BEST PRACTICE

TELEKOM SECURITY
DROHNENSCHUTZ
LAUSCHABWEHR
IT-FORENSIK
QUANTUM COMPUTING
CHRO-TALK MAGNA
INNOVATION CENTER

Ausgabe 2/2017

T · · Systems ·

BEST PRACTICE 2/2017

T · · Systems ·

UNDERCOVER

DAS HEFT DES HANDELNS GEGEN CYBERKRIMINALITÄT

Foto: Deutsche Telekom

Reinhard Clemens,
Vorstand T-Systems
Deutsche Telekom AG
und CEO T-Systems.

Cyberkriminelle – Stakeholder, die keiner braucht.

DASS WIR ZU BEGINN DIESES JAHRES die operative Arbeit mit dem Geschäftsfeld Telekom Security aufgenommen haben, macht zwei Dinge deutlich: Wir als Unternehmen müssen in der Lage sein, uns an neue Entwicklungen schnell anzupassen. Und ohne das Thema Security mitzudenken, werden wir beim Kunden keine Aussicht auf Erfolg haben.

Denn darüber, dass das Internet der Dinge, Big Data, Cloud & Co. die Sicherheitsanforderungen von Unternehmen grundlegend verändern werden, hat sich wohl kaum jemand Illusionen gemacht. Darüber, wie man sich und sein Unternehmen wirksam schützen kann, aber offenbar schon. Welche Folgen das hat, zeigt der jüngste Sicherheitsreport des Instituts für Demoskopie Allensbach: Danach waren es Ende vergangenen Jahres nur noch sieben Prozent der mittleren und großen Unternehmen in Deutschland, die noch nie von einem IT-Angriff betroffen waren. Mehr als 40 Prozent der Unternehmen werden mehrmals wöchentlich oder gar täglich attackiert. Dadurch entstand deutschen Unternehmen 2016 ein Schaden von 51 Milliarden Euro.

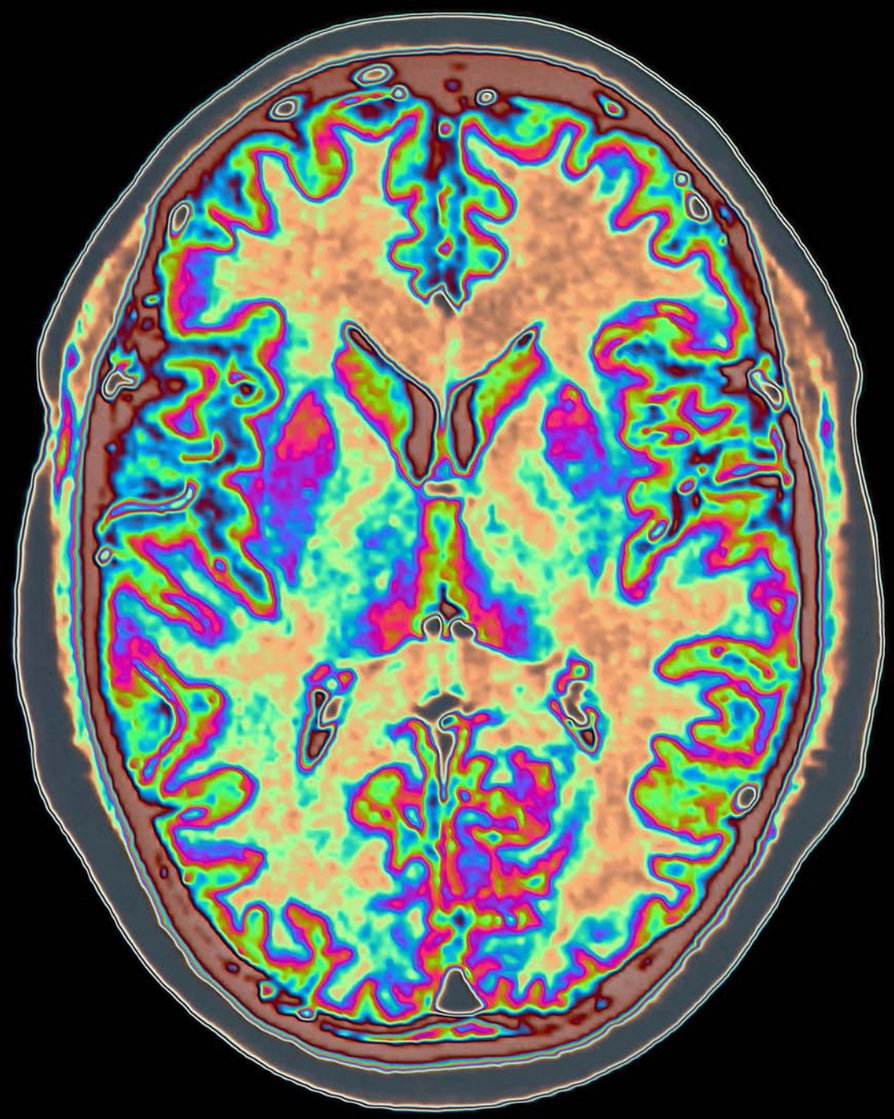
Leider gibt es gute Gründe anzunehmen, dass sich die Zahlen bis zur Veröffentlichung des nächsten Security-Reports ändern werden. Nur nicht zum Besseren. Denn die Beute, die sich Cyberkriminellen in Aussicht stellt, wird immer attraktiver. Denken wir nur an das autonome Fahren, den Gesundheitsmarkt oder an die intelligente Fabrik. Und an die dahinterliegenden Technologien wie Augmented Reality, künstliche Intelligenz, IoT, Analytics oder Quantum Computing – damit tun sich neue Forschungs- und innovative Geschäftsfelder auf, in die Unternehmen erst mal investieren müssen. Von Sachgütern über Intellectual Property bis zur Kreativität, Erfahrung und Expertise der Mitarbeiter. So werden allein die Security-Investitionen deutscher Unternehmen in diesem Jahr 8,5 Prozent höher ausfallen als 2016. Denn noch bevor sich Unternehmen auch berechtigte Hoffnung auf den ROI machen dürfen, hat ihr Engagement in neue Technologiefelder bei Wirtschaftsspionen längst was ganz anderes ausgelöst: reine Goldgräberstimmung. Suchen, schürfen, abschöpfen.

Wir wollen, dass diese Rechnung nicht aufgeht. Bei unseren Kunden nicht und bei uns selbst auch nicht. Mit der Bündelung der Kräfte aus allen Einheiten des Telekom-Konzerns im Geschäftsfeld Telekom Security können wir auf 1200 Experten zurückgreifen und werden damit vorrangig zwei Dinge erreichen, die uns besonders wichtig sind: unseren Kunden die zuverlässigsten und neuesten Security-Lösungen bereitzustellen, die bequem, unkompliziert und leicht zu bedienen sein müssen. Und das alles mit dem Ziel, dass Cyberattacken auf unsere Kunden und ihre Prozesse „Zero Impact“ haben.

Die zunehmende Vernetzung oder das Management von Sensoren, deren Zahl in Zukunft in die Milliarden gehen wird, sind nur zwei Beispiele für Angriffsvektoren, die sich in jedem Unternehmen auftun. Gleiches gilt auch für die nicht weniger riskanten Nischen einer Security-Architektur, die wir heute mit unseren Fachleuten und deren Services besetzen können. Von unseren erfahrenen IT-Forensikern über die Abwehr von Drohnenangriffen bis zu den BSI-zertifizierten Experten unseres Lauschabwehrteams, dem einzigen übrigens, das es bislang in Deutschland gibt. Das zeigt: Die Verknüpfung unseres Sicherheitsportfolios von Ende-zu-Ende, von skalierbaren Managed Security Services bis zu Speed-up-Einsätzen unserer Incident-Teams, ist der richtige Schritt.

Herzlichst Ihr

Reinhard Clemens



Der Rechner denkt.

Das Start-up Graphcore visualisiert die Lernprozesse von künstlichen Intelligenzen.

Wie sieht es aus, wenn künstliche Intelligenzen denken und lernen? Das britische KI-Chip-Start-up Graphcore hat diese Frage mit eindrucksvollen Bildern beantwortet. Die abgebildeten Cluster und Farben, die an menschliche Hirnscans (links) erinnern, zeigen die Kommunikations- und Lernprozesse künstlicher neuronaler Netze, während diese versuchen, in der Intelligence Processing Unit den Inhalt von Bildern zu klassifizieren. Schon jetzt sind die Leistungen solcher Systeme bemerkenswert, und die Komplexität steigt stetig, wodurch sie Probleme immer effizienter, abstrahierter und kreativer lösen können.

Lifestyle-Avantgarde.

Die Berliner Modeblogger Dandy Diary erobern neue Geschäftsmodelle.

Sie sind wild, provokant, erfolgreich und machen mit Dandy Diary den einflussreichsten Männermodeblog Deutschlands. Carl Jakob Haupt (l.) und David Kurt Karl Roth bewegen sich zwischen Kommerz und Kunst, kooperieren mit internationalen Marken und legen sich gerne auch mal mit der eigenen Branche an. Sie haben im Modezirkus erreicht, was man erreichen kann. Was also anstellen mit Reichweite und Aufmerksamkeit? Neue Geschäftsmodelle entwickeln! Die Content-Produzenten treten inzwischen als gefragte Experten auf, entwerfen Mode und veranstalten legendäre Partys, etwa eine „sexy“ Eröffnungsparty zur Documenta 14 im Juni in Kassel.

Foto: Amin Akhtar/Laif

Nummer eins im Greifen.

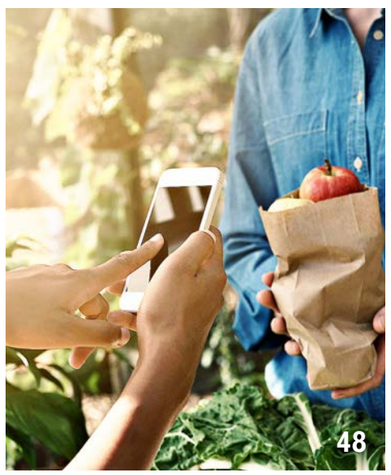
Das Familienunternehmen Schunk ist Weltmarktführer in der Entwicklung von Roboterhänden.

1945 als mechanische Werkstatt gegründet, hat sich Schunk zum Weltmarktführer mit über 2700 Mitarbeitern entwickelt. Der Hidden Champion aus der 11 000-Einwohner-Stadt Lauffen am Neckar setzte immer wieder Trends – von der Mikromontage bis zum Schwerlasthandling. Die jüngste Roboterhand des Unternehmens von CEO Henrik A. Schunk (Foto) orientiert sich in Aussehen und Beweglichkeit so nah wie nur möglich an der menschlichen Hand. Sie beherrscht unterschiedliche Greifabläufe und nutzt Tastsensoren in den Fingern für die benötigte Sensibilität. Die Schunk SVH 5-Fingerhand ist der weltweit erste von der Deutschen Gesetzlichen Unfallversicherung DGUV zertifizierte Greifer für den kollaborativen Betrieb.

Security: zwischen Multi-Channel und Multi-Challenge.

