Sicherheit im Web

Die rasant steigende Verwendung informationstechnischer Bauteile vergrößert die Verwundbarkeit der IT-Systeme. Zu dieser Auffassung kamen IT-Experten bei der IT-Defense 2016 in Mainz.

Die organisierte Cyber-Kriminalität hat bisher über industrielle Steuerungssysteme (Industrial Control Systems – ICS) wie etwa *SCADA* auf Transport- und Herstellungsprozesse zugegriffen", berichtete Eugene Kaspersky bei der IT-Defense 2016, die am 28. und 29. Jänner 2015 in Mainz stattfand. Um kriminellen Gewinn zu erzielen, wurde beispielsweise in die Steuerungsprozesse von Verladeeinrichtungen für Getreide eingegriffen, wurden die Liefermengen von Kohlebergwerken manipuliert oder wurden Treibstoffe abgezweigt. Derartige Dienste können auch gekauft werden – „Crime as a Service" (CaaS).

Die nächsten Angriffe könnten auf kritische Infrastruktur erfolgen, wobei die Frage nicht sei, ob sie stattfinden, sondern wann, wo und wie schwerwiegend. Für Kriminelle könnte die Motivation darin liegen, Geld zu erpressen. Hacktivisten könnten versuchen, politische Ziele durchzusetzen. Für Terroristen wären solche Angriffe, etwa auf Krankenhäuser oder Versorgungseinrichtungen, ein Mittel, Angst und Schrecken zu verbreiten. Letztlich käme ein Einsatz zu militärischen Zwecken in Betracht, „allerdings nur einmal", wie Kaspersky betonte. Entweder ist der Gegner zu Fall gebracht oder macht alle seine Systeme gegen einen derartigen Angriff in der Folge immun.

Kritische Infrastruktur kann über Systeme wie SCADA angegriffen werden oder durch Angriffe auf die Telekommunikation, im Speziellen das Internet. Dessen Ausfall hätte weitreichende Folgen auf die Energieversorgung, das Transport- und Finanzwesen, die Wasserversorgung bis zu den Telematiksystemen und Smart-Houses. Präventive Maßnahmen hätten bereits auf der Ebene der Gesetzgebung zu erfolgen, die für entsprechende Resilienz zu sorgen hätte. Staaten, die dies durchgesetzt hätten, wären laut Kaspersky Israel und Singapur.

Kritische Struktur müsste untersucht und Netzwerke abgesichert werden. In der Informatik müsste die Ausbildung von IT-Sicherheitsingenieuren forciert werden, von denen es weltweit zu wenige gebe. Eine Whitelisting-Policy müsste betrieben werden, also nur auf Vertrauenswürdigkeit geprüfte Programme einzusetzen bzw. nur mit solcherart geprüften Partnern in Verbindung zu treten. Der unvorsichtige Umgang mit Datenträgern müsste unterbunden werden. Als letzte, wenn auch teuerste Möglichkeit, würde sich anbieten, für industrielle Systeme überhaupt neue Betriebssysteme zu entwickeln.

Verwundbarkeiten. „In einem durchschnittlichen Auto befinden sich mehr als 100 Electronic Control Units, die miteinander in Echtzeit kommunizieren müssen", sagte Stephan Gerhager, *CISO* eines großen Versicherungsunternehmens. Diese Kleincomputer sind eher auf funktionale Betriebssicherheit (Safety) ausgelegt als auf IT-Sicherheit (Security). Die Schwächen zeigen sich dann, wenn die einzelnen Systeme zu einem Netzwerk verbunden werden. Das am meisten eingesetzte Bussystem *(CAN-Bus)* geht in seinen Ursprüngen auf das Jahr 1986 zurück. In diesem System kann jeder mitlesen, jeder empfängt alles. Eine Authentifizierung findet nicht statt, sodass die Kommunikation der Systeme untereinander ausgelesen und manipuliert werden kann. Entsprechende Tools dazu gibt es. Durch Manipulation der Einparkhilfe könnte sogar die Steuerung des Fahrzeugs übernommen oder in diese eingegriffen werden.

