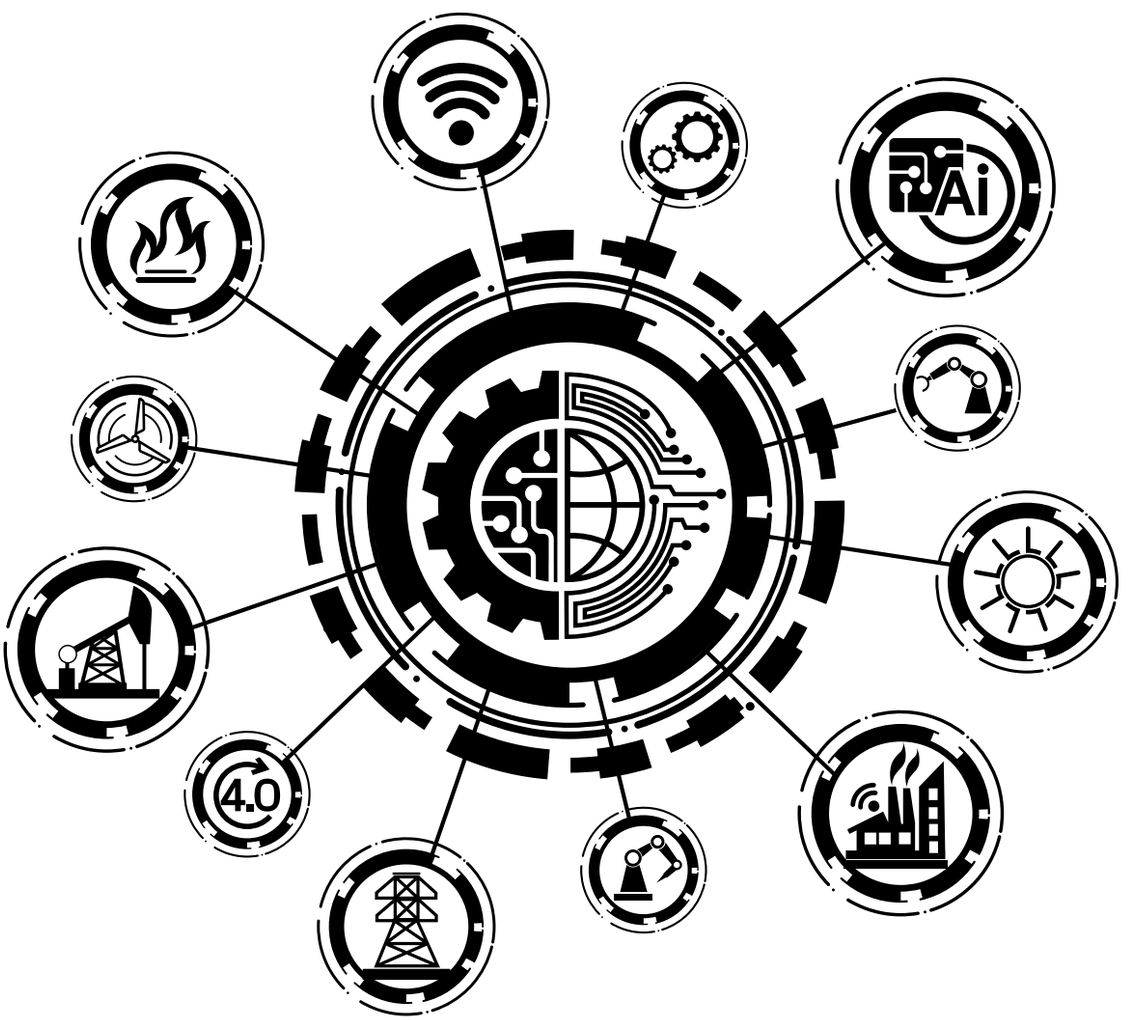
VON IDG

COMPUTERWOCHE

Ausgabe 2020 – 8-9 24. Februar 2020 Nur im Abonnement erhältlich

VOICE OF DIGITAL



Sicher ist: Nichts ist sicher

Crypto AG beschäftigt Sicherheitskonferenz.