Titel: Then Ong/Wired; Fotos: Stefan Hobmaier, Dominik Giglier, David Payr, pixdeluxe/Getty Images, Johannes Heuckeroth/gallery stock, T-Systems

BEST PRACTICES



Impressum

Herausgeber:
Sven Krüger,
T-Systems International GmbH
Weinsbergstraße 70
50823 Köln

Gesamtverantwortung:
Annette Nejedl
Redaktionsleitung:
Tatjana Geierhaas
Chefredaktion:
Thomas van Zütphen (V.i.S.d.P.)
Organisation: *Anke Echterling*
Art Direction: *Tobias Zabell*
Layout: *Nora Luther*
Bildredaktion: *Susanne Narjes*
Operation Manager:
Stefan M. Glowa
Schlussredaktion:
Ursula Junger
Autoren dieser Ausgabe:
Sven Hansel, Michael Hermann, Roger Homrich, Silke Kilz, Heinz-Jürgen Köhler, Yvonne Nestler, Thorsten Rack, Anja Steinbuch, Jan Ungruhe, Thomas van Zütphen

Verlag:
HOFFMANN UND CAMPE X, eine Marke der Hoffmann und Campe Verlags GmbH, Harvestehuder Weg 42, 20149 Hamburg Tel. (040) 441 88-457, Fax (040) 441 88-236, E-Mail: x@hoca.de

Geschäftsführung:
Christian Backen
Objektleitung
HOFFMANN UND CAMPE X:
Sandra Heiske
Herstellung: *Wym Korff*
Litho: *Olaf Giesick Medienproduktion, Hamburg*
Druck:
NEEF + STUMME premium printing GmbH & Co. KG, Wittingen

Schon gelesen?
Best Practice Online:
www.t-systems.de/bestpractice

Schon runtergeladen?
Best Practice+ App per QR-Code hier oder unter itunes.apple.com

Fragen und Anregungen:
bestpractice@t-systems.com

klimaneutral
powered by ClimatePartner°
Druck | ID 11895-1703-1001

„Alles roger!“

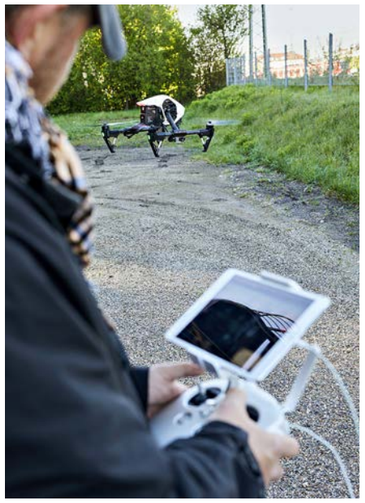
Drohnen heben gerade ab. Doch mit ihrem Boom in unterschiedlichsten industriellen Anwendungen nimmt auch ihre Attraktivität für Wirtschaftsspione rasant zu. Dafür entwickelte die Deutsche Telekom in weniger als 18 Monaten auf Basis von Funk-, Audio-, Video- und Radartechnologie den Magenta Drohnenschutzschild. Er lässt hochfliegende Pläne krimineller Piloten schnell an ihre Grenzen stoßen. In der Regel schon nach wenigen Sekunden.

Foto: Stefan Hobmaier

TEXT —— Thomas van Zütphen

Köln, 17. Mai, 11.44 Uhr. Parkplatz eines Schnellrestaurants, Dürener Straße. Anders als die anderen ersten Mittagsgäste aus dem umliegenden Gewerbegebiet parkt ein Besucher sein Auto weit abseits des Eingangsbereichs. Auf einem kaum einsehbaren Stellplatz, von den Überwachungskameras des Lokals weit entfernt. Mit links den Kofferraum zu öffnen und rechter Hand eine Drohne auf den Boden zu stellen ist für den Fahrer quasi eine Bewegung. Fernsteuerung einschalten, das leise Piepsen der sich aufbauenden Funkverbindung abwarten, und das Fluggerät hebt ab. Das anfangs nur sanfte – erst mit einer rasanten Beschleunigung vernehmliche – Sirren der Rotoren registriert keiner der an- und abfahrenden Restaurantbesucher.

Rein technisch ist dieses Szenario typisch für die Startabläufe von Multicoptern, wie sie täglich millionenfach auf der Welt von Drohnenpiloten ferngesteuert auf den Weg gebracht werden. Ihre Inbetriebnahme und Bedienung ist auch von Laien schnell erlernbar: für Luftaufnahmen von einer Hochzeitsfeier zum Beispiel oder den Kalender mit Landschaftsbildern eines Hobbyfotografen. Im professionellen Drohneneinsatz könnte es um die Vermessung von Flurstücken für das örtliche Katasteramt gehen oder das Ablesen von Barcodes in riesigen Hochregallagern, wozu etwa der Automobilzulieferer Magna bereits Drohnen bei Inventuren einsetzt (siehe Interview Seite 50). Allein aufseiten der Industrie schätzen die Wirtschaftsberater von PwC den Markt für die Einbindung von Drohnentechnologie in bestehende Geschäftsmodelle bis 2025 auf 127 Milliarden US-Dollar (siehe „Lotsen und Taucher“ Seite 42). Von möglicherweise neu aufkommenden Geschäftsfeldern, tiefdunklen oder zumindest zwielichtigen zum Beispiel, ist dabei noch keine Rede. Im Klartext: von unlauteren bis schwer kriminellen Geschäften.



Sobald der Pilot eine Funkverbindung zur Drohne aufbaut, kann der Magenta Drohnenschutzschild den Standort der Fernbedienung orten.

17. Mai, 11.45 Uhr. Wohin ist die Drohne unterwegs? Was sucht sie dort? Wie ist sie ausgerüstet? Wer steuert sie? Welche Bilder oder Videos schickt die Drohne an den Piloten? Nur wenige Gehminuten vom Schnellrestaurant entfernt sind das Fragen, auf die Frank Roby jetzt schnelle Antworten benötigt. In wenigen Augenblicken beginnt drei Flure über ihm die Vorstandssitzung der Hightechschmiede, die ihn vor langer Zeit als Leiter Werkschutz eingestellt hat. Unter anderem dafür, dass Veranstaltungen wie die, zu der gerade eine Limousine nach der anderen auf den Hof rollt, störungsfrei ablaufen. Dass eine Drohne im Anflug ist, hat Roby mittels einer neuen Technologie erfahren, die seit wenigen Wochen zur Ausstattung der Leitstelle des Unternehmens zählt. Eine Besonderheit des Magenta Drohnenschutzschilds der Telekom ist die frühzeitige Erkennung eines Piloten, der den Start einer Drohne vorbereitet – noch bevor die Drohne abhebt. Im Moment des Abgleichs von Fernbedienung und eingeschaltetem Fluggerät kann der Standort der Fernbedienung präzise bestimmt werden. Die komplexe Technologie ist auf dem Dach seines Unternehmens im Kölner Stadtteil Marsdorf zwölf Meter höher installiert. Von hier aus schützt das System Mitarbeiter, Prozesse, das geistige Eigentum der Firma und ist somit ein unverzichtbarer Teil der Sicherheitsarchitektur, zu der Roby vor Kurzem seinem Vorstand geraten hat. Die verschiedenen Sensoren aus Drohnentrackern, Frequenzscanner, Hochleistungsmikrofonen und Radartechnologie hoch über ihm sind eine Investition, die sich in den kommenden Minuten bezahlt machen wird: Denn das, was Drohnen abschöpfen können, ist den kriminellen Auftraggebern oft Millionen wert.

„Um auf eine mögliche Bedrohung aus der Luft reagieren zu können, muss diese zuverlässig und präzise erkannt werden“, erklärt Markus Piendl, verantwortlicher Produktmanager des Magenta Drohnenschutzschilds der Deutschen Telekom. Die Lösung haben Piendl und sein Team mit Unterstützung des Innovation Center von T-Systems (siehe Seite 38) über 18 Monate im Geheimen entwickelt und dabei die Hardware von 25 internationalen Anbietern auf deren Detektions- und Abwehrleistung ausführlich und fair getestet. „Unser Ziel“, so Piendl, den in- und ausländischen Behörden regelmäßig als Sachverständigen für Sicherheitstechnik ansprechen, „war es, einen lückenlos geschlossenen Schutzschirm anzubieten. Eine exzellente Lagedarstellung zeigt Angriffsverläufe in Echtzeit benutzerfreundlich und eingängig auf. Liegenschaften jeder Art werden vor Drohnenangriffen geschützt. Die verschiedenen Sensoren arbeiten akustisch, optisch, funk- oder radartechnisch.“ Eine benutzerfreundliche Managementsoftware bereitet alle Daten der Sensoren verschiedener Hersteller zu einem verständlichen Lagebild auf. Oftmals erfahren ausgespähte Unternehmen oder VIPs erst durch eine Veröffentlichung, dass sie gefilmt worden sind. Ein Traum für jeden Paparazzo, ein Albtraum für gefährdete Personen – und den Werkschutz von Industrieanlagen. Selbst dann, wenn sich herausstellt, dass es die Kameras der Drohnen nicht auf das Ausspähen von Infrastrukturen abgesehen haben, sondern auf Menschen.

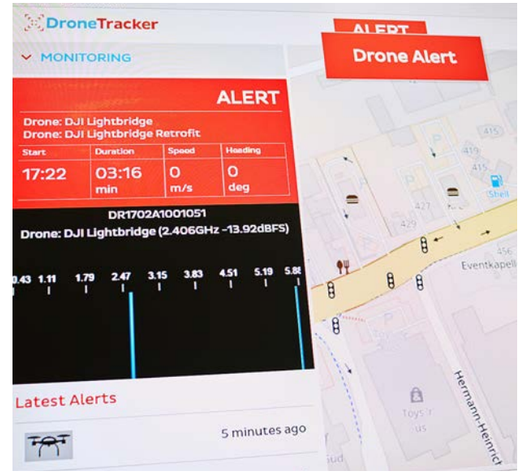
„Sofortige Drohnendetektion verschafft Kunden für ihre Abwehr wertvolle Zeit.“

PATRICK KÖHLER, Innovation Manager bei T-Systems

Auge in Auge. Lange bevor die Kamera an der Drohne den Tracker „sieht“, hat dessen Detektionstechnologie das Fluggerät erkannt.

17. Mai, 11.47 Uhr. Zumindest Robys letzte Frage wird sich schnell beantworten lassen. Um den Flugkörper zu klassifizieren, gegebenenfalls auch zu identifizieren, verfügt seine Installation über eine zentrale Datenbank. Jede Drohne hat spezifische Merkmale, die eine dahinterliegende Software in Beziehung setzt und als Signatur – oder Drone DNA – in einer Datenbank speichern kann. „Durch regelmäßige Updates kann jeder Kunde des Schutzschilds auch neue Drohnen sofort zuverlässig detektieren und gewinnt wichtige Zeit“, erklärt Innovation Manager Patrick Köhler vom T-Systems Innovation Center in München. „Mit diesem Vorsprung weiß der Kunde, bevor er die Drohne sehen kann, was buchstäblich gleich auf ihn zukommt.“

Zwischen dem nur 18 Gramm schweren kleinen Aufklärungsmonster „Black Hornet“ aus Norwegen, das durch handbreit gekippte Fensteröffnungen fliegen kann, und der fast zwölf Meter langen „Wing Loong 1“ eines chinesischen Anbieters reicht die Bandbreite käuflicher Drohnen – vom Kolibri bis zum Kondor. Zur möglichen Nutzlast können Hilfs- und Versor-



Auf den Monitoren des Drohnenschutzschilds werden jede Funkverbindung und jede Flugbewegung in einem definierten Radius präzise dargestellt.

Der Bildschirm „verrät“ in Echtzeit, was eine Drohne mit ihrer Kamera filmt oder gegebenenfalls bereits unverschlüsselt an ihre Bodenstation sendet.