Das Eindringen in das Fahrzeug kann physisch oder durch elektronische Angriffe auf die Außenhaut erfolgen. Angriffspunkte sind dabei jene Funktionen, die mit der Außenwelt in Verbindung stehen, wie der berührungslos sperrende Fahrzeugschlüssel oder eine funkbasierte Reifendruckkontrolle. Jedes zusätzliche Feature, das über Fernbedienung (oder über Handy-Apps) gesteuert werden kann, vergrößert die Angriffsfläche.

Letztlich kann ein Auto auch über Funktionen angegriffen werden, die mit dem Internet in Verbindung stehen. Wegen ihrer geringeren Leistungsfähigkeit fehlen Car-Browsern die meisten jener Sicherheitsmerkmale, wie sie in Standard-Browsern verwendet werden. Hackern sind derartige Browser sogar mehr vertraut als einzelne ECUs. „Wie oft werden wir unsere Autos in Zukunft patchen müssen?", fragte Gerhager. Es geht nicht nur um Diebstahl des Fahrzeugs oder dass es illegal getunt wird. Es könnten auch zielgerichtete Angriffe auf Personen durchgeführt oder die Herstellerfirmen erpresst werden.

Das Internet of Things (IoT) könnte sich zu einem Internet of Threats entwickeln, warnte John Matherly. Mit der von ihm entwickelten Suchmaschine *Shodan* können Geräte, die mit dem Internet verbunden sind, auf-

IT-DEFENSE

Expertentreffen

Seit 2003 veranstaltet die auf Informationssicherheit spezialisierte *cirosec GmbH* alljährlich gegen Ende Jänner/Anfang Februar an jeweils wechselnden Orten in Deutschland die IT-Defense als Treffen von IT-Sicherheitsexperten.

Die Teilnehmer – deren Zahl trotz der großen Nachfrage auf 200 beschränkt ist – kommen aus den Bereichen Polizei, Militär, Industrie und Verwaltung. Bei der jeweils zwei Tage dauernden Hauptveranstaltung wechseln in bunter Abfolge Vorträge rein technischen Inhalts, Berichte über Nutzanwendungen von Forschungsergebnissen und solchen, die IT-Sicherheitsprobleme eher unterhaltsam angehen, einander ab. Am jeweiligen Vortag finden Hacking-Trainings statt. Am vierten und letzten Tag werden in Round Tables Themen aus der Vortragsreihe vertieft behandelt.

www.cirosec.de;
www.it-defense.de

gespürt, analysiert und kartografiert werden. Die erfassbaren Anlagen reichen von Kraftwerken, Industriesteuerungen (ICS), Pumpen und Turbinen, Anlagen der Infrastruktur, Ampeln, Videokameras, Kennzeichenerfassungsgeräten, bis zu TV- und Haushaltsgeräten. Das in Entwicklung befindliche Internet-Protokoll IPv6 wird es ermöglichen, jedem von Menschen geschaffenen Ding eine eindeutige Internet-Adresse zuzuweisen.

Dass die Dinge zunehmend „smart" werden, vergrößert auch die Angriffsfläche. Der Kühlschrank könnte zum Spam-Versender werden; wie restartet man ihn? Braucht man, fragte Matherly, wirklich einen (smarten) Eierbehälter wie den Egg-Minder, bei dem über Internet abgefragt werden kann, wie viele Eier sich noch im Kühlschrank befinden? Für die Einhaltung der Grundrechte im Informationszeitalter setzt sich, als Nicht-Regierungsorganisation, die 1990 gegründete *Electronic Frontier Foundation* ein.

Geräte, die mit dem Internet der Dinge verbunden sind, können aufgespürt werden.

FOTO: FOTOLIA/MACROVECTOR

Schadprogramme können in einem einzelnen digitalen Bild versteckt sein und bei dessen Aufruf aktiv werden. Das Verfahren, geheime Botschaften in Bildern zu verbergen (Steganographie), ist an sich nicht neu. Neu hingegen ist die als Stegosploit bezeichnete Technik, die Saumil Shah vorstellte, nämlich ein ausführbares Schad-Programm so zu implementieren, das am Gesamteindruck des Bildes Veränderungen kaum merkbar sind. Er verlegt bei einem Schwarz-Weiß-Bild das Programm in die unterste der acht Bildstufen, somit in jene, die auf unterster Ebene (low significant) die Schattierung bestimmt, kaum aber die vornehmlich ins Auge springenden Konturen. Bei Farbbildern wird der Grün-Kanal verwendet. Das Programm wird auf Pixel aufgeteilt, von denen jeder acht Bits umfasst, die in einer bestimmten Ordnung angelegt sind. Beim Laden des Bildes wird der Code entschlüsselt und das Programm ausgeführt. Das Problem liegt beim Browser, wenn dieser das Laden von Java-Script gestattet.

