Sicherheit im elektronischen Universum

Neue Bedrohungspotenziale brauchen effektive Gegenstrategien und eine gemeinsame gesellschaftliche Anstrengung*

DI Helmut Leopold
AIT Austrian Institute of Technology GmbH,
Head of Digital Safety & Security Department

* Schriftliche Fassung des Vortrags im Rahmen des Workshops „Industrie 4.0“ im Palais Epstein, Wien, am 24.6.2015.

Durch die rasante Digitalisierung der Wirtschaft und auch aller Lebensbereiche haben sich unser Kommunikationsverhalten aber auch unsere Verhaltensweisen grundlegend verändert. Die Bewältigung vieler großer gesellschaftlicher Herausforderungen der nahen Zukunft ist heute entscheidend von IT-Innovationen abhängig: smarte Energieproduktion und -verteilung sowie sparsamer Verbrauch (smart grid), intelligente und auch autonome Verkehrssysteme, moderne Gesundheitsdienste (eHealth, Telemedizin und Betreuung im Alter), zeitgemäße Bürgerservices und neue Kommunikationsprozesse zwischen BürgerInnen und Behörden (eGovernment), modernes Umweltmanagement (eEnvironment), öffentliche Sicherheit, der Betrieb industrieller Fertigungsanlagen (Industrie 4.0), oder auch unser alltägliches Leben (eLife). Informations- und Kommunikationstechnologien (IKT) sind damit längst unsere zentrale Lebensader geworden und bilden für sich eine kritische Infrastruktur mit überragender Bedeutung für die Aufrechterhaltung zentraler gesellschaftlicher Funktionen.

Diese umfassende Vernetzung von physischen mit IT-Systemen wird durch das Schlagwort „Cyber Physical Systems (CPS)“ beschrieben. Begriffe wie „Machine-2-Machine (M2M) Kommunikation“ und „Internet of Things (IoT)“ charakterisieren die besonderen Systemeigenschaften, welche durch eine große Anzahl von Sensoren, Datenaustauschprozessen und Kommunikationsverbindungen gekennzeichnet sind.

Mit unserer enormen Abhängigkeit von elektronischen Technologien quer durch Unternehmen aller Größenordnungen in sämtlichen Wirtschaftsbranchen sowie bei Behörden und auch im persönlichen Umfeld, sind wir als Gesellschaft in Summe extrem anfällig gegen unterschiedlichste Bedrohungen aus dem Cyberspace geworden. Heute können wir unsere gesamten Kommunikations-, Produktions- und Entscheidungsprozesse nur im gewohnten Maß aufrechterhalten, wenn die IKT Infrastrukturen zuverlässig zur Verfügung stehen und gegenüber Ausfällen und Bedrohungen widerstandsfähig konzipiert sind. Die besondere Brisanz der Thematik liegt darin, dass durch die umfassende Vernetzung bzw. Digitalisierung eine unzureichende IT-Sicherheit nicht nur einzelne Unternehmenssysteme bedroht, sondern unsere positive gesellschaftliche Entwicklung insgesamt.

Wir müssen heute eine beunruhigende Professionalisierung als auch ein steigendes Ausmaß von Cyber-Angriffen attestieren, welches dazu führt, dass bislang bewährte Ansätze zum Schutz unserer kritischen IT-Infrastrukturen heute nicht mehr ausreichen. Die Sicherheitsanforderungen für den Schutz elektronischer Systeme können vor dem Hintergrund vielfältiger Motivationslagen der Angreifer und zunehmend ausgefeilter und komplexer werdender Angriffsmethoden nicht mehr mit einfachen technischen Ansätzen erfüllt werden. Sie bedürfen einer holistischen Betrachtungsweise, die technische Werkzeuge mit Prozessen, Organisationsstrukturen und Verhaltensmaßnahmen in Einklang bringt.

Vielschichtige Motivationslagen für Cyber-Attacken und enormer Anstieg der Angriffe

Der kriminellen Energie sind im Cyberspace so gut wie keine Grenzen gesetzt. Eine Vielzahl aktueller Beispiele belegt, dass durch Betriebsspionage, mit der neueste Forschungsergebnisse, geheime Produktionsdaten von Unternehmen oder auch Ausschreibungsinformationen ausgespäht werden, und durch Betriebssabotage, wo durch Manipulation von IT-Systemen Produktionsanlagen gestört werden, beträchtliche wirtschaftliche Schäden entstehen.

Der Diebstahl von persönlichen Informationen zum Zwecke der Erpressung wie z.B. von Promi-Fotos aus der Apple iCloud[1] und jüngst von Daten des Dating-Portals Ashley Madison[2] oder auch der Einsatz

[1] spiegel.de/panorama/leute/erin-heatherton-winona-ryder-opfer-von-promi-hacking-a-995475.html.