Fotos: Stefan Hobmaier

400 000

Die Zahl der aktuell in Deutschland betriebenen Drohnen nähert sich nach Schätzungen der Deutschen Flugsicherung schon bald einer halben Million.

gungsgüter für Erdbebenopfer oder schnelle Medikamentenlieferungen auf Nordseeinseln genauso zählen wie Sprengstoffe und Bomben mit dem Ziel eines Unternehmenscampus oder voll besetzter Sportstadien. Und genau das ist das Problem.

17. Mai, 11.49 Uhr. Schon seit fünf Minuten weiß Frank Roby, dass die Drohne, die er jetzt mit bloßem Auge sehen kann, eine „DJI Phantom" ist, so etwas wie der VW Golf unter den Quadrocoptern. Prinzipiell sind Drohnen nichts anderes als fliegende Computer, bestückt mit Sensoren. Doch was will sie? Die Zeit drängt. Ganz oben auf der Vorstandsagenda stehen Strategiethemen und damit verbundene brisante Investitionsentscheidungen. Sichtbar beunruhigt schießt schon ein Stabsleiter durch Robys Tür, um zu „wissen, was da draußen eigentlich los ist". Auch er hat die Drohne über der Auffahrt gerade bemerkt.

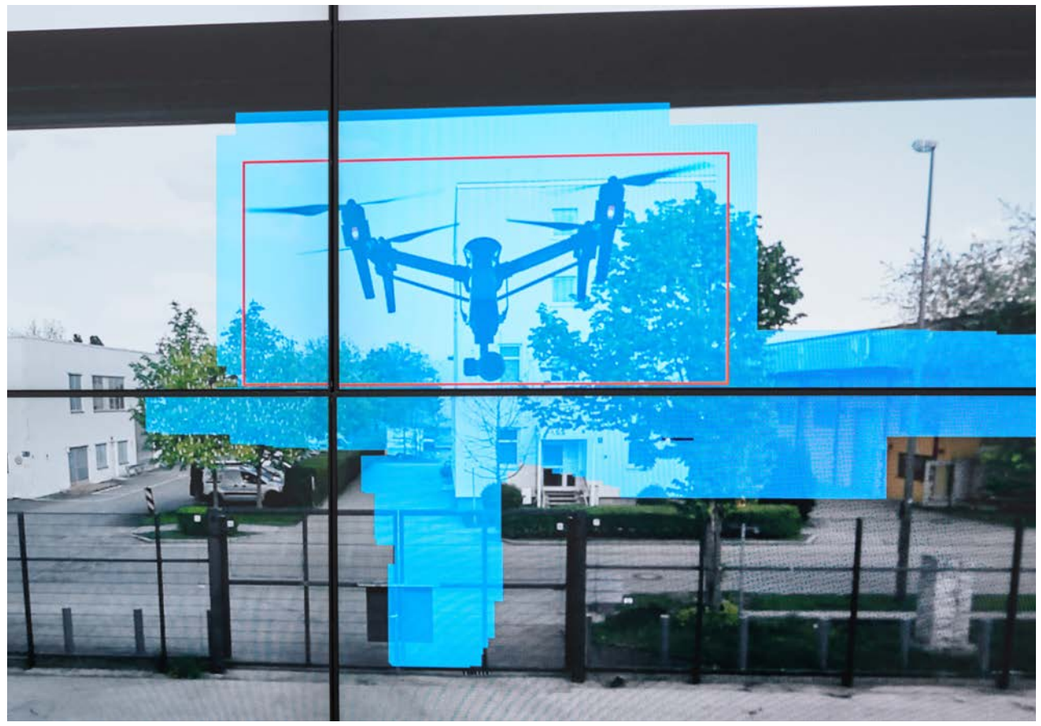
Werkschutzleiter Roby ahnt, worum es dem Drohnenpiloten wirklich gehen könnte. Eine „DJI Phantom" kann mit Richtmikrofonen oder Lasertechnologie ausgestattet werden, um jedes gesprochene Wort auch ungebeten mitzulauschen. Manch einer der fliegenden Spione überträgt alles, was er auffängt, zeitversetzt oder sofort an eine nahe liegende Bodenstation. Noch perfider: Andere laden ihre „Beute" sofort auf YouTube hoch. Doch zur Grundausstattung von Fluggeräten wie jenem, das in diesem Moment Roby immer näher kommt, gehört oft „nur" eine Kamera. Ein Blick auf den Monitor gibt Roby recht. Er verfolgt live mit, was die Drohne „sieht" und unverschlüsselt sendet. Das fliegende Mittelgewicht über dem Werkszaun ist in Lauerstellung. So reicht das Wort „Pilotensuche", um dem Stabskollegen deutlich zu machen, welches Interventionsprogramm das Werkschutzteam jetzt ablaufen lassen wird. Die Fernsteuerung des Piloten wird dank der übermittelten Sensorinformationen auf RF-Basis durch ein Werkschutzteam angefahren.

Nach Einschätzung der Deutschen Flugsicherung werden in Deutschland 400 000 UAVs – „Unmanned Aerial Vehicles" – eingesetzt. Die seit wenigen Jahren explodierende Zahl hat viele Gründe: Einfach zu steuern, verfügen sie über relativ hohe Reichweiten und können rein technisch fast überall gestartet werden. Neben der professionellen gewerblichen Nutzung in der Logistik zum Beispiel (siehe „Lotsen und Taucher" Seite 42), der Film- und Vermessungstechnik, im Agrarbereich, Bergbau und in der Geologie werden heute die meisten Multicopter von Hobbypiloten geflogen.

Doch der Arbeitsmarkt holt auf. Unbemannte Fluggeräte und ihr Betrieb entwickeln sich zum respektablen Wirtschaftszweig. Immer mehr Unternehmen sind auf der Suche nach Piloten, die für den Betrieb mit UAVs lizenziert sind. Allein in den USA gehen Arbeitsmarktprogosen in den kommenden acht Jahren von bis zu 100 000 zusätzlichen Jobs aus. Eine Entwicklung, die Christian Janke vom European Aviation Security Center (EASC) bestätigt: „Drohnentechnologien bedeuten enorme Chancen in der Wertschöpfung für innovative Geschäftsmodelle und wirtschaftlich extrem sinnvolle Anwendungsszenarien." Allerdings: „Die allermeisten Drohnen" heißt eben auch: nicht alle.

17. Mai, 11.51 Uhr. In Robys Job-Description dieses Tages hat ein Punkt absolute Priorität: Auf keinen Fall darf die Drohne, die mittlerweile durch den Alarm des Magenta Drohenschutzschilds für das menschliche Auge sichtbar über dem Werksgelände schwebt, zu sehen bekommen, wer hier in weniger als einer Minute aussteigt. Jemand, dessen Besuch dem Vorstand hochwillkommen ist. Obwohl diese Person selbst noch nicht dem Vorstand angehört.

Obligatorisch wurde die Anfahrt aller Sitzungsteilnehmer im Vorfeld bis ins Detail organisiert. So wird auch der Gast des heutigen Meetings von seinem Fahrer bis in die Tiefgarage chauffiert und erst direkt am Executive-Lift aussteigen. Den vom Fahrstuhl ohne Zwischenstopp ansteuerbaren Konferenzraum hat ein Team externer Lauschabwehrspezialisten tags zuvor akribisch auf Abhörsicherheit untersucht (siehe Reportage „Die Klaviatur des Bösen" Seite 26). Definitiv frei von Kameras, Wanzen & Co. wurde der Raum verschlossen und mit einem Siegel versehen, das in diesen Minuten entfernt wird.



Drohnen-Selfie. Im Anflug auf ein innensichtgeschütztes Bürofenster sieht die Drohnenkamera nur ihr eigenes Spiegelbild.

Foto: Stefan Hobmaier

Automatisch initiiert währenddessen die Drohnenerkennungssoftware den im Gebäude-Sicherheitsmanagementsystem hinterlegten Interventionsplan. Dazu zählt, dass die Notstromversorgung des Gebäudes vorsorglich auf Stand-by hochgefahren wird, sich alle Lüftungsklappen der ab sofort mit Umluft arbeitenden Klimaanlage automatisch schließen und sämtliche Jalousien des Gebäudes runterfahren. Auch die der Panoramafenster im Konferenzraum, wie Roby den Teilnehmern mit Hinweis auf „einen gegebenen Anlass" erklärt. Konkret steht dahinter die Möglichkeit, dass Angreifer via Drohnen von ungeschützten Fensterscheiben mittels Lasertechnologie Schallwellen abschöpfen und entschlüsseln. Das Ergebnis läge in kürzester Zeit in klarer Sprache vor.

Wirtschaft geht immer einher mit Wirtschaftskriminalität. Als herstellerunabhängiges Forschungszentrum für Luftsicherheit in Europa unterscheidet das EASC mit Sitz südwestlich von Berlin dabei grundsätzlich drei Bereiche, in denen der missbräuchliche Einsatz von Drohnen eine Rolle spielen könnte: den privaten Bereich als Verletzung von Hausfrieden und Persönlichkeitsrechten, den kommerziellen Bereich als Industriespionage und das Spektrum klassischer Kriminalität wie Schmuggel, Drogentransport oder die Einbringung von Gegenständen in Sicherheitsbereiche, auch zu terroristischen Zwecken.

„Je weiter die technischen Möglichkeiten gehen, desto weitreichender auch die kriminellen Optionen", sagt Jörg Lamprecht von der Firma Dedrone. „Neue Drohnen werden nahezu Tag für Tag autonomer, können länger und weiter fliegen. Dabei werden sie immer schwerere Lasten tragen und auch in Schwärmen agieren."

17. Mai, 11.52 Uhr. Wenn die Hochtechnologie auf der Dachkante in Köln-Marsdorf, Dürener Straße, so etwas wie ein Kernstück hat, sind es die Drohnentracker, RF-Sensoren und die Managementsoftware des von Lamprecht gegründeten Kasseler Start-ups Dedrone. Die Geräte werden an Fassaden oder Dächern montiert. Über eine intuitive, browserbasierte Benutzeroberfläche können die Kunden die Sensoren einfach konfigurieren und das überwachte Gebiet in Echtzeit beobachten. Bei einem Drohnenalarm werden die Sicherheitskräfte sofort benachrichtigt. Frank Roby und sein Team beispielsweise. Zwei seiner Kollegen werden in wenigen Augenblicken den Piloten der Drohne persönlich „begrüßen", der als Steuermann des ungebetenen Zaungastes ausgemacht werden konnte.

„Die Drohne zu detektieren ist Pflicht. Die Kür ist es, den Piloten zu finden."

MARKUS PIENDL,
Produktmanager Magenta Drohnenschutzschild bei T-Systems

„Die Drohne zu detektieren ist Pflicht. Die Kür ist, den Piloten zu finden, denn nur so kann das eigentliche Problem und dessen Verursacher angegangen werden", so Markus Piendl. Was jetzt folgt, ist schnell auf den Punkt gebracht: persönliche Ansprache, Polizei, Strafanzeige. Vorbehaltlich weiterer Maßnahmen.

