Neues aus der Cyber Akademie

Juli 2016

Themenseite in Kooperation mit:

CAk Cyber Akademie

IT-Sicherheit aus Expertensicht

(CAk/th) "Wir betreiben eine der weltgrößten Datenbanken", so Thomas Seifert, Vorstand Finanzen (CFO) bei der Symantec Corporation. Sein Unternehmen registriere weltweit 2.000 Cyber-Angriffe pro Sekunde. Die enorm große Datenbank ermögliche es, generelle Trends im Bereich Cyber-Sicherheit zu erkennen. Seifert sprach in seinem Vortrag von insgesamt fünf Trends.

Der erste sei, dass die zielgerichteten Angriffe im Jahr 2015 um 55 Prozent gestiegen seien. "Hier wird es dann sehr schnell persönlich", so *Seifert,* der sagte, dass Personen vor den Angriffen oftmals gezielt ausgespäht würden. Ein zweiter Trend sei die Zunahme sogenannter Zero-Day-Attacken. Hierbei würden unbekannte Sicherheitslücken ausgenutzt. In diesem Zusammenhang habe sich eine regelrechte Industrie entwickelt. Es sei möglich, Sicherheitslücken im Internet zu kaufen.

Als eine dritte Entwicklung hat der CFO eine neue Ausrichtung beim Thema Ransomware ausgemacht. "Die Attacken verlagern sich zunehmend vom Konsumenten auf die Unternehmen." Der vierte Trend seien verseuchte Webseiten, die verstärkt für Angriffe genutzt würden. Außerdem sei eine erhöhte Zahl an Cyber-Angriffen zu beobachten, die sehr hohe wirtschaftliche Schäden anrichten würden.

Trotz der spürbaren Professionalisierung der Angreifer steht für *Josip Benkovic* von der Paolo Alto Networks GmbH fest, dass gerade im Bereich des Basisschutzes zu wenig getan werde. "Stand heute ist es zu billig, erfolgreiche Angriffe zu starten", so *Benkovic,* der angab, dass 95 Prozent aller Angriffe ohne größeren Aufwand aufzuhalten seien. *Michael Kranawetter*, Head of Information Security und National Security Officer bei der Microsoft Deutschland GmbH, hält es für unerlässlich, dass sich Unternehmen in grundlegenden Dingen den Rat von Experten holen. "Beratung ist absolut notwendig", so *Kranawetter*. Des Weiteren sei Risikomanagement ein sehr wichtiges Thema.

"Der Cyber-Raum ist das Nervensystem der globalen Wirtschaft", sagte *Ulf Feger*, Chief Security Officer der Huawei Technologies Deutschland GmbH. Eine Herausforderung sei in diesem Zusammenhang die genaue Kontrolle der Zulieferer. "Lieferkettenmanagement verhindert Fälschungen", so *Feger.* Es sei darüber hinaus nötig, dass jeder einzelne Zulieferer hohe Sicherheitsanforderungen erfülle. Der Konzern macht sich dafür stark, internationale Sicherheitsstandards für Hard- und Softwarehersteller festzulegen und hat in diesem Zusammenhang bereits mehrere White Papers zum Thema IT-Security veröffentlicht.

"Das Internet of Things (IoT) ist das neue Big Data", sagte *Dr. Rolf Werner*, Vorsitzender der Geschäftsführung, Head of Central Europe bei der Fujitsu Solutions GmbH. Die neuen Technologien würden z. B. im Rahmen von Smart Home sämtliche Lebensbereiche betreffen. Dies gelte auch für die Sicherheit. "IoT betrifft das gesamte Portfolio für Informationssicherheit", so *Werner*, und die IT-Sicherheit müsse ins Zentrum der Industrie 4.0. Aufgrund der immer größeren Vernetzung steige auch die Gefahr von Cyber-Angriffen. *Werner* machte sich daher für eine "Ende-zu-Ende-Beratung" in der IT-Forensik stark, um Betroffenen nach einem erfolgten Angriff bis zur Abwehr kontinuierlich helfen zu können. Er vertrat die Auffassung, dass das Thema Sicherheit bei der Konzeption von IKT-Produkten inzwischen eine übergeordnete Rolle spiele. "Risikomanagement ist der globale Leitfaden des IoT."

Die Vertreter der IT-Anbieter beleuchteten das Thema IT-Sicherheit aus unterschiedlichsten Perspektiven. (v.l.n.r.): Thomas Seifert, Josip Benkovic, Michael Kranawetter, Dr. Rolf Werner und Uwe Feger. Fotos: CAk/Giessen

Führungskräfte diskutieren über Cyber-Sicherheit

(CAk/th) In seinem Impulsvortrag zum CIO-Talk machte sich Dr. Michael Wilhelm, CIO von Sachsen, für die Vereinheitlichung von IT-Standards auf Länderebene stark. "Es müssen Vereinheitlichungen her", so der Landes-CIO. Als Beispiel für diese These ging er auf das Thema E-Government ein, das in den Bundesländern unter verschiedenen Namen angeboten werde. In Sachsen beispielsweise ist das Angebot unter www.Amt24 zu erreichen.

Es sei im IT-Bereich erforderlich, dass "der Föderalismus neu definiert wird", da die Digitalisierung nicht an Landesgrenzen haltmache. Insgesamt stellte *Wilhelm* der öffentlichen Verwaltung ein positives Zeugnis aus. "Es wird Erhebliches geleistet", so der CIO.

