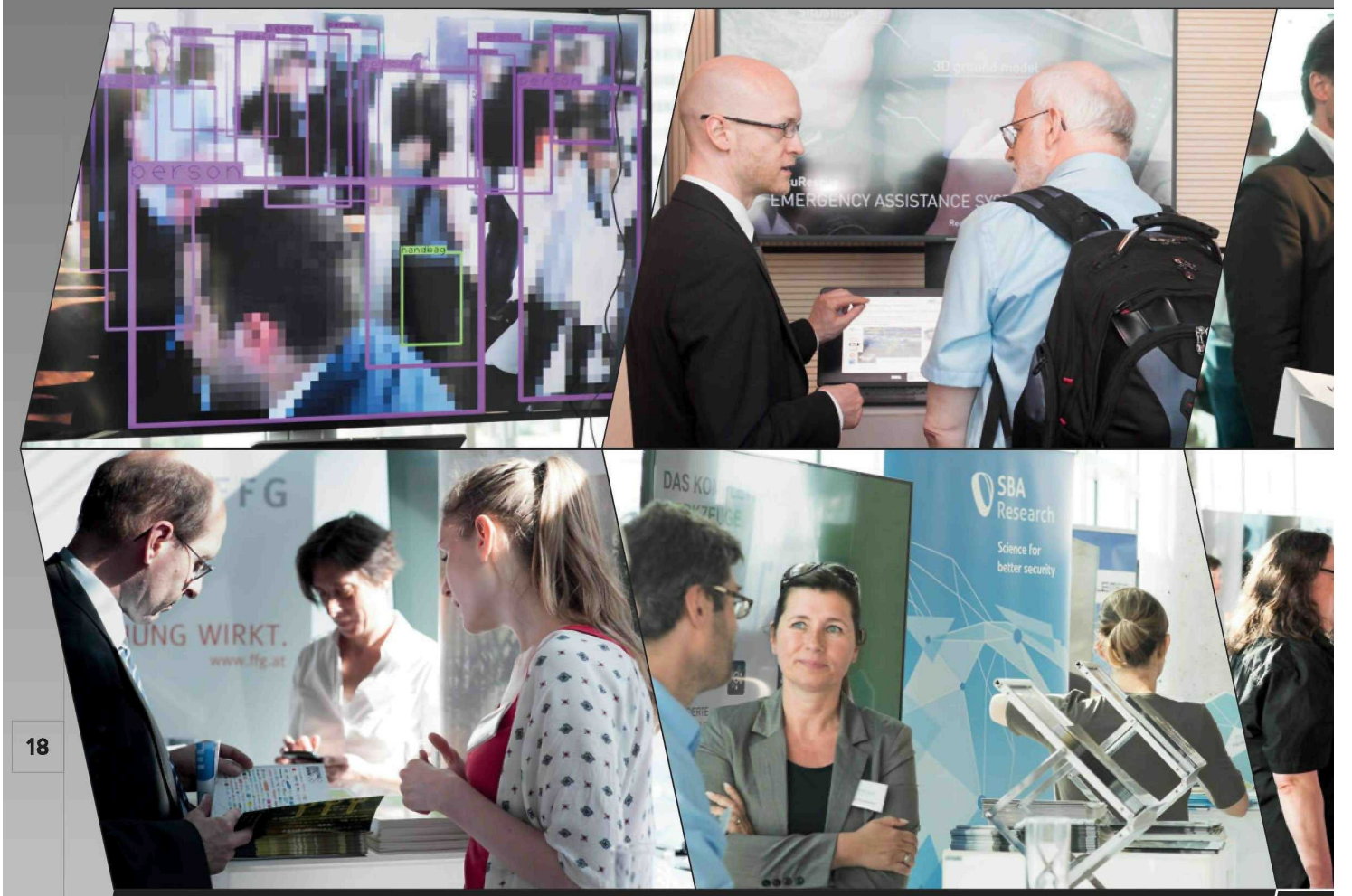
»OBSERVER«

Report (+) Plus
Mehrwert für Manager
Wien, im Juni 2017, Nr: 6, 11x/Jahr, Seite: 18-23
Druckauflage: 27 000, Größe: 95,6%, easyAPQ: _
Auftr.: 9626, Clip: 10672031, SB: Qualysoft GmbH

www.observer.at



SICHERHEITSTECHNOLOGIEN FÜR DEN GLOBALEN MARKT

Österreichische Spitzenforschung und Unternehmen mit globaler Marktpräsenz waren Themen der Technologieausstellung »Sehen und Verstehen – Cybersecurity« des AIT Austrian Institute of Technology Ende Mai.