Bei dem Einsatz elektronischer Störmaßnahmen wie dem sogenannten Jamming, das die Kommunikation zwischen Drohne und Fernsteuerung überlagert, sind der Privatwirtschaft vom Gesetzgeber sehr enge Grenzen gesetzt. Dass diese Störmaßnahmen grundsätzlich „behördlichen Bedarfsträgern" vorbehalten sind, gilt nicht nur in Deutschland. Weil in der Konsequenz Firmen und ihre Wachschutzmitarbeiter an dieser Stelle unkonventionell vorgehen müssen und in den allermeisten Fällen keinen Jammer einsetzen dürfen, sehen Unternehmen wie der kanadisch-österreichische Automobilzulieferer Magna „drängenden gesetzgeberischen Handlungsbedarf" (siehe Seite 50). Die Telekom bemüht sich bereits für besonders zu schützende Objekte um Ausnahmegenehmigungen bei den zuständigen Behörden.

17. Mai, 11.59 Uhr. Parallel zum Eintreffen der Polizei am Schnellrestaurant vergleicht Frank Roby die MAC-Adresse der Drohne mit seiner Datenbank. Er entdeckt schnell, dass die Drohne in den vergangenen Tagen mehrfach außerhalb seiner Liegenschaft in Betrieb war. Es liegt also nahe, dass der Pilot den heutigen Anflug geübt und das Objekt ausgespäht hat. Diese Daten wird Roby gerichtsfest sichern und den Ermittlungsbeamten zur Verfügung stellen. Die Polizei findet später heraus: Der Pilot auf dem Parkplatz war nur angeheuert. FairFleet, Airdolly oder Drohnen.pro 101 – Internetportale, auf denen jeder Drohnenpiloten buchen kann, gibt es Dutzende. Für genau diesen Auftraggeber, der per Kreditkarte bezahlt hat, wird's jetzt richtig teuer. Sicher ist für Roby in diesem Moment: In einer Minute kann die Vorstandssitzung pünktlich beginnen. Im Luftraum über dem Firmengelände ist wieder „alles roger".

markus.piendl@t-systems.com
www.t-systems.de/telekom/drohnenschutzschild
www.t-systems.de/video/magenta-drohnenschutzschild

Mit intelligenter Rückendeckung gegen Hacker.

Findiger, schneller, aggressiver. De facto vergeht keine Sekunde, in der nicht irgendwo auf der Welt Hacker daran arbeiten, ihre Attacken zu perfektionieren. Noch gewissenloser, brutaler, perfider. Die Armee der Bösen rüstet ständig auf, und ihre Angriffsmuster werden immer komplexer und raffinierter. Doch wo bleibt eigentlich die Armee der Guten, die dagegenhält?

Illustration: erhui1979/Getty Images

TEXT —— Thomas van Zütphen

Steht irgendwo geschrieben, dass sich die Angriffsziele – und 93 Prozent aller Großkunden und großen mittelständischen deutschen Unternehmen wurden 2016 schon angegriffen – fast immer als Einzelkämpfer verteidigen müssen? Und in Zeiten, in denen der Cyberwar keinen Waffenstillstand mehr kennt, genügt es einfach nicht, von einem IT-Dienstleister flankiert zu sein, der sein Brot- und Buttergeschäft einwandfrei beherrscht, aber womöglich vor der Hightech- Phalanx von Cyberkriminellen die weiße Fahne hisst.

Die Deutsche Telekom hält dagegen, stellt sich stark auf und hat zum 1. Januar dieses Jahres sämtliche Security Ressourcen des Konzerns mit nahezu 1200 Sicherheitsexperten gebündelt. Seither operiert die neue Konzerneinheit Telekom Security als eigenständiger Geschäftsbereich unter dem Dach der T-Systems. „Unsere Kunden befinden sich mitten in der digitalen Transformation. Diese ist für mich gekennzeichnet durch einen Dreiklang aus dem Internet der Dinge, Cloud und Sicherheit. Security ist dabei die Grundbedingung für eine erfolgreiche Digitalisierung“, so Telekom-Security-Geschäftsführerin Anette Bronder, die auch die Digital Division der T-Systems verantwortet. „Bei der Entwicklung von Produkten und Geschäftsmodellen denken wir das Thema Sicherheit von der ersten Idee an mit.“

Auf diese Herausforderung ist die Telekom schon aus der eigenen Unternehmensgeschichte heraus gut vorbereitet. Seit mehr als 20 Jahren schützen die eigenen Security-Spezialisten die Telekom als kritische Infrastruktur – immerhin mit aktuell 225 000 Mitarbeitern weltweit. Sie schützen die Rechenzentren, den Datenverkehr, die mobilen Geräte und Netze für die Kunden der Telekom. „Was liegt also näher, als dieselben hochprofessionellen Tools, die wir zu unserem Schutz einsetzen, auch unseren Kunden anzubieten?“, so Dirk Backofen, Leiter Telekom Security (siehe Interview Seite 25). „Zu unseren Kunden zählen viele Dax-Konzerne und mittelständische Marktführer der Schlüsselindustrien Automotive und Maschinenbau, Chemie und Pharma, Energie und Finance.“ Allein in Europa soll der Markt von derzeit 13 Milliarden Euro bis 2020 jährlich sieben bis acht Prozent wachsen.

Vertrauen und Vertrauensvorschuss zugleich

Allein um weitere 300 Mitarbeiter baut die Telekom Security ihr Expertenteam aktuell aus, um den Anforderungen im Markt Rechnung zu tragen. Quasi verankert in der DNA jedes der dann 1500 Spezialisten in den Bereichen Consulting, Sales, Presales, Engineering, Produktion und Operative Abwehr ist das Ziel: Zero Impact. „Cyberattacken, egal ob auf Privatkunden, Mittelstand oder Großkonzern, können zwar grundsätzlich nicht verhindert werden, aber deren Auswirkungen“, so Dirk Backofen. „Wir wollen die Cybersecurity-Allianz all unserer Kunden gestalten.“

Das nötige Security-Equipment ist praktisch an jeder Straßenecke zu bekommen. Die eigene Messlatte „Zero Impact“ jedoch kann die Telekom bei ihren Kunden nur deshalb so hoch hängen, weil sie im Unterschied zu anderen Anbietern das Thema Security tief in die Themen Konnektivität und Cloud integriert und in der Lage ist, das Zusammenspiel unterschiedlichster Lösungen zu orchestrieren. Gelernt ist gelernt. Dazu bildet unter anderem eine Honeypot-Landschaft mit rund 1000 virtuellen Sensoren im Netz unterschiedlichste Geräte ab: Smartphone, Laptop, PC oder Data-Center-Rack. Damit bieten die Konzernspezialisten eine Angriffsoberfläche, die täglich vier Millionen Angriffe registriert und vollautomatisch auswertet. Dazu analysieren die Experten der Telekom täglich hoch spezialisierte und zielgerichtete Angriffe auf das eigene sowie auf andere Unternehmen. Mithilfe dieser Erkenntnisse lassen sich die Abwehrmechanismen immer weiter verfeinern, und das Wissen über die Angreifer wird verbessert.

In der Summe registriert das Unternehmen aus mehr als 3000 Datenquellen etwa eine Milliarde sicherheitsrelevante Events pro Tag und muss möglichst in Echtzeit identifizieren, welcher Vorfall so kritisch und alarmierend ist, dass man ihm sofort nachgehen muss. Der dafür nötige Abgleich erfolgt voll automatisiert in einer rund 20 Millionen Schadcodes und Angriffsindikatoren umfassenden Security-Datenbank, in die täglich neue, auch von den Telekom-Experten selbst geschriebene Virensignaturen und Zero Day Exploits eingespeist werden. „Diesen Schatz nutzen wir auch regelmäßig dafür, um neue Lieferanten und deren Produkte auf ihre Detektionsfähigkeit zu testen“, so Backofen. „Das gehört zu unserem Anspruch, denn wir wollen nur die Innovativsten und Besten der Besten in unser Portfolio und Partnernetzwerk aufnehmen, um damit den Schutz, den wir unseren Kunden bieten können, ständig zu verbessern.“ Denn die Aufgabe, das permanente Wettrennen mit Cyberkriminalität immer offen zu halten oder den Angreifern sogar voraus zu sein, ist gewaltig – und allein von niemandem zu schaffen. Im Ergebnis kooperiert Telekom Security heute mit 50 Partnern weltweit, deren Lösungen jedes denkbare Spektrum möglicher Angriffsflächen eines Unternehmens abdecken.

„CEOs und ihre Sicherheitsverantwortlichen erwarten zu Recht, dass Security einfach, bequem und übersichtlich bleibt und ihnen ein Maximum an Managed Security Services geboten wird.“

DIRK BACKOFEN,
Leiter Telekom Security

Transparenz in die Tätertaktik

Auch dahinter steckt die Philosophie des Aufbaus einer „Armee der Guten“, eines Cybersecurity-Schutzschilds für alle Kunden weltweit, vom Dax-Konzern über den Mittelstand bis zum Privatkunden. Zur Ausgestaltung dieser Art Cyberallianz zählt unter anderem, die Informationen und Ergebnisse jeder bei einem Kunden registrierten neuen Angriffsform – sei es in einem bei ihm installierten Sensor oder real – sofort in die Sicherheitssysteme aller anderen Kunden zu integrieren.

Doch was verbirgt sich hinter Mobile Protect Pro, Internet Protect Pro, Vulnerability Scan as a Service, Security Operations Center oder Industrial Control Systems Security? Was leisten die am Markt gefühlt täglich neu aufpoppenden Sicherheitslösungen, wie nützen sie meinen Geschäftsprozessen und konkret wobei? Allein die Fragen dokumentieren den zentralen Bedarf an Security Operation. Dessen Treiber sind Tempo und Komplexität neuer Angriffstechnologien auf der einen und hochmoderne Präventions-, Detektions- und Abwehrtechnologien auf der anderen Seite. Dirk Backofen: „Um die bei uns erworbenen Tools und Lösungen guten Gewissens einzusetzen, erwarten die CEOs unserer Kunden und ihre Sicherheitsverantwortlichen unserer Kunden zu Recht, dass Security für ihre Anwender einfach, bequem, handlich und übersichtlich bleibt. Wir wollen und können als Managed-Security-Services-Provider unseren Kunden die Angst vor der Komplexität im Bereich Cybersecurity nehmen.

Die Wahl zwischen wehrhaft und schwach

Eine herausragende Rolle für das Erreichen dieses Ziels spielt die Einrichtung eines neuen Security Operations Centers (SOC), in dem die Sicherheitsbelange der Telekom-Security-Kunden genauso professionell angegangen werden wie die des eigenen Konzerns (siehe Seite 22). Dessen eigene Angriffsvektoren reichen, wie praktisch in jedem Unternehmen heute, von der Data-, Application- oder Network-Security-Ebene bis zur Endpoint/Mobile Security, Industrial Control Systems Security und ID-Sicherheit. Um diese Komplexität im Betrieb zu managen, laufen sämtliche sicherheitsrelevanten Informationen aus allen genannten Layern zentral im SOC auf. Damit wird das neue Center zum Fundament von Lösungskonzepten und deren Implementierung.

Doch wie steht es generell um das Security-Fundament der Unternehmen? Grundsätzlich attestieren Sicherheitsexperten neun von zehn Corporate-Netzwerken deutscher Firmen mit den typischen Data-Center- und Office-Strukturen bereits ein ganz vernünftiges Schutzlevel. Doch noch immer arbeiten viele vor allem mit klassischen Advanced Security Hubs, die mit der traditionellen Logik von Firewalls und Intrusion-Prevention-Systemen, Web-Proxy-/Mail-Relay-Systemen unterwegs sind. Und wissen dabei oftmals nicht, dass sie damit nur nach sogenannten Known Threats suchen können. Aber wie detektieren sie eine Bedrohung, von der man noch nie gehört hat? Spätestens dafür sollten Unternehmen einen neuen Sicherheitslayer einbauen, um sich auch vor bislang unbekannten Angriffen wie Advanced Persitent Threats und Zero Day Exploits zu schützen.