Seite 6

Der optimale Service-Desk

Der Kauf eines ITSM-Tools ist nur ein Anfang.

Seite 32

Continuous Learning

Lernen ist eine Frage der Unternehmenskultur.

Seite 40

Erfolgsgeschichte Internet of Things

Die COMPUTERWOCHE hat den Markt analysiert und kommt zu erfreulichen Ergebnissen.

Seite 14

Kontinuierliches Lernen wird zur Schlüsselaufgabe

In vielen Unternehmen gelten Fortbildungen und Trainings als notwendiges Übel, die Mitarbeiter sollen arbeiten, nicht die Schulbank drücken. Diese Einstellung muss sich rasch ändern.

Heinrich Vaske, Editorial Director

Im vergangenen Jahr hat die COMPUTERWOCHE-Redaktion mit großem Enthusiasmus den Kongress „Lernen 21" ins Leben gerufen, im Herbst folgt Auflage 2 – wir freuen uns darauf! Warum ist uns das Thema wichtig (siehe auch Seite 40)? In den kommenden Jahren werden Unternehmen jede Menge neue Skills brauchen, wenn sie sich im digitalen Zeitalter behaupten wollen. Automatisierung und künstliche Intelligenz sind allgegenwärtig, zwischen Mensch und Maschine wird die Arbeit neu aufgeteilt.

Gesucht werden technisch qualifizierte Mitarbeiter mit ausreichenden Softskills – doch die gibt der Arbeitsmarkt nicht her. Die Situation wird sich weiter verschlechtern, weil Millionen Angehörige der Baby-Boomer-Generation in den Ruhestand gehen. Die Unternehmen müssen jetzt handeln, und zwar nicht, indem sie veraltete Trainings- und Lernkonzepte wieder hervorkramen, sondern indem sie kontinuierliches, toolgestütztes Lernen tief in ihrer Organisation verankern.

Dazu ist ein kultureller Wandel erforderlich, in dessen Folge die Beschäftigten ermutigt werden, sich weiterzuentwickeln – auch während der Arbeitszeit. Vorgesetzte sollten mit gutem Beispiel vorangehen, indem sie sich selbst weiterbilden und ihren Beschäftigten Anreize für aktives Lernen bieten. Hilfsmittel gibt es genug: Adaptives Lernen richtet die einzelnen Lerneinheiten individuell an den Fortschritten des Lernenden aus, Microlearning stellt Mitarbeitern kleine Lern- und Testfragen über elektronische Endgeräte bereit, Knowledge-on-Demand unterstützt Menschen im Kontext ihrer Arbeit, und Gamification bringt Spaß auch in dröge Materie. Mit Virtual und Augmented Reality dürften schon bald neue Verfahren in der Fläche verfügbar sein. Jetzt kommt es darauf an, was die Betriebe daraus machen.

Herzlich,
Ihr

Heinrich Vaske, Editorial Director

Lernen im 21. Jahrhundert:
Am 12. November 2020 findet im Airport Business Centre München der Kongress Lernen im 21. Jahrhundert statt. Mehr dazu unter lernen21.computerwoche.de/

Titelfoto: Pand P Studio/Shutterstock

Praxis

Job & Karriere

China wird gern als der Buhmann in Sachen Cyberspionage hingestellt. Der Skandal um die Crypto AG, die dem BND und der CIA gehörte, und mit deren Hilfe über 100 Staaten ausspioniert wurden, macht indes deutlich, dass auch die westlichen Nachrichtendienste wenig Skrupel kennen.

Skandal um Crypto AG überschattete Sicherheitskonferenz

Auf der Munich Cyber Security Conference (MCSC) herrschte Ratlosigkeit: Während neue Technologien wie 5G und IoT die Netze anfälliger machen, wächst die Dreistigkeit der Angreifer – auch die der staatlich sanktionierten.