An insgesamt 27 Ständen präsentierte die österreichische Spitzenforschung gemeinsam mit heimischen Top-Unternehmen neueste Sicherheitstechnologien, Dienstleistungen und Produkte zu wichtigen und aktuellen Cybersecurity-Herausforderungen. Den Abschluss des gut besuchten Events am 30. Mai im Wiener Tech Gate bildete eine Podiumsdiskussion, zur der Gastgeber Helmut Leopold, Leiter des Centers für Digital Safety & Security am AIT, Führungskräfte erfolgreicher österreichischer IT-Security-Unternehmen geladen hatte. Vorgestellt und diskutiert wurden »Österreichische Sicherheitstechnologien im Spannungsfeld heimischer Markt vs. globaler Markt«.

Der Grundtenor der rund einstündigen Diskussion: Österreichische Cybersecurity-Technologien genießen international vielfach hohes Ansehen, werden jedoch im eigenen Land oft nur ungenügend in ihrer Exzellenz wahrgenommen. Mit anderen Worten: »Österreich ist Weltspitze, aber hierzulande unbemerkt.« Es sind vor allem mentale Dispositionen, »wonach der Prophet im eigenen Land nichts zählt«, die eine durch-

»OBSERVER«

Report (+) Plus
Mehrwert für Manager
Wien, im Juni 2017, Nr: 6, 11x/Jahr, Seite: 18-23
Druckauflage: 27 000, Größe: 96,43%, easyAPQ: _
Auftr.: 9626, Clip: 10672031, SB: Qualysoft GmbH

> Mit dem akademischen Know-how und den vielen Forschungszentren ist Österreich Weltspitze in Hightech. »

schlagende Industrialisierung österreichischen Know-hows rund um das Thema Cybersecurity erschweren. Das nationale Bekenntnis müsse über die durchaus gut organisierte F&E-Förderung hinausgehen, um wirklich Märkte für die heimischen Spitzenentwicklungen zu schaffen, war man sich am Podium einig.

Die Ausstellung selbst wurde in Ergänzung zu Informationsständen des AIT von Cybersecurity-Unternehmen und Forschungspartnern des Forschungsinstituts bestückt: Huemer IT Solution, Thales Austria, CyberTrap Software, Ardexa, SBA Research, RadarServices Smart IT-Security, LieberLieber Software, Riegl Laser Measurement Systems, Ikarus Security Software, T-Systems Austria – sowie Wirtschaftsagentur Wien, DigitalCity Wien, Österreichische Forschungsförderungsgesellschaft FFG und das KIRAS Sicherheitsforschungsprogramm des Bundesministeriums für Verkehr, Innovation und Technologie. ■

DIESE SCHWERPUNKTE ZEIGTE DAS AIT

1. Cybersecurity-Kompetenz & Cyber-Range-Trainingscenter: Die Erfahrung des AIT im Cybersektor wurde am Stand »Resiliente Cyber-Infrastrukturen durch künstliche Intelligenz« demonstriert. Hier arbeiten ExpertInnen an Technologien und Lösungen im Bereich Machine-Learning, um zukünftigen Bedrohungen für kritische IKT-Systeme begegnen zu können. Um dazu Stakeholder aus Industrie, Wissenschaft und der öffentlichen Hand auf einem gemeinsamen, aktuellen Wissensstand zu bringen, wurde die Trainingsplattform »Castle« gemeinsam mit der IAEA aufgebaut und betrieben. Hier wird eine praxisbezogene Produktionsumgebung simuliert, um den richtigen Umgang mit Sicherheitsvorfällen und Attacken in verschiedenen Erfahrungsstufen zu trainieren und zu analysieren.

2. Crowd-Tasking-Services und Lagebilderstellung für das Krisen- und Katastrophenmanagement: Das Österreichische Rote Kreuz hat die Resilienz der Bevölkerung und der Freiwilligen zu einer der großen Herausforderungen im Krisen- und Katastrophenmanagement erklärt. Am AIT werden Kommunikationsinstrumente entwickelt, die auf dem Einsatz neuer Social-Media-Kanäle basieren und für den optimierten Einsatz von Freiwilligen der Initiative »Team Österreich« des Roten Kreuzes geschaffen wurden. Auf diese Weise wird eine effektive Kommunikationsplattform für die Interoperabilität aller Akteure – Behörden, Ministerien, Bund, Länder, Gemeinden, NGOs und Bevölkerung – geschaffen.