450 Milliarden € Schaden

Der weltweite wirtschaftliche Schaden durch Cyberkriminalität erreichte bereits 2016 umgerechnet fast eine halbe Billion Euro. Fast Prozent davon, mehr als 51 Milliarden Euro, „verbuchte“ allein die deutsche Wirtschaft.

(The Global State of Information Security Survey 2015, PricewaterhouseCoopers)

Illustration: erhui1979/Getty Images

Auch Stand-Alone lässt sich veredeln

Solche Layer zum Beispiel baut Telekom Security mit einer Sandbox-Umgebung als Advanced Persistent Threat Protection wahlweise für die On-premise-Bereitstellung mit dem Partner Cisco oder als Cloudlösung von Checkpoint. Dabei werden verdächtige Mails schon beim Eintreffen in einer hochsicheren, abgeschirmten Umgebung geöffnet, die einen Arbeitsplatz simuliert. Zunächst einmal „gecacht“, werden die Mail und ihre Anhänge erst nach erfolgreicher Emulation dem Nutzer zugestellt. Dabei arbeiten aufgesetzte Telekom-Security-Services wie Mobile Protect Pro (MPP) auf den Endgeräten der Kunden wie ein Dauer-EKG. Wenn eine Korrelation der über 1000 Vektoren auftaucht, die MPP noch nie gesehen hat, ist die Wahrscheinlichkeit groß, dass es sich um einen Angriff handelt. Damit neben dem Smartphone oder Tablet auch wahlweise der Zugang zum Firmennetz abgeschaltet wird, ist MPP direkt mit dem beim Kunden bereits installierten Mobile-Device-Management-System verbunden.

Noch schlechter als bei der Corporate-IT fällt das Zeugnis der Experten aus, das sie den Industrienetzwerken ausstellen. So wird geschätzt, dass nur zehn Prozent aller Kunden in Deutschland ihre Industrienetze richtig absichern. Galt lange Zeit als bester Schutz, das Industrienetz isoliert vom Internet zu betreiben, ist diese Trennung in Zeiten von IoT, Realtime- und Maintenance-Prozessen buchstäblich kontraproduktiv. Jeder Remote-Support braucht einen physikalischen Zugang, sonst kann der Lieferant oder Hersteller einer Maschine nicht unterstützen. Dafür müssen Servicetechniker auf andere Protokolle zugreifen, um die jeweiligen Schnittstellen als potenzielles Einfallstor von Angreifern zu sichern.

„Vom solitären Datensatz bis zur vollständigen Intellectual Property eines Unternehmens – die Aussicht auf Beute wird Hacker nie ruhen lassen.“

DIRK BACKOFEN, Leiter Telekom Security

93 %=
flächendeckend

So großflächig wie Internetkriminelle die Konzernlandschaften unter Beschuss nehmen, bleibt – wie 2016 – de facto kaum noch ein Großunternehmen von Cyberattacken verschont.

(Sicherheitsreport Entscheider 2016, Institut für Demoskopie Allensbach)

Rendezvous im virtuellen Raum

Zur Industrial Control System Security (ICS) der Telekom gehört neuerdings mit Industrial Access Protect Pro auch eine flexible Fernwartungslösung des Telekom Security Partners genua aus Kirchheim. Die Lösung liegt in der Cloud oder am Kundenstandort und bietet eine granulare Kontrolle jedes einzelnen Zugriffs zur Überwachung von Fernwartungszugriffen in Echtzeit und deren Dokumentation. Der Clou und damit ein zentrales Sicherheitsmerkmal ist, dass sie keine direkten Zugriffe durch externe Techniker auf die betreuten Anlagen zulässt. Denn die Wartungsarbeiten erfolgen zunächst in einem virtuellen Raum in der Cloud, in dem Techniker und Technik miteinander interagieren können, ohne dass ein Externer bereits direkten Zugriff auf die Anlage hat. Wartungsverbindungen nutzen Verschlüsselungsinstanzen und müssen stets kundenseitig über einen sogenannten Rendezvous-Server erst freigeschaltet werden.

Weitere Herzstücke des Industrial-Control-Systems-Security-Angebots, von der permanenten Schwachstellenanalyse über die automatische Angriffserkennung bis zum Compliance Reporting, sind ein Security Incident and Event Management (SIEM), eine Firewall sowie ein Identity and Access Management, die über Lösungen der Partner CyberX und radiflow industriell, also netzwerkweit, in den typischen Sprachen der Industrienetzwerke operieren können.

Doch Angriffe drohen Unternehmen immer häufiger nicht mehr nur aus dem Netz. Zur Sicherung originärer Industrieanlagen vor Angriffen aus der Luft erfährt ein Service der Telekom Security eine immense Nachfrage: das Magenta Drohnenschutzschild der Deutschen Telekom (siehe Reportage Seite 12). Für Dirk Backofen hat „das herausragende Kundeninteresse an unseren Security-Lösungen im hochaktuellen Bereich Drohnenkriminalität auch eine alarmierende Seite: Die Aussicht auf Beute, vom solitären Datensatz bis zur vollständigen Intellectual Property eines Unternehmens, wird die Hacker da draußen niemals ruhen lassen“.

dirk.backofen@t-systems.com
www.t-systems.de/magenta-security
www.t-systems.de/unternehmenssicherheit
www.t-systems.de/video/magenta-security

Wo Profis gegen Profis kämpfen.

Anschleichen, geduldig abwarten, unerkannt zuschlagen. Die Art, wie Advanced Persistent Threats IT-Systeme attackieren, Daten abgreifen und ganze Unternehmen lahmlegen, steht für die neueste Generation hochprofessioneller Cyberangriffe. Um sich vor ihnen nachhaltig zu schützen, setzen immer mehr Unternehmen auf externe Security Operations Center. Ein Dienst, den die Telekom via Cloud als SOC as a Service zur Verfügung stellt.

TEXT —— Roger Homrich

Sie heißen Operation Pawn Storm, Office Monkeys oder Fancy Bear. Chic sind sie jedoch nicht. Eher raffiniert – und bereiten Sicherheitsexperten besondere Kopfschmerzen. Denn sie agieren wie Auftragseinbrecher, sind Cybersöldner, die im Auftrag Dritter zielgerichtet Infrastrukturen von Unternehmen attackieren. Dafür nisten sie Schadsoftware unbemerkt in Netzwerke ein. Der Schädling verbreitet sich dann klammheimlich, sammelt Daten und sendet sie an Angreifer und Auftraggeber. Durchschnittlich 208 Tage dauere es, bis ein Cyberspion auffliegt, hat das Bundesamt für Sicherheit in der Informationstechnik berechnet. Oftmals jedoch noch viel länger. „Der aktuell von uns festgestellte Rekord liegt bei fünf Jahren“, sagt Dr. Alexander Schinner, IT-Forensiker bei T-Systems, der als Spurensucher Jagd macht auf Angreifer aus dem Netz (siehe Interview S. 29).

APT28 – Advanced Persistent Threats 28 – heißt eine Hackertruppe, die seit Jahren mit gezielten Angriffen ihr Unwesen treibt. Die Fancy Bears schlagen überall dort zu, wo ihre Auftraggeber sie hinschicken – wenn sie genug Geld in die Hand nehmen. So sollen die russischen Cyberkrieger sich während des US-Wahlkampfs auf den Servern der Demokraten eingenistet haben. Und vermutlich steckt APT28 hinter dem Angriff auf den Deutschen Bundestag im Mai 2015 sowie dem Hack auf Emmanuel Macron, nur wenige Tage vor der Stichwahl im französischen Präsidentschaftswahlkampf im Mai 2017.

Vorsicht bei E-Mails von „Freunden“

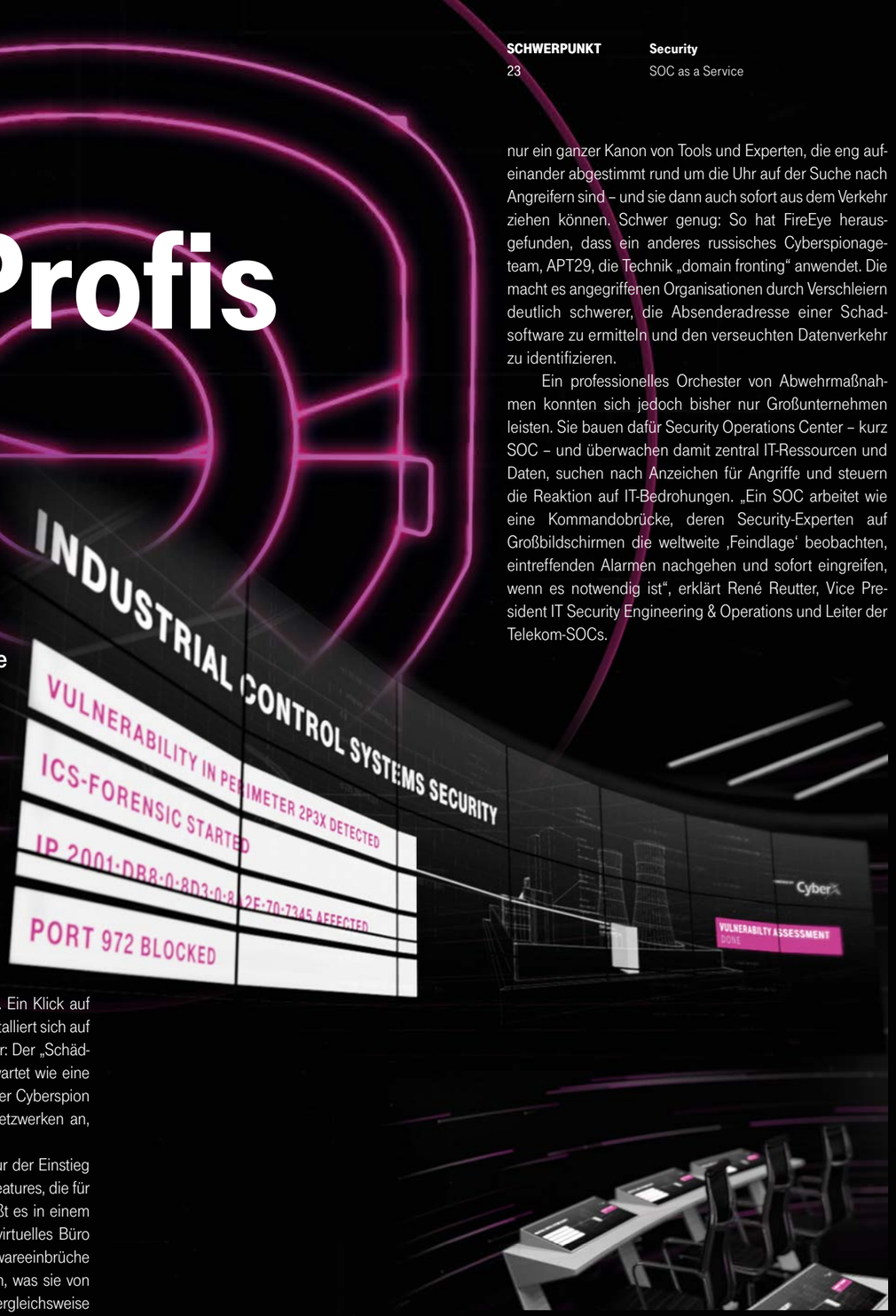
Die Vorgehensweisen der Spione sind unterschiedlich. Beliebt und simpel zugleich ist das Spearfishing. Der Hacker beobachtet sein Opfer, lernt es kennen und sendet ihm irgendwann eine unauffällige E-Mail zu. Absender: ein Bekannter, Freund oder Familienmitglied. Ein Klick auf Anhang oder Link reicht, und die Malware installiert sich auf dem Zielrechner. Es geht aber noch einfacher: Der „Schädling“ sitzt auf einer infizierten Website und wartet wie eine Zecke im Gras auf arglose Besucher. Oder der Cyberspion greift über bekannte Sicherheitslücken in Netzwerken an, die zu spät geflickt werden.