Dr. Ing. Timo Kasper zeigte am Beispiel von berührungslosen Zutrittskontrollsystemen auf, dass auch vermeintlich sichere Systeme „Tage der offenen Tür(en)" ermöglichen. Die gezeigten technischen Angriffe (Seitenkanal-Attacken) erfordern zwar entsprechende Fachkenntnisse und qualifizierte technische Ausrüstung, zeigen aber, dass für die Industrie die Notwendigkeit besteht, laufend an Verbesserungen ihrer Produkte zu arbeiten.

Auch hochentwickelte mechanische Sperrsysteme können überwunden werden. In den letzten Jahren sind patentierte Schließzylinder auf den Markt gekommen, bei denen ein bewegliches Element im Schlüssel abgefragt wird. Bei einem bloßen Abformen eines derartigen Schlüssels bleibt die Beweglichkeit des Sperrelements nicht erhalten; der Schlüssel sperrt nicht bzw. kann von vornherein nicht in das Schloss eingeführt werden. Mit einer speziellen, von Alexandre Triffault vorgeführten Gießtechnik kann auch dieses Problem überwunden werden. Wie er berichtete, wird der 3D-Druck von Schlüsseln zunehmend präziser; Open-Source-Programme und einfach zu bedienende CAD-Software wurden für diese Technik entwickelt. Schlüssel sollten daher ähnlich sorgsam verwaltet werden wie Passwörter im IT-Bereich. Beide eröffnen Zugänge zu Bereichen, die anderen gegenüber verschlossen bleiben sollen.

Safe-Harbor. Beim Cloud-Computing wird IT-Infrastruktur wie Rechenkapazität, Datenspeicher, Software dem jeweiligen Bedarf entsprechend zur Verfügung gestellt; aus Nutzersicht fern und undurchsichtig, wie von einer „Wolke" verhüllt, sagte Rechtsanwalt Dr. Joerg Heidrich *(www.recht-im-internet.de)*. Das wirft Fragen des Vertragsrechtes auf, des Datenschutzes, der betrieblichen Mitbestimmung, der IT-Sicherheit und der Compliance




Referenten bei der IT-Defense: Timo Kasper, Eugen Kaspersky, John Matherly, Jörg Heidrich.

sowie der Lizenzprobleme und der Rechtswahl nach internationalem Recht.

Probleme ergeben sich dann, wenn eigene Daten in die Obhut von Dritten gegeben werden: Wo befinden sich die Daten geografisch, wie sind sie gesichert, wer hat Zugriff auf sie? Welche Kontrollmöglichkeiten bestehen gegenüber dem Anbieter; wird dieser auch auf lange Sicht zur Verfügung stehen; was passiert bei Insolvenz oder Ausfall; bestehen Zugriffsmöglichkeiten beispielsweise für die Steuerprüfung; welche Möglichkeiten bestehen zur Rechtsdurchsetzung? Die zu erwartenden Probleme sollten vertraglich möglichst genau gelöst werden.

Personenbezogene Daten. Bei der Weitergabe von personenbezogenen Daten an Dritte ergeben sich Rechtsfragen vor allem im Bereich des Datenschutzes, insbesondere bei einer Weitergabe in das EU-Ausland. Als Beispiele für personenbezogene Daten brachte Heidrich neben Name, Alter, Anschrift, auch Werturteile wie zum Beispiel Zeugnisse sowie Daten, über die sich mittelbar ein Personenbezug herstellen lässt, wie Kfz-Kennzeichen, Konto- oder Matrikelnummer. IP-Adressen fallen ebenfalls darunter. Personenbezogene Daten zu verschlüsseln, wird von den deutschen Datenschutzbehörden als nicht ausreichend angesehen. Hingegen fallen anonyme Statistiken, Lagerbestände, Verkaufs- oder Produktionsdaten, technische Zeichnungen nicht unter personenbezogene Daten.