3. Big-Data- und Blockchain-Kompetenz in Österreich: Ob im Kampf gegen Cyberkriminelle im jüngst gestarteten EU-Projekt Titanium oder zur Entwicklung neuer Blockchain-Dienste für die Wirtschaft: Das AIT bietet mit der in jahrelanger Forschungsarbeit entwickelten »GraphSense«-Plattform ein Tool zur forensischen Analyse virtueller Währungstransaktionen. Die Big-Data-Analyseplattform kann hunderte Gigabyte in wenigen Minuten verarbeiten und ist durch die darunterliegende verteilte und somit skalierbare Rechner-Infrastruktur auch für die Zukunft gerüstet. Wichtige Grundlagen für die Entwicklung des Graphsense-Tools wurden im bilateralen KIRAS Projekt BITCRIME, das vom BMVIT gefördert wurde, geschaffen.
Ziel von Titanium ist wiederum die Entwicklung technischer Lösungen zur Untersuchung und Bekämpfung krimineller und terroristischer Handlungen im Netz, die mithilfe virtueller Währungen begangen werden.

4. »Security by Design« für Industrial Control Systems: Die zunehmende Komplexität der IT-Systeme verlangt neue Methoden der Systementwicklung, um Sicherheitsmaßnahmen aber auch den Schutz der Privatsphäre von Anfang an im Systemdesign zu berücksichtigen. Das AIT hat dazu im Rahmen internationaler Forschungsinitiativen gemeinsam mit Betreibern kritischer Infrastrukturen, wie Energienetzbetreibern und Herstellern von IT-Systemen, neue Methoden und Werkzeuge entwickelt, um sichere Systeme bauen zu können. Dazu gehören auch neue kryptographische Lösungen, wie zum Beispiel intelligente Verschlüsselungstechnologien, um IoT-Sensorsysteme und Cloud-basierte Systemlösungen vor unerlaubten Datenzugriff zu schützen, sowie auch die laufende Selbstüberprüfung von IT-Systemen im Betrieb. Bei diesem modernen Monitoring (Runtime-Verification) und modernsten Testwerkzeugen von cyber-physikalischen Systemen hat AIT international eine führende Rolle eingenommen.

»OBSERVER«

Report (+) Plus
Mehrwert für Manager
Wien, im Juni 2017, Nr: 6, 11x/Jahr, Seite: 18-23
Druckauflage: 27 000, Größe: 94,47%, easyAPQ: _
Auftr.: 9626, Clip: 10672031, SB: Qualysoft GmbH

www.observer.at

HELMUT LEOPOLD,

HEAD OF CENTER FOR DIGITAL SAFETY & SECURITY, AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

> »In unserer Forschungsarbeit sind wir dem Markt voraus und können die industrielle Markteintrittszeit und auch die Entwicklungskosten für viele Innovationen halbieren. Dennoch lassen sich nicht sehr viele Industriepartner auf ein offenes Abenteuer mit Technologien ein, die vielleicht noch nicht für den Markt reif sind. Natürlich ist auch die Größe des Marktes in Österreich eine besondere Herausforderung. Ich bin aber überzeugt, dass sich Österreich im Hightech-Sektor nicht zu verstecken braucht. Wir haben ja bereits viele Forschungsergebnisse, die auch vermarktbar sind.

Den 100-Milliarden-Euro-Auftrag wird es in Österreich nicht geben, wir sind hier auch in der Förderlandschaft kleinteiliger unterwegs. Umso wichtiger sind Kooperationen – das betrifft auch den Bereich IT-Security. Dazu braucht es auch mehr Mut, um für künftige Herausforderungen mit neuen Lösungsansätzen gewappnet zu sein und damit echte Marktplätze schaffen zu können. Die Fachkräfte sind jedenfalls in Österreich vorhanden. Dafür sorgen die sehr guten Ausbildungen der heimischen Universitäten und Fachhochschulen. Mit dem akademischen Know-how und unseren vielen Forschungszentren in Österreich sind wir Weltspitze. Die hier vertretenden Unternehmen sind die besten Beispiele für erfolgreiche Produkte am weltweiten Markt. Gegen den Ur-Reflex, große internationale Marken zu kaufen, hilft nur ein größeres Selbstbewusstsein.

