Gemeinsam für IKT-Sicherheit

Das Bewusstsein für IKT-Sicherheitsmaßnahmen zu stärken, war eines der Ziele der IKT-Sicherheitskonferenz 2013 des Bundesheeres in Linz.

Im Rahmen der Bestrebungen, Bewusstsein für die IKT-Sicherheit in breite Schichten der Bevölkerung und insbesondere der Wirtschaft zu tragen, finden die vom BMLVS getragenen und vom Abwehramt des Bundesheeres organisierten IKT-Sicherheitskonferenzen, beginnend mit Pamhagen im Burgenland 2012, auch in den anderen Bundesländern statt.

Die 12. Konferenz wurde am 5. und 6. November 2013 im Design-Center in Linz abgehalten – mit Unterstützung des Landes Oberösterreich und der Stadt Linz, der FH Oberösterreich sowie zahlreicher Wirtschaftsunternehmen. Die Fachvorträge gliederten sich in die Gruppen „Mensch und Recht", „Sichere Industrie", „Cybersecurity und Management" sowie „Technik – Good Practice". An den beiden Tagen wurde die Veranstaltung von insgesamt mehr als 1.200 Teilnehmern, davon etwa 550 aus dem BMLVS, besucht. Im Foyer waren 36 Aussteller mit Ständen vertreten.

Generalstabschef General Mag. Othmar Commenda gab einen Überblick, wie sich das Bundesheer in den gesamtstaatlichen Prozess der Cybersicherheit einbringt, unter anderem durch ein Cyber-Modul in der Grundausbildung. Landeshauptmann-Stellvertreter Franz Hiesl verwies in seiner Ansprache auf die Notwendigkeit einer Bewusstseinsbildung für die Nutzung des Internet.

Steve Purser berichtete über die Tätigkeit der 2004 gegründeten *European Union Agency for Network and Information Security – ENISA*. Die Organisation versteht sich als Expertengremium, das Institutionen der EU sowie den privaten und öffentlichen Sektor in Fragen der Informationssicherheit zusammenführt. Nicht ein Mehr an Informationen hierüber ist das Ziel, sondern sie auf das Wesentliche zu beschränken und für Risikomanagement und Bewusstseinsbildung anwendbar zu machen. Die Cyber-Strategie der EU – zu deren Realisierung ENISA aufgerufen ist – ist darauf ausgerichtet, Resilienz zu erzeugen, Cyber-Kriminalität drastisch zu senken und die industriellen

Aussteller bei der IKT-Sicherheitskonferenz im Design-Center in Linz.

Simulierter Hacker-Angriff auf eine Smart-Grid-Stromversorgung.

sowie die technischen Ressourcen für Cybersicherheit zu entwickeln.

Einen Einblick, was sich im Cyber-Untergrund abspielt, gab Volker Kozok. Da tummeln sich Cyber-Aktivisten, Cyberoccupier, Cyberwarrior, Cyberleaker. Gemeinsam ist ihnen, dass sie politische Änderungen anstreben, die öffentliche Meinung beeinflussen wollen, gegen staatliche Organisationen auftreten und politische oder soziokulturelle Ziele durchsetzen wollen. Für die Freiheit der Netze treten Hacktivisten und Leaker ein, den anderen geht es eher um Destabilisierung. Gegen missliebige Unternehmen oder Meinungen werden Shitstorms entfacht. Über das Netz ist es leicht wie nie zuvor, Protest zu organisieren, mit Auswirkungen bis in die Stabilität von Staaten („Arabischer Frühling").

Max Klaus, Meldestelle MELANI.

Othmar Commenda, BMLVS.

Der Einsatz von sozialen Netzwerken bietet für Unternehmen Chancen, birgt aber auch Risiken. Die Chancen und der Mehrwert der Nutzung sozialer Netzwerke liegen, wie Tony Wehrstein von *IBM* ausführte, darin, dass sich Experten untereinander austauschen. Damit dabei wichtige Informationen (Patente, Entwicklungen) nicht abfließen, sollen die Gruppen unter sich geschlossen bleiben und für Außenstehende unsichtbar sein. Um dennoch einen Kontakt nach außen zu haben, bietet sich ein firmenintern angelegter „Expertenpool" an. Wird dort eine Problemstellung eingegeben, erfährt der Anfragende, welche Personen für die Lösung dieses Problems in Frage kommen könnten, und kann sich dann, eigenverantwortlich und unter Wahrung der Sicherheitsrichtlinien, mit dem Betreffenden in Verbindung setzen.