Das Installieren der Schadsoftware ist nur der Einstieg ins System. „APT28 nutzt eine Malware mit Features, die für andauernde Operationen gedacht sind“, heißt es in einem FireEye-Report. Die Hacker bauen sich ein virtuelles Büro auf, über das sie größer angelegte Softwareeinbrüche durchführen. Dafür brauchen sie Ressourcen, was sie von den Alltagshackern unterscheidet, die ihre vergleichsweise einfach gestrickten Viren und Würmer massenhaft versenden und deren Erfolge eher auf Zufall beruhen – dafür auch weniger kosten.

Zentrale Überwachung der IT-Infrastruktur

Für die Abwehr von Schädlingsmassenware reichen herkömmliche Virenscanner, Firewalls und Antiphishing-Programme in der Regel aus. Aber gegen APT hilft zumeist nur ein ganzer Kanon von Tools und Experten, die eng aufeinander abgestimmt rund um die Uhr auf der Suche nach Angreifern sind – und sie dann auch sofort aus dem Verkehr ziehen können. Schwer genug: So hat FireEye herausgefunden, dass ein anderes russisches Cyberspionageteam, APT29, die Technik „domain fronting“ anwendet. Die macht es angegriffenen Organisationen durch Verschleiern deutlich schwerer, die Absenderadresse einer Schadsoftware zu ermitteln und den verseuchten Datenverkehr zu identifizieren.

Ein professionelles Orchester von Abwehrmaßnahmen konnten sich jedoch bisher nur Großunternehmen leisten. Sie bauen dafür Security Operations Center – kurz SOC – und überwachen damit zentral IT-Ressourcen und Daten, suchen nach Anzeichen für Angriffe und steuern die Reaktion auf IT-Bedrohungen. „Ein SOC arbeitet wie eine Kommandobrücke, deren Security-Experten auf Großbildschirmen die weltweite ‚Feindlage‘ beobachten, eintreffenden Alarmen nachgehen und sofort eingreifen, wenn es notwendig ist“, erklärt René Reutter, Vice President IT Security Engineering & Operations und Leiter der Telekom-SOCs.



Fotos: T-Systems

Eng aufeinander abgestimmte Tools

Dafür steht den Abwehrteams eine ganze Reihe von Sicherheitslösungen zur Verfügung, die automatisiert die zu schützenden IT-Systeme beobachten. Diese sind über Schnittstellen mit dem SOC verbunden, sodass jeglicher Datenverkehr beobachtet und analysiert wird. Da der Aufbau und der Betrieb teuer sind und Topexperten unterschiedlicher Qualifikation gebraucht werden, setzen immer mehr Unternehmen auf extern gemanagte SOCs – und damit auf Kostenteilung.

Die Cloud macht jetzt möglich, den Schutz eines Security Operations Center auch als Dienstleistung bereitzustellen (SOC as a Service), bei dem ein Security-Provider wie die Telekom nicht länger jedes Center exklusiv für einen dedizierten Auftraggeber betreibt, sondern viele Kunden parallel aus einem SOC heraus beliefern kann.

So ermöglicht die Telekom unter anderem dem deutschen Mittelstand, Heimat der Hälfte aller Hidden Champions weltweit, Security auf einem Niveau zu beziehen, das bis vor Kurzem nur Großkonzernen zur Verfügung stand. Zugleich macht der IT-Dienstleister damit den beiden größten „Show-Stoppern“ kleinerer und mittlerer Unternehmen in Sachen Security ein Ende: Der Mittelstand muss nicht länger im War for Talents nach eigenen Experten suchen und nicht mehr selbst in eigene, teure Technik investieren. Gerade mit Blick auf den anhaltenden Fachkräftemangel, so Frank Luzsicza, Bereichsleiter ICT & Business Solutions des TÜV Rheinland, „wird Vertrauen in einen kompetenten externen Partner für Cybersecurity zu einem der wichtigsten Erfolgsfaktoren für die Absicherung des Unternehmens“.

Treiber sind Kritis und das IT-Sicherheitsgesetz

„Grundsätzlich ist das Thema SOC nicht wirklich neu“, sagt Rüdiger Peusquens, „das IT-Sicherheitsgesetz und die zunehmende Qualität der Angriffe haben allerdings erst jetzt verstärkt die Aufmerksamkeit auf das Thema gelenkt“, so der Leiter des Cyber Defense Center der Telekom, verantwortlich für den Schutz der Telekom als kritische Infrastruktur. So ist inzwischen die Kritis-Verordnung zur Umsetzung des IT-Sicherheitsgesetzes in Kraft getreten. Unternehmen aus den Sektoren Energie, Informationstechnik und Telekommunikation, Wasser, Ernährung sowie Finanzen, Transport und Verkehr müssen besondere Maßnahmen umsetzen, um die Verfügbarkeit und Sicherheit ihrer IT-Systeme sicherzustellen.

Erst im März 2017 hat ein großes Energieunternehmen das Threat- und Vulnerability-Management sowie moderne Analysemethoden zum störungsfreien Betrieb der Infrastruktur an die Telekom ausgelagert. „In einem SOC zentral sämtliche Informationen aus allen Prozesslayern eines Unternehmens zu bündeln und zu bewerten hat eine enorme Bedeutung“, so Dirk Backofen, bei der Telekom Leiter der neuen konzernweiten Business Unit Telekom Security. „Nur mit dieser Informationslage kann man die eigene Betriebsumgebung mit ihren unterschiedlichen Sicherheitsleveln

steuern.“ Dafür ist es allerdings auch nötig, auf allen Ebenen des Kundenbusiness entsprechende Security-Angebote vorzuhalten und den Kunden beraten zu können, was für seine Use-Cases die beste Kombination ist.

Dass es auch dabei viel Erfahrung braucht, um die schiere Menge möglicher Technologien richtig zu nutzen, ist nur einer der Gründe dafür, dass der Kundenbedarf an Security-Cyber-Defense-Orchestration weltweit steigt. Eine Nachfrage, der das neue, in Bonn eingerichtete SOC der Telekom Security in Kombination mit dem Cyber Defense Center der Telekom vom Herbst dieses Jahres an Rechnung tragen wird.

Im dritten Quartal dieses Jahres, so die Planung, wird das Bonner Security Operations Center, in Kombination mit dem Cyber Defense Center des Konzerns, den Betrieb zur zentralen Überwachung der IT-Infrastrukturen der Telekom-Kunden aufnehmen.

Prävention, Detektion, Response

Das verwirrende Durcheinander von Angriffs- beziehungsweise Verteidigungstechnologien, das hier beherrscht werden will, bekommt Struktur, wenn man die Arbeit eines SOC auf drei Ebenen „zerlegt“: Prävention, Detektion, Response. In anderen Worten: Wie schütze ich ein Unternehmen im Vorfeld? Wie stelle ich fest, wann die Firewall – was völlig normal ist – Ransomeware, APTs & Co. bis zum Betrieb der Systeme freien Durchgang gewährt und automatisch Lösungen wie Intrusion Prevention oder Advanced Threat Protection aktiviert werden müssen? Und wer oder was hilft 24/7/365, wenn ein System infiziert ist und ein Helferteam quasi auf Knopfdruck nottut, um remote oder on premise kürzestmögliche Reaktionszeiten zu gewährleisten? Etwa um eine Malware zu isolieren oder einen infizierten Rechner zu deinstallieren. Und das sind noch die leichteren Aufgaben des Incident Response Retainer Service, den die Telekom Security für solche Fälle bereithält. Im Zweifelsfall mindestens so wichtig sind die Rückverfolgbarkeit von Angriffen und Antworten auf Fragen wie: Was ist überhaupt passiert? Welche Daten sind verloren gegangen? Wohin wurden sie versendet? Waren Geschäftsgeheimnisse darunter? Solcherlei hoch qualifizierte Forensikexperten, wie die Telekom Security ein gutes Dutzend beschäftigt, gibt es nur sehr wenige in Europa. Doch nur sie können ermitteln, welche Wege was in welcher Form genommen hat.

„Ein SOC arbeitet wie eine Kommandobrücke, deren Security-Experten die weltweite ‚Feindlage‘ beobachten und sofort eingreifen können.“

RENÉ REUTTER, Leiter Telekom Security Operations Center

Sicherheit für industrielle Anlagen

Mit Industrienetzen und verknüpften Rechner-, Mess-, Steuer- und Regelsystemen in der Produktion können APTs in der Sicherheitsarchitektur von Unternehmen eine riesige Flanke aufreißen. „Die Anlagen sind häufig mit veralteter Technologie ausgestattet und verfügen über keine Gegenmaßnahmen gegen Cyberattacken, da sie einfach nicht für den vernetzten Betrieb konstruiert wurden“, sagt Bernd Jäger, Experte für Industrial Control Systems Security (ICS) bei der Telekom. „Normale IT-Sicherheitssysteme wie IT-Firewalls können in diesem Bereich nicht eingesetzt werden, und Know-how für Cybersicherheit in Industrienetzen ist oft nur rudimentär vorhanden.“ Die Telekom weitet daher die Partnerschaftslandschaft im Security-Umfeld mit Anbietern aus, die auf Industrieanlagen zugeschnittene Sicherheitslösungen entwickelt haben. Dabei geht es im Fokus von ICS-Security darum, vor allem die Detektion möglicher Angriffe zu beschleunigen sowie die angemessenen Entscheidungen von Unternehmensverantwortlichen durch die intelligente Dosierung automatisierter Gegen- und Schutzmaßnahmen zu unterstützen. „Auch diese Lösungen sind dann bei Bedarf Bestandteil eines gemanagten Security Operations Center“, erklärt René Reutter.

Wie wichtig SOCs sein können, zeigt der Kampf gegen Doping im Sport. Möglicherweise hätte ein SOC der Welt-Anti-Doping-Agentur (Wada) viel Ärger erspart. Die Fancy Bears statteten den Datenbanken der Wada schon mehrfach einen Besuch ab – und geben das unverhohlen zu: „Grüße an alle Bewohner der Welt“, heißt es auf der Startseite von Fancybear.net, „wir stehen ein für Fair Play und sauberen Sport. Wir werden euch sagen, wie Goldmedaillen gewonnen wurden. Wir haben die Datenbank der Wada gehackt und waren schockiert über das, was wir gesehen haben.“ Manchmal kann Hacking auch sinnvoll sein.

reutter@t-systems.com
www.t-systems.de/telekom/security-operation-center
www.t-systems.de/loesungen/cyber-security

Fotos: T-Systems

INTERVIEW

„Wir wollen es, und wir können es.“

Dirk Backofen, Leiter der Telekom Security, über den Kundennutzen einer europäischen SOC-Landschaft, den Boom am Markt für Managed Security Services (MSS) und den Ansatz „Zero Impact“, um Unternehmen bei Cyber-Attacken schadlos zu halten.