Man könnte nun leicht fordern, österreichisches Steuergeld bei Investitionen nur für Produkte und Dienstleistungen aus Österreich auszugeben – ich halte das aber für den völlig falschen Weg. Gerade im Bereich Cybersicherheit sind die geografischen Grenzen verschwimmend. Die heimische Wirtschaft arbeitet sehr erfolgreich mit internationalen Partnern zusammen. Die Ergebnisse daraus kommen uns allen zugute.

Ich gebe zu bedenken, dass in der rasend schnell wachsenden Technologiewelt wichtig ist, im eigenen Land über entsprechendes Know-how zu verfügen. Dynamische Bereiche wie Industrie 4.0, automatisierte Fahrzeuge, Internet of Things – hier Herausforderungen oder Probleme im Nachhinein mit ein paar IT-Beratern zu lösen, wird künftig nicht funktionieren. Deshalb sind österreichische Pilotprojekte und Referenzkunden so wichtig.«

THOMAS HOFFMANN,

CEO RADARSERVICES SMART IT-SECURITY

> »In Österreich und auch in Deutschland – ich würde das auch auf Zentral- und Osteuropa ausweiten – herrscht ein Ingenieursgeist mit einem Qualitätsbewusstsein bei Produkten und Dienstleistungen. Die Kunden sind durchaus bereit, für einen gewissen Level an IT-Sicherheit auch etwas zu zahlen. Viele europäische Anbieter sind hier auch deutlich günstiger als amerikanische Mitbewerber.

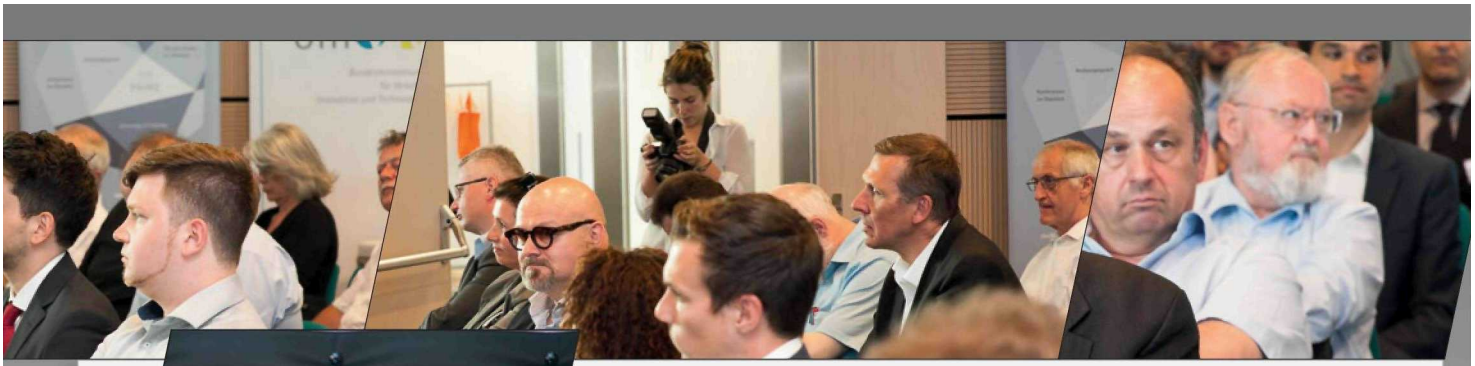
Wir beschäftigen uns mit Sicherheitsmonitoring von IT-Infrastruktur bei Unternehmen. RadarServices überwacht Systeme und bietet punktgenau und tagesaktuell eine Übersicht über drohende Risiken. Wir begleiten unsere Kunden bei ihrem weltweiten Geschäft und befinden uns deshalb mitten im globalen Wettbewerb. Wir können das sehr gut und können mit jedem Wettbewerber im internationalen Umfeld mithalten. Schließlich setzen wir auch auf Eigentechnologie: 25 unserer 130 Leute sind in der Entwicklung und in der Forschung beschäftigt. Mit unseren Qualitätsstandards treffen wir genau die hohen Anforderungen etwa von großen Mittelstandsunternehmen mit ihren jeweiligen Compliance-Vorgaben. Das ist schon ein Riesenunterschied zu Regionen wie den USA, wo Lösungen ›quick and dirty‹ eingekauft werden und dort vor allem einmal ein gutes Marketing zählt.

