. Für Hersteller allerdings gelte es, rasch auf dem Markt zu sein, möglichst viele „Features“ und bequem bedienbare Produkte anzubieten. Andererseits könnten Benutzer, die durch ihr Kaufverhalten Einfluss auf die Hersteller nehmen könnten, „Sicherheit“ nicht beurteilen. Die Lösung sieht Schaumann in der Einführung eines Gütesiegels, wie es beispielsweise für elektromechanische Geräte in Form des VDE-Zeichens bereits besteht.

„Von der menschenähnlichen Maschine sind wir nicht mehr weit weg“, meinte Damianos Soumelidis *(Nagarro Managements)*. Humanoide Roboter würden in der Betreuung von Menschen eingesetzt. Roboter anderer Art würden an im 3D-Druck aus Weichplastik hergestellten Organen lernen und chirurgische Operationen durchführen. *Virtual Reality* werde es ermöglichen, unabhängig von Zeit und Ort Konferenzen abzuhalten, sich sein Haus mit Möbeln einzurichten, im Supermarkt einzukaufen und touristische Sehenswürdigkeiten zu besichtigen. Die Entwicklung werde man nicht verhindern können, sondern man sollte versuchen, aktiv daran teilzunehmen. *Kurt Hickisch*

FOTOS: KURT HICKISCH