TEXT — Thomas van Zütphen

Herr Backofen, der Markt für gemanagte Sicherheitslösungen – wie die Bereitstellung von SOCs – boomt. Warum?
Kunden haben nicht die Ressourcen, der enormen Geschwindigkeit von neuen Technologien und der Komplexität der vielen Lösungsanbieter im Security-Markt noch adäquat zu folgen. Diese neuen Technologien werden aber im Zweifel von Hackern sehr schnell für Cyber-Attacken genutzt. Das heißt, Unternehmen brauchen einen starken Partner, der in unterschiedlichsten Technologie-Feldern viel Know-how mitbringt, um ein möglichst vollständiges Cybersecurity-Schutzschild anbieten zu können. Wir als Telekom sind dieser starke Partner. Wir können das. Seit 20 Jahren schützen wir nicht nur uns selbst, sondern große Teile der deutschen Wirtschaft und der öffentlichen Hand.

Was wird sich durch die Bündelung Ihrer konzernweiten Security-Ressourcen zur Telekom Security ändern?
In einem Zeitalter, in dem jedes kleinste Gerät schon zum Supercomputer mutiert und alle Geräte miteinander verbunden werden, haben wir eine Welt der Everything-Konnektivität geschaffen. Dafür brauchen wir nun auch eine Everything-Security. Das ist ein Brocken. Um dieses Ziel zu erreichen, bündeln wir das Know-how unserer aktuell 1200 Spezialisten in einer leistungsfähigen, agilen Business Unit und investieren so unmittelbar in den Schutz unserer Kunden. Allein ihre Eigensicherung mit den weltweit besten verfügbaren Lösungen am Markt lässt sich die Telekom selbst etwa 250 Millionen Euro pro Jahr gruppenweit kosten. Und das wird naturgemäß jedes Jahr mehr. Dahinter stecken viel Expertise, Management und Organisation. Nichts liegt näher, als auch unsere Kunden von diesem Investment direkt profitieren zu lassen.

Dirk Backofen, Leiter des Konzerngeschäftsfelds Telekom Security.

Welchen Ansatz verfolgt die Telekom Security dabei konkret?
Vor allem den, Security für Kunden einfach zu machen. Bequem, handlich, übersichtlich – aber dennoch hochsicher. Und das immer mit dem Ansatz „Zero Impact“. Wir können Cyber-Attacken niemals verhindern, aber deren Auswirkungen.

Sie haben das Stichwort angesprochen: Security gilt vielen Firmen nicht nur als kompliziert, sondern auch als teuer. Was ist Ihre Antwort darauf?
Dass das nicht stimmt! Natürlich kostet Sicherheit Geld. Aber sie sofort im Kontext von Sparen zu sehen ist im ersten Schritt falsch. Tatsächlich hilft Security, wenn man sie richtig installiert und orchestrieren kann, viel teurere Schäden zu vermeiden. Und dann wird Security auch als richtige und wichtige Investitionsentscheidung verstanden. Auf die Frage vieler Unternehmensverantwortlicher, „Wo sollte ich sinnvollerweise investieren?“, hat Telekom-Chef Tim Höttges einen deutlichen Ratschlag gegeben: „Liebe CEO-Kollegen, wenn es um Cybersecurity geht, hört nicht auf eure CFOs, sondern hört auf eure Nerds.“ Diese Auffassung teile ich zu 100 Prozent.

Zurück zu den SOCs – warum bauen Sie die Landschaft Ihrer Security Operation Center aus?
Wir haben schon eine Reihe spezialisierter SOCs in Bad Kreuznach, Kiel und Leipzig – aber auch Ungarn, der Slowakischen Republik, aber auch in Südafrika. Unser neues, modernes SOC in Bonn wird vom Herbst an das Know-how der verschiedenen SOCs in der Vielzahl der Telekom-Netze zur proaktiven Gefahrenabwehr koordiniert nutzen. Dazu werden wir es erstmals als integriertes Cyber Defence und Security Operation Center gestalten, in dem dann die Telekom als ein Mandant neben den Mandanten unserer Kunden – immer gemäß derer vereinbarten SLAs – von der Erfahrung unserer Cyber Security Spezialisten und Threat Analysten profitieren können Ein Beispiel dafür sind unsere Use-Cases, für die wir verschiedenste Analyseverfahren einsetzen. So können wir Threat Intelligence mit kognitiven Sicherheitstechnologien verknüpfen. Auf diese Weise werden auf Basis künstlicher Intelligenz und Data Mining neue Services bereitgestellt, mit denen wir die Kommunikation der „Schädlinge“ blockieren können. Wir wissen also immer, was gerade bei Hackern en vogue ist und versuchen denen bei unseren Kunden immer einen Schritt voraus zu sein.

dirk.backofen@t-systems.com

Fotos: Dominik Pietsch

Alte Meister. Im Bespielen der Instrumente, die Wirtschaftsspione und ihre „Einsatzmittel“ auffliegen lassen, sind die Experten des Lauschabwehrteams der Telekom jahrzehntelang geschult – vom Hochfrequenz-Spektrum-Analyzer über Videoendoskope bis zu Halbleiterdetektoren.

Die Klaviatur des Bösen.

Trotz boomender Cyberkriminalität hat die klassische Wanze Hochkonjunktur. In ausgefeiltesten, leistungsstarken Varianten. Um seine Kunden vor Angriffen zu schützen, arbeitet das BSI-zertifizierte Lauschabwehrteam der Deutschen Telekom mit dem Cutting Edge weltweit verfügbarer Abwehrtechnologien.

TEXT —— Thomas van Zütphen

Manchmal sind Fachleute einfach uneins. Bei der Einschätzung zum Beispiel, welche Schäden Wirtschaftsspionage in Unternehmen Jahr für Jahr verursacht. Mindestens 50 Milliarden Euro, sagt der Bundesverband der Deutschen Industrie. „Mit eher 100 Milliarden“ rechnet der Verein Deutscher Ingenieure VDI. Unbestritten steht hingegen Folgendes im Raum: Jetzt, hier und heute sind acht Prozent aller deutschen Unternehmen verwanzt*. Mit Objektiven, Mikrofonen, Sendern, SIM- oder SD-Speicherkarten. Die, einmal verbaut, wo sie mit Strom versorgt werden, nicht selten jahrelang unentdeckt bleiben.

Bei Firmen mit mehr als 500 Mitarbeitern, so eine BITKOM-Studie, werde sogar jedes zehnte Unternehmen hierzulande abgehört. Natürlich nicht flächendeckend. Mitunter nur in einem einzigen Raum. Und dort irgendwo versteckt, hinter 40 Quadratmeter Deckenverkleidung vielleicht. Oder 30 Meter umlaufender Teppichleiste. Dem Konferenztisch. Whiteboard, Stehlampe, Monitor, Telefonspinne, WLAN-Router, Rauchmelder, Steckdose, Netzwerkkabel, USB-Anschluss oder an einem nur stecknadelkopfgroßen i-Punkt im Branding der Raumklimasteuerung. Gleich rechts neben der Tür. Haben Sie’s bemerkt?

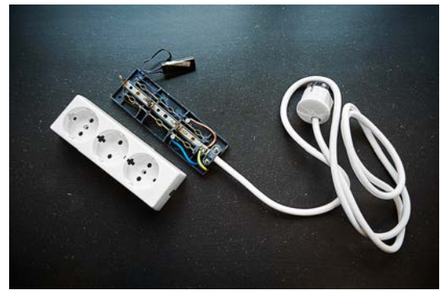
Die heute zumeist winzigen Abhörsysteme auffliegen zu lassen erfordert buchstäblich konzentrisches Arbeiten. Von der fassadenbreiten Fensterfront „runter“ zum Drehgelenk jeder einzelnen Jalousie. Denn den für Spionagezwecke vollkommen ausreichenden Audio- oder Videoinstallationen bietet schon die kleinste Herberge Platz. Die Spitze einer Kugelschreibermine zum Beispiel. Wo man doch unbedarft einfach vermuten könnte, das Schreibgerät sei schlicht vom Vortag liegen geblieben.

Elektronischer Hausfriedensbruch hat Konjunktur

Dabei sind das nur die nicht auf Anhieb, aber doch grundsätzlich sichtbaren „Mittel zum unberechtigten Informationsabfluss“. Deutlich perfider und sehr beliebt bei Wirtschaftsspionen ist es, mit einem Laser-Doppler-Vibrometer durch Fensterscheiben akustische Schwingungen aufzunehmen. Um anschließend de facto Schallwellen auch über größere Entfernungen hinweg via Infrarotlaser zu entschlüsseln.

„Das ist schon High-Performance“, berichtet Jens Bolte, Leiter Executive, Event & Eavesdropping Protection der Deutschen Telekom. „Da sind, bei aller moralischen Geringschätzung für ihr Tun, schon absolute Cracks am Werk.“ Deren in Sachen Wirtschaftsspionage veritables Œuvre in Anspruch zu nehmen ist nicht billig. Aber wenn Informationen aus wichtigen Strategiemeetings womöglich neun- bis zehnstellige Investitionsentscheidungen betreffen, ist den Auftraggebern hochgerüsteter Lauscher mitunter nichts zu teuer. Daran ändert auch nichts, dass Internetkriminalität boomt wie nie. Zumal Cybercrime-Defense-Dienstleister Unternehmen an dieser Flanke immer besser schützen können. „Das hält die Konjunktur vom Handwerkszeug klassischer Industriespionage extrem hoch“, so Bolte.

*Quelle: www.bitcom.org



Mikrofone in Steckern und Steckdosen – sie zu enttarnen ist für das Lauschabwehrteam eine der leichteren Übungen. Sie zu verstecken ist das Spionen dennoch immer wieder einen Versuch wert.

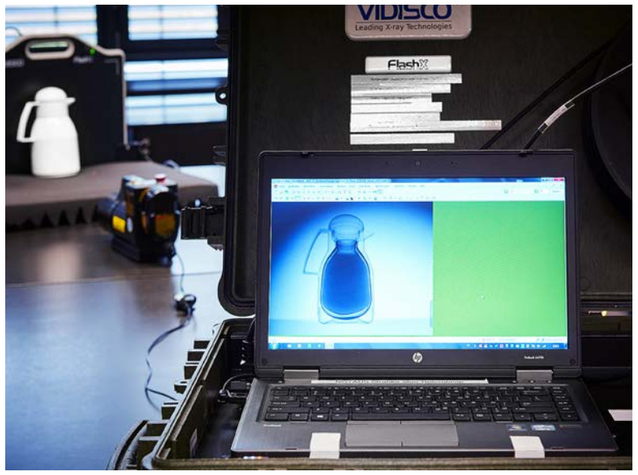
Der Sicherheitsexperte ist Chef der Telekom Lauschabwehr. Einer Spezialeinheit aus Technikern, die allesamt sicherheitsüberprüft sind und seit vielen Jahren im Konzern arbeiten. Wer dazugehören will, hat in der Regel ein Nachrichtentechnik- oder Elektroingenieur-Studium hinter sich und herausragende Kenntnisse im Bereich Funk- und Leitungstechnologie. Nach jahrelanger professioneller Erfahrung in der Lauschabwehr beherrscht jeder im Team die Klaviatur von Spionagehardware so filigran wie nur wenige der Angreifer, die sie einsetzen. Und das ist nur eine Messlatte. Ihren Service „Technical Surveillance Countermeasures“ bietet die Telekom auch den eigenen Kunden an. Bei den vier- bis fünfköpfigen Einsatzteams, mit denen die Lauschabwehr der Telekom ausrückt, ist ein Mitarbeiter schon lange dabei: Horst Glaser. Der 62-Jährige ist Sachverständiger für Abhörsicherheit, von denen es – „öffentlich bestellt und vereidigt“ – bundesweit überhaupt nur zwei gibt.