Spitzentechnologie alleine ist aber nicht entscheidend. Für eine internationale Aufstellung braucht es auch die Unterstützung österreichischer Behörden als staatlicher Auftraggeber. In den USA ist das gang und gäbe und hilft aufstrebenden Technologieunternehmen so schnell zu wachsen, wie man das aus Silicon Valley eben kennt. Auch in der Tagespolitik gehen mir die Technologiethemen ab. Das gehört einfach auch ins Bewusstsein in der öffentlichen Diskussion – genauso wie das Thema IT-Sicherheit heutzutage jedem Vorstand und jedem Geschäftsführer wichtig sein sollte.«

»OBSERVER«

Report (+) Plus
Mehrwert für Manager
Wien, im Juni 2017, Nr: 6, 11x/Jahr, Seite: 18-23
Druckauflage: 27 000, Größe: 100%, easyAPQ: _
Auftr.: 9626, Clip: 10672031, SB: Qualysoft GmbH

www.observer.at



PETER OROS, CEO QUALYSOFT GRUPPE

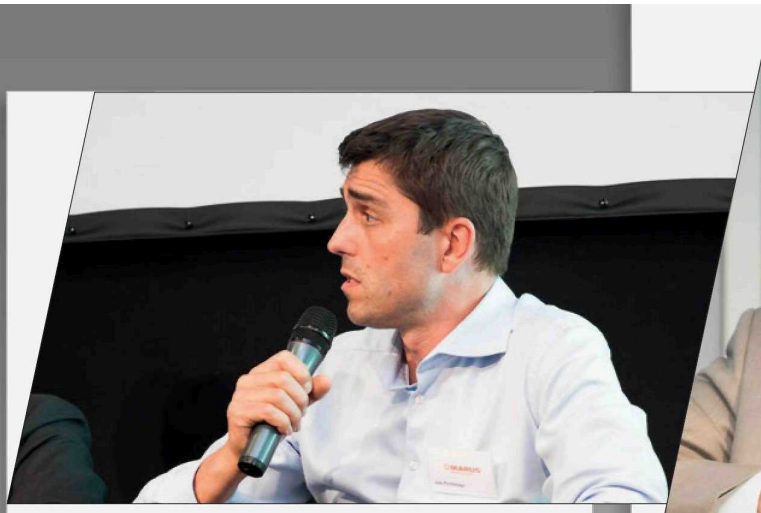
»Seit einigen Jahren ist Qualysoft neben dem Schwerpunkt auf Europa auch in Asien und in den USA tätig. Wir beschäftigen uns mit Lösungen im Bereich E-Government sowie Cybersecurity im Cloud-Umfeld. Wir sind sicherlich nicht der billigste Anbieter auf diesem Markt – das merken wir bei Ausschreibungen –, doch können wir mit unserer Expertise punkten. Auch für uns sind Kooperationen mit Partnern und Forschungsinstituten enorm wichtig, um die vielschichtigen Herausforderungen in der Wirtschaft lösen zu können. Das beginnt schon beim Sicherheitstraining und der Ausbildung der Mitarbeiter in Unternehmen. Langzeitarchivierung von Daten und Dokumenten, Datensicherheit in der Cloud – das wären zum Beispiel geeignete Themen für eine Zusammenarbeit mit dem AIT.

Forscher und Entwickler in Europa ticken anders – Qualität und Ingenieursausbildung sind top. Trotzdem brauchen wir auch Exportunterstützung – andere Länder machen dies mit der aktiven Promotion von Unternehmen durch die Politik vor – und eine bessere Selbstvermarktung. Durch die immer komplexer werdende Vernetzung wird Cybersecurity zur wichtigsten Herausforderung sowohl im privaten, wie auch im beruflichen Umfeld. Für österreichische IT-Firmen ist das nicht nur eine Herausforderung, sondern auch eine große Chance, sich mit ihren hervorragenden Security-Lösungen auf dem Weltmarkt zu etablieren.