In der anschließenden Podiumsdiskussion stand u. a. die Frage im Raum, auf welcher Ebene IT-Security bei den einzelnen Unternehmen angesiedelt sei. *Axel Petri* von der Deutschen Telekom AG nahm für sein Unternehmen in Anspruch, hier eine Vorreiterrolle einzunehmen. "Seit 2008 ist IT-Security direkt im Vorstand angesiedelt". Auch gebe es keinerlei Trennung zwischen der IT-Sicherheit und der physikalischen Sicherheit im Konzern.

BYOD: Bedrohungen müssen gesehen werden

Zum Thema Bring your own Device hatten die Diskussionsteilnehmer eine eindeutige Meinung. Es sei unerlässlich, dass die IT der Unternehmen die genutzten Endgeräte verwalte und Zugriff hierauf haben müsse. "Man muss die Bedrohungen sehen", so *Dr. Kim Nguyen*, Geschäftsführer der D-Trust GmbH. Des Weiteren sollten sich IT-Verantwortliche mit der Frage beschäftigen, in welchen Staaten sie ihre Daten speichern. "Location matters", sagte *Nguyen* mit Blick auf die NSA-Affäre. *Carsten Scholz*, Head of IT-Risk & IT-Security bei Allianz SE, ergänzte zum Thema BYOD, dass Android aufgrund großer Sicherheitslücken im Prinzip nicht nutzbar sei. Für IT-Verantwortliche sei es bisweilen schwierig, gegenüber dem Vorstand die passenden Argumente für die Erhöhung des IT-Sicherheitsniveaus zu finden. Der Grund hierfür liegt laut *Scholz* auf der Hand. "IT-Sicherheit ist nicht messbar." Vorstände würden grundsätzlich Zahlen sehen wollen.

Um ein möglichst hohes Sicherheitsniveau zu erreichen, ist es laut *Petri* erforderlich, dass IT-Sicherheit nicht als Kostenfaktor betrachtet werde. "IT-Sicherheit muss ein Standortfaktor werden", so der Sicherheitsexperte. Damit dies erreicht werden könne, sei Transparenz ein wichtiger Baustein. Dieser fehle aktuell besonders auf staatlicher Seite.

In der Podiumsdiskussion ging es unter anderem um Vorgaben zum Thema BYOD. Foto: CAk/Giessen

"Es ging immer darum, Produktivität zu erhöhen"

(CAk/th) "Der Mensch hat sich immer Dinge erschaffen, um sich das Leben zu erleichtern", so Dr. Michael Haag, Senior Vice President für den Bereich Research und Development bei der KUKA Roboter GmbH. In diesem Kontext seien auch die Entwicklungen der Industrie 4.0 zu betrachten.

Im Vergleich zu früheren industriellen Revolutionen gebe es aber Unterschiede. Diese lägen darin, dass die erwarteten Verbesserungen in der Produktion bereits vorausgesetzt, ohne dass dies erwiesen sei. "Es ging immer darum, Produktivität zu erhöhen", so *Haag*, der cyber-physische Systeme wie zum Beispiel lernende Roboter als Schlüsseltechnologie der Zukunft ausgemacht hat. Diese würden sich unter anderem dadurch auszeichnen, dass Maschinen inzwischen auch untereinander kommunizieren würden. *Haag* hält die aktuelle Entwicklung in der Industrie 4.0 für unumkehrbar. "Die Business-Modelle werden sich völlig verändern", so *Haag,* der davon überzeugt ist, dass künftig "Produktionsprozesse digital optimiert werden". Ein Unterschied zu Produktionen vor den Entwicklungen der Industrie 4.0 sei, dass der Grad der Automatisierung inzwischen frei gewählt werden könne, während es früher nur die Wahl zwischen null und 100 Prozent Automatisierung gegeben habe.

Die Herausforderungen der IT-Sicherheit im Bereich Industrie 4.0 standen im Zentrum des Vortrags von Dr. Michael Haag. Foto: CAk/Giessen

Smarte Produktionsstätten als Modell der Zukunft

Damit die Produktion im Rahmen der Industrie 4.0 funktioniere, sei der Faktor IT-Sicherheit maßgeblich entscheidend. "Smarte Produktionsstätten sind nur möglich, wenn wir die IT-Sicherheit in den Griff bekommen." Fabriken der Zukunft werden sich laut *Haag* dadurch auszeichnen, dass sie sehr flexibel gestaltet werden. "In Zukunft werden die Produktionszyklen kürzer sein als die Lebensdauer der Produktionsanlagen." *Haag* sieht in sensitiven Robotern die Verbindung zwischen der realen Welt und der Cyber-Welt.

Für viele Produktionsstätten stellt die IT-Sicherheit laut *Haag* eine große Schwierigkeit dar. "Never change a running system" gelte für sehr viele Industrieanlagen. Dies habe zur Folge, dass Änderungen sehr schwer möglich seien bzw. erst bei einem Ausfall kompletter Anlagen in Angriff genommen würden, daher sei u. a. eine Verschlüsselung der verwendeten Daten nicht immer möglich. "In der Produktion ticken die Uhren anders als in der IT-Welt."