Von Martin Bayer, Deputy Editorial Director

Wenn es um Cyber-Security geht, sind wir nur so gut geschützt wie das schwächste Glied“, sagte Margrethe Vestager, geschäftsführende Vizepräsidentin der EU-Kommission und Kommissarin für Digitales, anlässlich der Münchner Sicherheitskonferenz. Angesichts neuer Technologien rund um den Mobilfunkstandard 5G und das Internet of Things wächst demnach die Sorge um die Sicherheit. Zu groß ist die Abhängigkeit von funktionierenden, immer stärker vernetzten IT-Infrastrukturen. Das betrifft nicht nur die Unternehmen, deren Produktion und Lieferketten sowie Partner und Kundennetze digital verknüpft werden. Auch für die Gesellschaft kritische Infrastrukturen wie die medizinische Versorgung, Energienetze und Fahrzeuge hängen mehr und mehr von IT und Vernetzung ab.

Das bietet eine größere Angriffsfläche für Hacker und Cyber-Kriminelle. Im jüngsten Risikobarometer der Allianz stuften die befragten Manager Cyber-Bedrohungen erstmals als höchstes Unternehmensrisiko ein. Die zu erwartenden Schäden sind immens. Beispielsweise verursachen Angriffe via Social Engineering und Phishing-E-Mails immer höhere Schäden. Seit 2016 haben betrügerische Aufforderungen, Geld zu transferieren, die angeblich vom Management des beauftragenden Unternehmens stammen, weltweit Verluste in Höhe von rund 26 Milliarden Dollar verursacht.

Doch ein Patentrezept, dieser Probleme Herr zu werden, gibt es nicht. Das wurde auf der 6. Munich Cyber Security Conference (MCSC) am 13. Februar deutlich. Rainhard Ploss, CEO von Infineon Technologies, berichtete von einem Experiment. In einer Fake-Mail, angeblich vom Infineon-Management, wurden Mitarbei-

Foto: BeeBright/Shutterstock

die eigenen Infrastrukturen seien. Antworten auf die anstehenden Sicherheitsfragen blieben die Teilnehmer des MCSC indes schuldig. Alle Risiken zu eliminieren sei illusorisch, konstatierte Gurría. Es werde weitere Attacken geben. „Wir müssen lernen, damit umzugehen und die Risiken zu reduzieren."

Huawei – ja, nein, vielleicht?

Wie mit potenziellen Risiken umzugehen sei, wurde in München kontrovers diskutiert. Derzeit geht es unter anderem darum, welche Rolle der chinesische Netzausrüster Huawei beim Aufbau der 5G-Netze spielen soll. Die USA werfen dem Unternehmen vor, eng mit dem Staatsapparat und den Geheimdiensten zusammenzuarbeiten. Deshalb soll Huawei nach Ansicht der Amerikaner von der Auftragsvergabe ausgeschlossen werden – am besten weltweit.

Andere Staaten, darunter Großbritannien und Deutschland, wollen dagegen nicht auf die Technik aus dem Reich der Mitte verzichten. Hierzulande zweifelt man in Regierungskreisen offen an den Spionagevorwürfen der USA und den angeblichen Belegen für Hintertüren in Huawei-Geräten. In Berlin sprechen manche Politiker hinter vorgehaltener Hand von Propaganda und falschen Anschuldigungen. Andere stehen in dieser Angelegenheit auf der Seite der Trump-Administration. Der Vorsitzende des Ausschusses Digitale Agenda, Manuel Höferlin (FDP), teilt deren Skepsis. „Aufgrund der Erfahrung der vergangenen Jahre ist klar, dass chinesische Anbieter beim 5G-Ausbau keine vertrauenswürdigen und verlässlichen Partner sind, sondern ein unkalkulierbares Risiko für die IT-Sicherheit in Deutschland", sagte er jüngst der „Süddeutschen Zeitung".