Wir leben in einem Zeitalter der Informatik mit Riesenmöglichkeiten für IT-Dienstleister, Hersteller und Forschungsinstitute, die Weltbühne zu betreten. Wann, wenn nicht jetzt? In der ganzen Welt entsteht der Bedarf für IT-Lösungen und für Produktsicherheit auf allen Ebenen und in allen Bereichen. Wir haben hier in Österreich Produkte für diesen Bereich. Jetzt ist der perfekte Zeitpunkt, damit auch ins Ausland zu gehen und die Welt zu erobern.«

»OBSERVER«

Report (+) Plus
Mehrwert für Manager
Wien, im Juni 2017, Nr: 6, 11x/Jahr, Seite: 18-23
Druckauflage: 27 000, Größe: 95,08%, easyAPQ: _
Auftr.: 9626, Clip: 10672031, SB: Qualysoft GmbH



JOSEF PICHLMAYR

CEO IKARUS SECURITY SOFTWARE

»Wir alle sind auf internationale Kooperationen angewiesen, um Gefahren im Netz frühzeitig zu erkennen. Im Bereich der Malware-Protection ist relativ früh ein internationaler Schulterschluss entstanden – die Hersteller hatten rasch die Sinnhaftigkeit gesehen, über den Tellerrand hinauszudenken und zu kooperieren. Dieser stete Austausch von Informationen ist wesentlich effizienter, als Abwehrmaßnahmen einzeln durchzuführen.

Wir sind seit 30 Jahren erfolgreich in den Bereichen Malware-Protection und Content-Security tätig, liefern Bausteine für Sicherheitsarchitekturen etwa im industriellen Umfeld, prüfen und analysieren Inhalte und schützen in der Endpoint-Protection auch PCs, Laptops, Tablets und Smartphones. Unsere Dienste werden überdies auch in Japan sehr geschätzt – mit heuer bereits über 180.000 Mobile-Security-Kunden.

Dennoch könnte in der Security-Branche noch besser zusammengearbeitet werden. Das beginnt bei einer denkbaren gemeinsamen Incident-Response, bei der auch betroffene Unternehmen vertrauensvoll Informationen zu erfolgten Angriffe untereinander austauschen. Dies wäre wichtig, um sich ein Bild über die aktuelle Lage zu machen. Ich denke, dass auch für den Zugang zum europäischen Markt Kooperationen von heimischen IT-Sicherheitsunternehmen helfen würden.

Leider haben wir auch die kritische Masse an Awareness in der Politik zum Thema IT-Sicherheit bei weitem noch nicht erreicht. Es fehlt eigentlich auch eine größere Strategie. Der Etat, welcher der digitalen Roadmap Österreichs zu Verfügung steht, ist gerade einmal 20 Millionen Euro schwer. Da gibt es noch ein großes Potenzial – nicht nur in Österreich, sondern eigentlich in ganz Europa. Die Amerikaner haben sehr früh die Vorteile der globalen Kontrolle von IT-Infrastruktur und Information erkannt.

Heute ist Software im Wesentlichen ein Thema für US-Hersteller, die Hardware kommt von asiatischen Unternehmen. Hier läuft gerade auch ein spannendes Match zwischen den Herstellern, die am liebsten die IT-Sicherheit im Alleingang aus dem Netz bereitstellen würden, und ihren langjährigen Integrationspartnern. Was Europa bleibt, sind seine hellen Köpfe. Solange wir die in ausreichender Zahl haben und ausbilden können, werden wir nicht ins Hintertreffen geraten.«

MARKUS ROBIN

GESCHÄFTSFÜHRER SEC CONSULT

»Als wir 2002 mit den ersten Sicherheits- und Penetration-Tests auf den Markt gekommen waren, war vielen dieses Thema noch völlig unbekannt. Als ›Diagnostiker‹ im Bereich Cyber- und Informationssicherheit beschäftigt SEC Consult das wohl größte White-Hat-Hackerteam in Österreich. Rund 80 Personen simulieren Angriffe auf IT-Infrastrukturen und helfen so den Unternehmenskunden bei der Aufdeckung von Cybersecurity-Schwachstellen. SEC Consult unterstützt auch bei der Behebung dieser Schwachstellen – sowohl bei Prozessen in Bezug auf die Datenschutzgrundverordnung (DSGVO) als auch bei der Entwicklung von sicherer Software. In unserer kleinen, aber feinen Produktpalette befindet sich auch eine Lösung, um Hackern Fallen zu stellen. Die Sicherheitslösung CyberTrap war eine der ersten Deception-Technologies weltweit.