Die Risiken bestehen darin, dass sich ein außenstehender Angreifer über ein soziales Netzwerk gezielt in das Vertrauen einer ausgewählten Person einschleicht (Spear phishing) und diese beispielsweise verleitet, einen bestimmten Link anzuklicken. Dieser ist korrumpiert und lädt Schadsoftware auf das Gerät des Opfers (Cross-Site-Scripting; XSS), das in der Folge ausgespäht wird. Eröffnete „Hintertüren" ermöglichen den Zugang zu weiteren Informationen, die vom Angreifer abgesaugt werden. „SQL-Injection, also die Manipulation von Datenbanken durch von außen eingebrachte Befehle, die leicht abgeblockt werden könnten, und Cross Site Scripting sind seit Jahren die dominierenden Schwachstellen", sagte Walter Karl von der *IBM X-Force*. Schon während der Entwicklung müssen Programme auf Fehlerhaftigkeit überprüft werden (White Box Testing). Die Fehlerbehebung wird mit jedem weiteren Stadium der Entwicklung immer teurer, und am teuersten dann, wenn das Produkt bereits auf dem Markt ist. Geeignete Programme können Hilfestellung für das Aufdecken von Schwachstellen bieten.

FOTOS: KURT HICKISCH

Cyber-Security-Challenge: Innenministerin Johanna Mikl-Leitner mit dem Schweizer Siegerteam.

Die aktuelle Bedrohungslage schilderte Marco Preuss von *Kaspersky Labs*. Bisher noch unentdeckte Schwachstellen in Programmen, gegen die noch keine Patches entwickelt wurden (Zero-day-exploits), erzielen unter kriminellen Interessenten, je nach Programm, Marktpreise zwischen 5.000 und 250.000 $. Soziale Netzwerke werden für Angriffe eingesetzt. Ein unbedachter Klick auf einen noch so harmlos aussehenden Link kann den Rechner mit einem Schadprogramm infizieren.

Live-Demos. Es ist möglich, auf Daten zuzugreifen, auch wenn die Festplatte eines Laptops verschlüsselt und das Gerät abgeschaltet ist. Das demonstrierte Gunnar Porada, Geschäftsführer des Schweizer Unternehmens *Innosec*. Das Mittel dazu ist die Cold-Boot-Attack, die darauf beruht, dass die Speicherinhalte der Prozessoren eines Rechners nach dem Abschalten des Stroms nicht sofort erlöschen, sondern eher dahinschwinden („faden"). Dieser Prozess kann durch Kühlung, etwa mit einem Kältespray, hinausgezögert werden. Dazu kommt, dass beim Hochfahren des Laptops der Schlüssel zur Entschlüsselung mit hochgeladen wird. Die Frage ist nur, auf welchen Speicherplatz er abgelegt wird und wie man ihn von dort auslesen kann. Dazu gibt es für Hacker Programme, die als „Forensic Tools" angeboten werden. Der Laptop wird hochgefahren, bis die Eingabe des Passwortes für den Entschlüsselungsvorgang verlangt wird. Die Prozessoren werden vereist und mit Hilfe der Tools wird das Passwort ausgelesen.

Der Schutz kritischer Infrastruktur kann auf eine gemeinsame Basis zurückgeführt werden, nämlich die Sicherheit der Stromversorgung. Bricht diese zusammen, geraten auch die übrigen Strukturen ins Wanken. Im Buch „Blackout" werden die sich als Folge eines Stromausfalls ergebenden Szenarien romanhaft geschildert. In Anwesenheit des Autors Marc Elsberg simulierte Cyrill Brunschwiler, Compass Security, Schweiz, einen Hacker-Angriff auf eine über ein Smart Grid laufende Stromversorgung, bei der die Daten der Messeinrichtung über Funk verschlüsselt übermittelt werden. Der – ebenso drahtlos erfolgte – Angriff gelang. Die Kaffeemaschine, die die außer Betrieb gesetzte Tankstelle simulieren musste, konnte durch die Übertragung von Steuerungsbefehlen abgeschaltet werden. Bei der Tankstelle hätte nicht einmal mehr für Einsatzfahrzeuge oder für Aggregate zur Notstromversorgung nachgetankt werden können.

LH-Stellvertreter Franz Hiesl.

Gunnar Porada, Innosec.

Gegenstrategien. Mit dem Auftrag, kritische Infrastruktur zu schützen, ist seit 2004 in der Schweiz die *Melde- und Analysestelle Informationssicherung MELANI (www.melani.admin.ch)* operativ tätig. Deren stellvertretender Leiter Max Klaus wies auf die Unerlässlichkeit der Mitarbeit der Wirt-

FOTOS: KURT HICKISCH

Cyber-Security-Challenge: Innenministerin Johanna Mikl-Leitner und Mitglieder des österreichischen Teams.

schaft im Sinne einer Public Private Partnership (PPP) hin. *MELANI* betreibt das Eidgenössische Lagezentrum zum Schutz kritischer Infrastrukturen und unterstützt die Betreiber solcher Einrichtungen durch Weitergabe von Informationen.

Besonderes Augenmerk gilt der Bekämpfung von Botnetzen, die fast allen kriminellen Aktivitäten im Internet zu Grunde liegen. Bei Phishing-Attacken werden Server, von denen diese Angriffe ausgehen, blockiert und Banken verständigt. Gezeigt wurden Beispiele, wie über Annoncen mit der Aussicht auf schnellen Gewinn Finanzagenten angeworben werden, die die betrügerisch herausgelockten Gelder reinwaschen sollen. Die von *MELANI* getroffenen Maßnahmen zur Cyber-Resilienz (Prävention, Reaktion, Kontinuität und Unterstützung) haben mittlerweile dazu geführt, dass die Schweiz zunehmend nicht mehr im Blickpunkt von Cyber-Kriminellen ist.