[2] itgovernance.co.uk/blog/weak-credentials-ultimately-led-to-ashley-madison-hack/.

von Schadsoftware, um die Verwendbarkeit persönlicher IT-Systeme nur gegen Bezahlung wieder zu erlauben (sog. Cryptolocker")[3] zeigen wie verletzlich verbundene Systeme letztlich sind.

Darüber hinaus ist auch der Missbrauch des Internets für politische und terroristische Zwecke eine sehr aktuelle Problematik. Sony wurde angegriffen um durch Erpressung die Ausstrahlung eines Spielfilms zu verhindern[4]. Propagandamaßnahmen wie z.B. die Anwerbung europäischer Jugendlicher für den Islamischen Staat (ISIS) über Plattformen wie „Cyber Caliphate“[5] zeigen die Gefahren auf, die im Netz noch schwerwiegende gesamtgesellschaftliche Auswirkungen haben können. Wenn dann noch ganze Nationen das Netz als Ersatz-Kriegsschauplatz benutzen, werden unsere IT-Systeme zum beliebten Angriffsziel um gesellschaftliche Funktionalität entsprechend zu beeinträchtigten.

Eine quantitative Betrachtung von Cyberattacken zeigt auch die enorme Zunahme von Angriffsversuchen. Der britische Regulator Ofcom registrierte in nur 2 Monaten im Jahr 2014 1.658 Cyber-Attacken[6]; in Österreich wurden 2014 vom CERT (Computer Emergency Response Team) 16.000 Fälle mit Sicherheitsrisiko erfasst[7]; ein Virenscanner muss heute an die 400.000.000 verschiedenen Typen von Schadsoftware erkennen[8]. Die starke Zunahme dieser Aktivitäten ist allerdings erst in den letzten 8 Jahren in diesem massiven Ausmaß erfolgt und zeigt damit eine neue Dynamik, mit der wir erst lernen müssen umzugehen.

Diametraler Gegensatz zwischen Systemkomplexität und Systemverständnis

Unsere umfassende Vernetzung der Systeme, wodurch wir sogenannte „Systems of Systems“ erhalten, führt zu einer grundlegenden Steigerung der Systemkomplexität. Damit verbunden ist ein stetig sinkendes Systemverständnis durch einzelne ExpertInnen. Die Abhängigkeit einzelner Systemteile untereinander hat eine neue Dimension erreicht. Die mit den Cyber Physical Systems entstehende Komplexität und die Abhängigkeit der Systemkomponenten untereinander, führen bei Fehlfunktionen und Störungen leichter zu Kettenreaktionen mit wesentlich größeren Konsequenzen.

Gleichzeitig dazu nimmt aber auch das versierte Technologie Know-how auf Seite der Angreifer zu, was ihnen die Möglichkeit gibt, immer raffiniertere Angriffsszenarien aufzusetzen. Sogenannte „Advanced Persistent Threats“ (APTs) sind eine Dimension der Cyber-Bedrohung die wir zu berücksichtigen haben. Dabei werden verschiedene Angriffsmethoden miteinander kombiniert, wie z.B. Social Engineering zum Sammeln von persönlichen Informationen und der Einsatz von Phishing-Software zum Identifizieren von persönlichen Sicherheitsinformationen wie z.B. Login-Daten und Passwörtern. Dadurch kann Schadsoftware auf IT Systemen geschickt so platziert werden, dass diese oft lange unentdeckt bleibt. Eingeschleuste Schadsoftware kann nun das IT System „von innen“ beobachten und neue Schwachstellen identifizieren, um schlussendlich gezielte und unbemerkte Angriffe durchzuführen.

---

3 en.wikipedia.org/wiki/CryptoLocker.

4 en.wikipedia.org/wiki/Sony_Pictures_Entertainment_hack.

5 Newsweek 7.8.2015, page 19, Beauty queen and vigilante female hackers declare online war on Isis.

6 itgovernance.co.uk/blog/ofcom-faces-more-than-1600-cyber-attacks-in-just-two-months/.

7 cert.at/static/downloads/reports/cert.at-jahresbericht-2014.pdf.

8 av-test.org/de/statistiken/malware/; trendmicro.de/media/ds/anti-malware-nss-labs-datasheet-de.pdf.