Damit werden auch Debatten rund um die Frage der digitalen Souveränität neu befeuert. Gerade in Russland und China gibt es derzeit Abschottungstendenzen. Die russischen Machthaber wollen eine Art eigenes Internet im Land aufbauen, das sich auf Knopfdruck vom Rest des globalen Netzes abkoppeln lassen soll. In China hat das Regime die Devise ausgegeben, dass die eigene IT-Infrastruktur in einigen Jahren komplett auf einheimischen Produkten basieren soll – vom Chip bis zur Software. BSI-Präsident Arne Schönbohm hält nichts von solchen Diskussionen. „Digitale Souveränität haben wir nicht und hatten wir noch nie." Er verweist auf global vernetzte Lieferketten und die international arbeitende IT-Industrie. Markus Brändle, Chef der IT-Sicherheit bei Airbus, hält die Debatte sogar für naiv. Digitale Souveränität lasse sich nicht auf die Technik reduzieren. Das Thema sei komplexer und habe viele Aspekte. So gehe es auch um Infrastrukturen und Daten.

Der CISO hat es schwer

Für die Unternehmen wird es in dieser Gemengelage schwieriger, den Durchblick in Sachen IT-Security zu behalten. Zumal es den Sicherheitsverantwortlichen nach wie vor schwerfällt, mit ihren Anliegen durchzudringen. Shinichi Yokohama, CISO von NTT in Japan, berichtete, er habe fünf Monate gebraucht, um auf dem C-Level seines Unternehmen Gehör zu finden und eine Security-Agenda setzen zu können. Auch die Bereitschaft, für Sicherheit Geld in die Hand zu nehmen, ist nach wie vor gering. Claudia Eckert, Direktorin des Fraunhofer Instituts AISEC, beobachtet, dass viele Hersteller trotz Regularien die Integration von Sicherheitstechniken in ihre Produkte vernachlässigen. Der Grund: Deren Kunden seien nicht bereit, dafür höhere Preise zu zahlen. Aber auch innerhalb der eigenen Organisation seien Kosten für mehr Sicherheit in den eigenen Produkten schwer zu verargumentieren, berichtete Natalia Oropeza, CISO bei Siemens.

Teilweise macht sich schon ein gewisser Fatalismus breit. Infineon-Chef Ploss stellte die „Vertrauensfrage": Vertrauen habe man in Menschen, Regierungen oder Institutionen. Maschinen und das Internet müssten sich erst noch des Vertrauens würdig erweisen. „Ich habe aber keine Idee, wie das gehen soll", räumte der Manager offen ein.

Trau, schau, wem!

„Sicherheit braucht Vertrauen", hatte EU-Kommissar Schinas noch zu Beginn der Konferenz gefordert. Doch die Aufrufe, sich gegenseitig mehr zu vertrauen, wurden durch einen Skandal, der kurz vor der Münchner Sicherheitskonferenz ans Licht der Öffentlichkeit kam, zur Farce. Der deutsche Bundesnachrichtendienst BND und der US-Geheimdienst CIA haben über Jahrzehnte Hintertüren in Verschlüsselungstechnik der Crypto AG eingebaut und damit die Kommunikation in über 100 Staaten belauscht, die entsprechende Geräte eingekauft hatten. Beiden Diensten gehörte die Schweizer Firma. Doch die Eigentumsverhältnisse wurden über Treuhandgesellschaften verschleiert.

Angesichts solcher Nachrichten wird immer unklarer, wer im globalen Spiel der Mächte Freund oder Feind ist. Auch die Anschuldigungen der USA gegenüber China erscheinen in einem neuen Licht. Kaum jemand fragt hierzulande, ob Geräte von US-Ausrüstern manipuliert sein könnten. „Dabei wissen wir seit Snowdens Enthüllungen im Jahr 2013, dass die National Security Agency (NSA) in den USA über Jahre systematisch fremde Staaten und die eigenen Bürger ausspioniert hat", sagte Mitte Februar Security-Experte Bruce Schneier der „Neuen Züricher Zeitung" (NZZ), „unter anderem, indem Hintertürchen in die Verschlüsselungstechnologien der US-Sicherheitsfirma RSA eingebaut wurden." Schneier gibt sich keinen Illusionen hin. Wenn die chinesische Regierung eine Hintertür will, werde Huawei liefern. Genauso wie CIA und NSA schnell Hersteller fänden, die ihre Produkte gemäß den Anliegen der Nachrichtendienste manipulierten. Schneiers Bilanz ist ernüchternd: „Ja, wir leben im goldenen Zeitalter der Überwachung."