Für diesen technologischen Vorsprung braucht es klar auch eine Zusammenarbeit mit der Forschung. Ein anderes Beispiel ist eines der ersten Smart-Grid-Security-Projekte ›SG2‹ gemeinsam mit dem AIT, bei dem bereits vor einigen Jahren die Sicherheitsrisiken in Energienetz-Infrastrukturen analysiert worden waren.

Wir haben Geschäftsstellen in ganz Europa und auch in Asien. Auch Hersteller im Silicon Valley vertrauen auf SEC Consult. Da im Bereich Sicherheit österreichische Qualität zählt, sind wir gerade dabei, etwa in Singapur große Mitbewerber im Finanzbereich abzulösen. Das zeigt: Wir müssen uns hier nicht verstecken und können erfolgreich exportieren.

Freilich braucht es auch im eigenen Land bessere Rahmenbedingungen und höhere Investitionsvolumina für die Umsetzung von Cybersecurity. Als Herausforderung bei vielen Unternehmen sehen wir die schleppende Vorbereitung auf die im Mai 2018 in Kraft tretende DSGVO. Auf politischer Ebene wurde die Umsetzung der NIS-Richtlinie in nationales Recht nach gutem Beginn im Finish leider völlig verschlafen.

In den USA und in Israel investiert die öffentliche Hand massiv in IT-Sicherheit. Strategien für große Investitionen findet man in Österreich bestenfalls für Verkehrsinfrastruktur. 300 Millionen Euro, die für die Sicherheit von Autobahntunnels in Österrreich ausgegeben werden – von solchen Größenordnungen kann unsere Branche nur träumen.«

»OBSERVER«

Report (+) Plus
Mehrwert für Manager
Wien, im Juni 2017, Nr: 6, 11x/Jahr, Seite: 18-23
Druckauflage: 27 000, Größe: 100%, easyAPQ: _
Auftr.: 9626, Clip: 10672031, SB: Qualysoft GmbH

www.observer.at

Martin Szelgrad (Report) mit Thomas Hoffmann, Helmut Leopold, Peter Oros, Joe Pichlmayr, Markus Robin und Matthias Tischlinger.

MATTHIAS TISCHLINGER

LEITER ABTEILUNG DATA SERVICES BEI ENERGIE AG OBERÖSTERREICH TELEKOM

»Als Dienstleister der Energie AG Oberösterreich sind wir für die komplette technische Kommunikation bis hin zur Systembetreuung der Steuerung von Strom- und Gasleitsystemen verantwortlich. Für mich ist es enorm wichtig, mit österreichischen Unternehmen zusammenzuarbeiten. Für uns ist die Herkunft von Sicherheitslösungen auf jeden Fall ein Thema. Wöchentlich werden Informationen von technischen Hintertüren bekannt, die in Produkten etwa aus den USA oder Israel aufgefunden werden.

Generell gilt: Massenmarktsysteme haben Sicherheitslücken, daher sind Offenheit gegenüber Bedrohungen und ein Threat-Information-Sharing zwischen den betroffenen Unternehmen eine wichtige Voraussetzung für eine sichere Energiezukunft. In der Energiewirtschaft ist diese Zusammenarbeit und ein offener Informationsaustausch sicherlich einfacher, da die Netzbetreiber in einem regulierten Markt agieren und nicht in direkter Konkurrenz zueinander stehen. Hundertprozentige Sicherheit gibt es nirgendwo. Sicherheit kann aber mit entsprechenden Anstrengungen und Schulungen der Mitarbeiter beherrschbar werden. Das betrifft auch Smart Meter, die ebenfalls ständig geprüft und getestet werden müssen. Gerade hier sind wir überzeugt, in die Technik der Zukunft zu investieren. Auch wenn heute viele die Vorteile der Digitalisierung im Stromnetz noch nicht erkennen können – in fünf bis zehn Jahren wird eine flexible Laststeuerung im Smart Grid Standard sein.

Die Energieversorger befassen sich mit der EU NIS-RL Netz- und Informationssicherheitsrichtlinie bereits seit Jahren und führen gemeinsam mit der Regulierungsbehörde E-Control und den Ministerien Risikoanalysen ihrer Systeme durch. Dazu wurde in einem ersten Schritt ein ›Austrian Energy Computer Emergency Response Team (AEC)‹ umgesetzt. Damit wird die Sicherheit erhöht – das wird auch in den Nachbarländern beachtet.«