Cyber Security ist eine gemeinsame Aufgabe der Gesellschaft

Herkömmliche Schutzmechanismen sind heute diesen komplexen neuen Angriffsmethoden nicht mehr gewachsen. Die Security-Industrie hat schon seit einiger Zeit erkannt, dass allgemein übliche Methoden wie z.B. Firewalls und Virenschutz, die nur einem „Zutrittsschutz" entsprechen, nicht mehr ausreichen, um moderne Angriffe abzuwehren.

Daher müssen wir jetzt in kollektiver gesellschaftlicher Anstrengung von Netzbetreibern, Service-Anbietern, Herstellern von IT-Equipment, Systemintegratoren, der IT-Security-Forschung sowie von politischen Verantwortungsträgern neue Werkzeuge und Methoden sowie Maßnahmen entwickeln. Darüber hinaus haben wir ein noch wenig ausgeprägtes Bewusstsein über diese Problematik in der Bevölkerung, aber auch bei Unternehmensvertretern zu attestieren. Viele technische Entwicklungen werden ohne ausreichende Berücksichtigung der Cyber Security Problematik durchgeführt. Grund dafür ist einerseits ein unzureichendes Verständnis im Management von Unternehmen und andererseits der wesentliche Kulturunterschied zwischen IT-ExpertInnen, die mit dieser Problematik schon seit Jahren konfrontiert sind, und anderen Industrie-Technikern, für die dies ein neues Phänomen ist (Stichwort „Safety – Security" Problematik).

Wir müssen in der Wirtschaft die vielfach noch bestehenden kulturellen Unterschiede in Bezug auf Systemzuverlässigkeit (Safety) und IT-Sicherheit ausräumen und zu einem konsolidierten Verständnis von Safety und Security beitragen. Ein Techniker, der sein System auf hohe Verfügbarkeit und Zuverlässigkeit abstimmt („Safety") nimmt die Wichtigkeit von „sicheren Systemen gegen Angriffe" anders war. Zudem widersprechen sich die Systemanforderungen dieser zwei Bereiche oft.

Kernelemente eines modernen, zukunftssicheren Schutzkonzeptes umfassen somit:

i. Steigerung des Bewusstseins über die Problematik in der breiten Bevölkerung aber auch im Management vieler Unternehmen.
ii. Risikomanagement, Evaluierung des Bedrohungspotenzials sowie die Identifizierung möglicher Angriffsziele, um den Umfang und den Fokus der Schutzmaßnahmen festzulegen.
iii. Festlegung von strukturellen Maßnahmen – Organisationsstrukturen und Prozesse, um Sicherheitsmaßnahmen zu implementieren.
iv. Neue Methoden und Werkzeuge, um unbekannte Angriffe zu identifizieren – z.B. durch Anomalieerkennung über CAIS Cyber Attack Information Systeme[9]; und
v. ein frühzeitiger und effektiver Informationsaustausch für eine Analyse als auch eine potentielle Vorwarnung anderer Stakeholder des Systems über CIIS Cyber Incident Information Systeme.

IT-Sicherheit darf nicht zum „Show-Stopper" der Wettbewerbsfähigkeit unseres Wirtschaftsstandortes und unserer positiven gesellschaftlichen Entwicklung werden

Für die Anforderungen einer zeitgemäßen Cyber Security müssen wir ein öffentliches Bewusstsein auf breiter Basis schaffen. Das Erlernen der digitalen Kulturtechnik und damit die Sensibilisierung für Ge-

[9] H. Leopold, Th. Bleier, F. Skopik, *Cyber Attack Information System - Erfahrungen und Erkenntnisse aus der IKT-Sicherheitsforschung*, Springer Verlag, 2014.

fahren aus dem Netz müssen in Schullehrpläne Einzug halten und fixer Bestandteil in der Erwachsenenbildung werden.

Weiters ist die Ausbildung von fundiertem Fachwissen im IT-Sicherheitsbereich auf universitärer Ebene in gleichem Maße wichtig wie umfassende Forschungsaktivitäten, um entsprechende Technologiekompetenzen am Wirtschaftsstandort Österreich zu etablieren. Nur mit einem Reservoir an akademischen und industriellen Fachkräften, gekoppelt mit verfügbaren Technologien durch potente Unternehmen am Wirtschaftsstandort, werden wir auch neue IT-getriebene Wirtschaftsbereiche am globalen Markt erfolgreich positionieren können. Für diese Expertisenbündelung am Wirtschaftsstandort Österreich braucht es die Kooperation aller relevanten Akteure, um eine kritische Masse an Kompetenz bei IT-Security zu realisieren. IT-Security und der Schutz kritischer Infrastrukturen sind somit eine gesellschaftliche Anstrengung, welche durch die Politik, die Industrie sowie Forschung und Entwicklung zusammen vorangetrieben werden muss.