ObstdG Mag. Walter J. Unger, Leiter der Abteilung Cyber Defense des Abwehramts, verglich das Leben im Cyber-Raum mit dem in einem Haifischbecken. „Der Cyber-Raum ist Spielwiese, Aktionsraum, Tatort und Gefechtsfeld/Kriegsgebiet. In ihm treiben sich Script-Kiddies, Aktivisten, Anarchisten, Kriminelle, Spione, Terroristen und Warriors herum." Die Unterscheidung liegt in Motivation, Zielsetzung, zur Verfügung stehenden Ressourcen und Fähigkeiten. Pro Tag werden nach Feststellungen des BSI etwa ein Dutzend bisher noch unbekannte Schwachstellen in Programmen entdeckt. Dem steht gegenüber, dass etwa 40 Prozent der Nutzer in Österreich nicht einmal Patches für bekannte Schwachstellen einspielen und ihre Rechner damit leicht als Teile eines Botnetzes übernommen werden können. Aktuell sind etwa 1.150 solcher Netze bekannt, doch gestaltet sich die Bekämpfung, die internationale Kooperation erfordern würde, schwierig.

Cyber-Sicherheit ergibt sich aus dem Zusammenwirken von Cyber-Verteidigung (Bundesheer), der Cyber-Kriminalitätsbekämpfung (BMI, Strafverfolgungsbehörden), dem privaten Sektor und der Cyber-Diplomatie, und wird vom Bundeskanzleramt koordiniert. Der einzelne User kann seinen Teil dadurch beitragen, dass er eine Firewall und Anti-Viren-Programme installiert, diese Programme regelmäßig updatet, für das Internet ein Zweitgerät verwendet, nicht mit der Administrator-Berechtigung im Internet auftritt, die Finger von dubiosen Programmen lässt, Mails von Unbekannten löscht und nur bei seriösen Anbietern über das Internet einkauft.

Cyber-Security-Challenge 2013. Im Rahmen der IKT-Sicherheitskonferenz wurden die Finalentscheidungen der Cyber-Security-Challenge 2013 ausgetragen, erstmalig zwischen einem Team aus Österreich und einem aus der Schweiz, und aufgeteilt in die Kategorien Schüler und Studenten. Der Grundgedanke des nach 2012 zum zweiten Mal ausgetragenen Wettbewerbs ist, jungen IT-Talenten die Möglichkeit zu bieten, sich auf legale Weise in ihrer Altersklasse mit in gleicher Weise Befähigten beim Aufdecken von Schwachstellen in der IT-Sicherheit zu messen. In weiterer Folge sollen ihre Fähigkeiten und Stärken gefördert und Nachwuchskompetenzen herangebildet werden.

Dem Bewerb lag in Österreich eine Initiative *(www.verbotengut.at)* des Vereins *Cyber-Security Austria (CSA)* in Kooperation mit dem Abwehramt zu Grunde. In der Schweiz übernahm der Verein „Swiss Cyber-Storm" im Patronat von *MELANI* und *Swiss Police ICT* die Organisation.

392 Bewerber aus Österreich hatten sich seit 17. Juli 2013 dem Auswahlverfahren in einem „Hacking Lab", einem IT-Sicherheitslabor, gestellt. 378 Lösungen wurden erarbeitet. Aus den daraus hervorgegangenen Finalisten wurden am 4. November die nationalen Sieger, jeweils fünf Schüler und fünf Studenten, ermittelt. Bei der Endausscheidung versuchten beide Teams mehr als elf Stunden lang Codes zu entschlüsseln, Sicherheitslücken zu finden und mögliche Zugänge zu Mobiltelefonen und Tablets zu finden. Schließlich siegte das Team der Schweiz knapp vor dem österreichischen Team.

Bei der Siegerehrung am 7. November 2013 im Rahmen des Führungskräfteseminars 2013 des Bundesheeres im Heeresgeschichtlichen Museum in Wien würdigte Innenministerin Mag.ª Johanna Mikl-Leitner die Leistungen der Teilnehmer und hob die gute Zusammenarbeit zwischen dem BMI und dem BMLVS hervor. Die Innenministerin überreichte mit dem stellvertretenden Generalstabschef, GenLt Mag. Bernhard Bair, Paul Karrer, Obmann von CSA, und Dr. Bernhard Tellenbach, Präsident Swiss Cyber Storm, die Preise.

Anmeldungen für die „European Cyber-Security-Challenge" 2014 sind unter *www.verbotengut.at* und *www.verbotengut.ch* möglich. Zudem wird 2014 erstmals auch Deutschland mit einem Team vertreten sein.

Die IKT-Sicherheitskonferenz 2014 wird am 4. und 5. November 2014 in Fürstenfeld stattfinden; der Abschlussevent mit Siegerehrung am 6. November 2014 im Heeresgeschichtlichen Museum in Wien. *Kurt Hickisch*

FOTO: KURT HICKISCH