Das Hauptproblem bei Big Data stellt dar, dass Daten nur zu dem Zweck verwendet werden dürfen, für den sie erhoben wurden. Ein bloßes „Nice-to-have“ reicht bei einer Interessenabwägung nicht aus.

Die Verwendung personenbezogener Daten ist entweder auf Grund einer gesetzlichen Erlaubnis oder bei Einwilligung des Betroffenen zulässig. Diese setzt allerdings den informierten User voraus, kann also rechtswirksam nicht auf bereits vorangekreuzte Formulare erteilt werden.

Bei der Verarbeitung von Daten in einer Cloud handelt es sich um eine Auftragsdatenverarbeitung nach § 11 BDSG bzw. Überlassung von Daten zur Erbringung von Dienstleistungen nach § 10 DSG 2000. Das bedeutet, dass den Auftraggeber die Verpflichtung trifft, nur einen Dienstleister zu beauftragen, der ausreichende Gewähr für eine rechtmäßige und sichere Datenverarbeitung bietet, dass die notwendigen Vereinbarungen hierzu getroffen werden und sich der Auftraggeber über die Einhaltung dieser Maßnahmen überzeugt. Die Vereinbarungen sind schriftlich festzuhalten (§ 11 Abs. 2 DSG).

Die Übermittlung und Überlassung von Daten an Empfänger in Vertragsstaaten des Europäischen Wirtschaftsraumes ist genehmigungsfrei (§ 12 Abs. 1 DSG). Genehmigungsfrei erfolgen die Übermittlung und Überlassung auch in Staaten, die ein angemessenes Datenschutzniveau aufweisen. Diese sind die Schweiz, Argentinien, Guernsey, Insel Man, Jersey, Färöer Inseln, Andorra, Uruguay und Neuseeland sowie Kanada und Israel (§ 1 Abs. 1 und 2 Datenschutzangemessenheits-Verordnung – DSAV, BGBl II 2013/150, zuletzt BGBl II 2015/449). Hinsichtlich der „Five-Eyes“-Staaten Australien, Canada, Neuseeland, UK und USA bezeichnete Heidrich diese Einstufung als inzwischen fragwürdig.

Keine „sicheren Drittländer“ sind die USA, China, Indien, Japan. Bisher hat für US-Unternehmen die Möglichkeit bestanden, sich gegenüber dem US-Handelsministerium durch freiwillige Erklärung zur Einhaltung bestimmter datenschutzrechtlicher Bestimmungen (Safe Harbor Principles) zu verpflichten und so zum „sicheren Hafen“ zu erklären. Auf der entsprechenden Liste des US-Handelsministeriums waren bis September 2015 etwa 5.500 amerikanische Unternehmen eingetragen, darunter auch IT-Marktführer.

Mit Urteil des Europäischen Gerichtshofs vom 6. Oktober 2015, Az C-362/14, wurde die Safe-Harbor-Entscheidung 2000/520/EG der Kommission, auf der die Safe-Harbor-Regelung beruht, für ungültig erklärt. Unter anderem hätten die Befugnisse der nationalen Kontrollstellen nicht beschränkt werden dürfen (Rn 103 des Urteils). Eine Datenübermittlung auf Grund des Safe-Harbor-Urteils ist somit nicht mehr zulässig. In Deutschland hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26. 10. 2015 ein Positionspapier verfasst *(www.datenschutz.hessen.de/ft-europa.htm#entry4521)*. Datenschutzbehörden in Deutschland werden nach der am 1. Februar 2016 abgelaufenen Stillhaltefrist auf Safe-Harbor gestützte Datenübermittlungen in die USA untersagen. Es wird sich, sagte Heidrich, aus Datenschutzsicht dringend empfehlen, einen Provider zu wählen, der garantiert, dass seine Daten auf Servern in Deutschland oder innerhalb der EU verbleiben.

Weitere Vorträge haben Web-Technologie, Spionage-Hardware und die Herangehensweise beim Erstellen von Statistiken behandelt.

Kurt Hickisch

Fotos: Kurt Hickisch