Eine Kunst für sich

Nicht zuletzt aufgrund der Möglichkeit, solch ein hoch qualifiziertes Team zusammenstellen zu können, ist die Telekom der erste und bis heute einzige IT-Security-Dienstleister, der eine vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierte „Lauschabwehr in der Wirtschaft“ anbieten kann. Voraussetzungen dafür sind unter anderem die Implementierung eines auditierten Qualitätsmanagementsystems (QMS), ein positiver Sicherheitsbescheid auch für die Geheimschutzbetreuung und, wie es im Amtsdeutsch der Behörde heißt, „ein Erfüllungsnachweis der fachlichen Anforderungen“ jedes Teammitglieds. Was Letzteres bedeutet, wird jedem klar (das allerdings sind wiederum nur wenige), der das Lauschabwehrteam einmal bei der Arbeit gesehen hat: die virtuose Bedienung aller am Markt verfügbaren Abwehr- beziehungsweise Detektionstechnologien.

Hochfrequenzmessungen zur Funkanalyse zum Beispiel. Also zur Detektion und Lokalisierung von durch Spione eingebrachten technischen Funkeinrichtungen zum Abhören. „Das ist eine Kunst für sich, weil viele Abhörgeräte heute versteckt in Frequenzbändern senden, die auch von

Handys oder Tablets genutzt werden“, erklärt Andreas Nees, Einsatzleiter des Telekom-Teams. Live in concert quasi. So wird mit einem Spektrumanalysator auch noch der kleinste unübliche Ausschlag von Frequenzwellen registriert und lässt die Abwehrexperten sofort hellhörig werden. Zur sechs bis sieben Zentner schweren Spezialausrüstung, mit der Nees und seine Kollegen bei Kunden anreisen, gehören auch hochempfindliche Wärmebildkameras, die Mobilfunksender aufstöbern, sobald deren Hitzeabstrahlung sie auf den Displays der Kameras als tiefroter Fleck enttarnt. Ebenso zählen Halbleiterdetektoren, Videoendoskope und eine Röntgenkamera, die noch durch 40 Millimeter dicken Stahl tief blicken lässt, zum Besteck der Lauschabwehrer.



Alles, was zur beweglichen Ausstattung eines Konferenzraums und der dort stattfindenden Meetings gehört, wird von Röntgenkameras durchleuchtet. Diese Kaffeekanne ist wanzenfrei.

Das ganze Orchester verfügbarer Abwehrtechnik

„Neben der Detektion optischer Systeme im sichtbaren und unsichtbaren Bereich zählt auch das Aufspüren inaktiver Abhöreinrichtungen, die ihre gesammelten Informationen oftmals erst zeitversetzt über WLAN an ihren unbefugten originären ‚Installateur‘ übertragen, zu unserem Repertoire“, erklärt Horst Glaser. Gleiches gilt für die beschädigungsfreie Überprüfung nicht zu öffnender Gegenstände und technischer Geräte. Doch Glaser weiß, „dass jedes Cleaning eines Raums nur so lange hält und zuverlässig bleibt wie fortan dessen lückenlose Kontrolle“. Einmal gecheckt, werden deshalb alle Geräte und Einrichtungen eines Raums auf Wunsch versiegelt. Dabei bekommt jedes nicht mehr zerstörungsfrei zu entfernende Siegel eine zur Identifizierung eindeutige Nummer. Für böswillige Spione quasi die Signatur der Künstler.

Für den „Sweep“, das Säubern eines Standardbüros mit einer Größe von maximal 30 Quadratmetern und zwei Arbeitsplätzen, kalkuliert das Reinigungsteam etwa drei Stunden. Allerdings, so Jens Bolte, „ist dann die Nachhaltigkeit jeder Aktion stark von der Wirksamkeit des Sicherheitskonzepts des Kunden abhängig“. Besonders vom Zutrittsschutz bestimmter Räume, der festlegt, wer zum Beispiel zur Durchführung von Reinigungsarbeiten oder für ein vorgesehenes Catering berechtigt bleibt, den Raum zu betreten. Denn was nützt ein einmal gesäuberter Raum, wenn bis zum vorgesehenen Meeting anderntags befugte oder unbefugte Mitarbeiter dort beliebig ein und aus gehen können? „Teil unserer Überprüfung ist darum immer auch die Bewertung des Sicherheitskonzepts und die Abgabe von Empfehlungen in einem Revisionsbericht“, so Jens Bolte.

VARIABLE FAKTOREN
Die Preise für eine Lauschabwehrüberprüfung durch das BSI-zertifizierte Team der Telekom sind von mehreren Faktoren abhängig: Größe des Raums, Ausstattung, Beschaffenheit von Boden, Decke und Wänden, Zeitpunkt der Überprüfung (werktags, nachts, Wochenende) und Ort (In- oder Ausland).

Kluge Unternehmen bauen vor

Wie schnell das in Darmstadt ansässige Lauschabwehrteam bei einem Kunden eingreifen kann, ist abhängig von der Auslastung zum Zeitpunkt der Anfrage. Im Idealfall kann eine Überprüfung sofort oder je nach Entfernung am nächsten Tag durchgeführt werden. Allerdings – die „Ticket-Nachfrage“ steigt. Genaue Angaben zur Zahl ihrer Einsätze oder der Klientel, die ihren Service in Anspruch nimmt, macht die Telekom naturgemäß nicht. Das ist Teil einer Vertraulichkeitserklärung, die das Team vor Beginn einer Untersuchung unterschreibt. Dazu zählt auch – Stichwort „gewohntes Verkehrsaufkommen“ auf den Unternehmensfluren zum Beispiel –, dass das Lauschabwehrteam je nach Wunsch des Kunden im unauffälligen Overall x-beliebiger Servicetechniker auftaucht oder auch mal im feinen Zwirn der üblichen Vorstandsetagenbesucher.

Zur garantierten Absicherung eines einmal abhörgesicherten Raums bietet das Lauschabwehrteam seinen Kunden auch eine Konferenzbegleitung an. Nach einem Statusscan von Funkfrequenzen zu Beginn eines Meetings lassen sie während der kompletten Sitzung in einem Nebenraum permanent einen Vergleichsscan laufen. So lassen sich gegebenenfalls Abhöreinrichtungen feststellen, die erst nach Beginn der Veranstaltung – von ebenso willigen wie ungebetenen Mithörern – remote eingeschaltet oder buchstäblich serviert werden. In einer Kaffeekanne zum Beispiel.

„Internetkriminalität boomt. Trotzdem hat das Handwerkszeug klassischer Industriespionage Hochkonjunktur.“

JENS BOLTE,
Leiter Executive,
Event & Eavesdropping Protection

jens.bolte@telekom.de
www.t-systems.de/telekom/lauschabwehr
security.t-systems.de
www.t-systems.de/video/lauschabwehr

INTERVIEW

„Schon eine Spur reicht.“

Dr. Alexander Schinner, theoretischer Physiker und Senior Cyber Security Consultant bei T-Systems, über die forensische Erfassung, Analyse und Auswertung digitaler Spuren und die Vorsorge, die Unternehmen mit Blick auf Cyberangriffe treffen können.

TEXT —— Thomas van Zütphen

Herr Dr. Schinner, wer sind Ihre Kunden?
Was sie eint, ist Angst um das eigene Unternehmen oder sogar Panik. Das sind aber völlig normale Reaktionen. Denn fast immer entstammen unsere Anrufer, und übers Telefon erfolgt der erste Kontakt, einer von zwei Gruppen: Entweder hatten sie ihrer Sicherheitsarchitektur vollständig vertraut oder, oft aus Kostengründen, darauf gesetzt, dass es sie nie erwischen würde. Je länger Letzteres gut geht, desto perplexer ist man, wenn diese Kalkulation schlagartig in unbekannten Kanälen versickert. Vor allem für Konzerne, Betreiber kritischer Infrastrukturen und die Hidden Champions unseres Mittelstands gilt: Es ist schlichtweg illusionär anzunehmen, dass es nur einen Tag in der Woche geben könnte, an dem man nicht angegriffen wird.

Wozu raten Sie im ersten Schritt?
Ruhe zu bewahren. Und zwar aus zwei Gründen: Ein falscher erster Schritt kann sämtliche Spuren beseitigen und eine übereilte Reaktion, etwa meinen kompletten Betrieb auszusetzen, den Schaden nur noch größer machen. Aber, noch mal, am wichtigsten für unsere Arbeit ist: nichts zu verändern und den Tatort quasi abzusperren. Nur dann können wir sichergehen, dass bis zu unserem Eintreffen keine Spur verwischt wird.

Ist IT-Forensik also Detektivarbeit?
Der Vergleich passt. Bei Sherlock Holmes reichen die Beweismittel beziehungsweise Spuren von der Leiche bis zur Zigarettenasche. Bei uns sind sie nur eben digital. Und für Angreifer ist es sehr sehr schwierig, überhaupt keinen Fehler zu machen und nicht wenigstens eine Spur zu hinterlassen. Und eine davon reicht.

Wie sieht Ihre Spurensicherung praktisch aus?
Im Grunde relativ standardisiert. Zunächst einmal: zuhören und Fragen stellen. Dann werden Logfiles und verschiedene andere Daten gesichert und mitunter die Personalvertretung eingeschaltet, weil gegebenenfalls Innentäter oder deren Hardware ausgeschlossen oder identifiziert werden sollen. Erst dann geht’s an den Tatort.

Und dort passiert was?
Je nachdem, wonach wir suchen. Galt der Angriff einem Mitarbeiterrechner oder einem Server, kam er von außen oder von innen? Tatsächlich wird zunächst einmal alles fotografiert, um hinterher so simple Fragen beantworten zu können wie: Wo steckte welches Kabel? Dann erstellen wir eine vollständige forensische Kopie der Festplatte oder sichern gleich das ganze Laptop.

Und dabei spielt keine Rolle, ob Innen- oder Außentäter?
Selbstverständlich. Den Unterschied macht, was der Kunde erreichen will. Es ergibt ja wenig Sinn, einen Angreifer in China zu identifizieren. In dem Fall will der Kunde von uns wissen: Was haben die Angreifer getan, wie konnten sie reinkommen, welche Verluste habe ich erlitten, und wie setze ich sie wieder vor die Tür? Anders ist es, wenn sich der vermeintlich chinesische Angreifer als Kollege Meier aus der Buchhaltung entpuppt. Dann lohnt es, den Täter zu identifizieren und ihn vor Gericht zu bringen. Ein essenzielles Element der IT-Forensik ist, dass die von uns sichergestellten digitalen Beweismittel gerichtsverwertbar sind und auch alle nachfolgenden Aktivitäten von uns lückenlos dokumentiert einer juristischen Auseinandersetzung standhalten. Ansonsten könnte das Gericht bei einem Prozess ein Beweismittel ablehnen.

Was braucht es dafür?
Aufseiten eines echten IT-Forensikers, und davon gibt es sehr wenige in Deutschland, Konzentration, Disziplin und Akribie. Wir zerstören keine Beweismittel, wenn wir am Betriebssystem vorbei sehr tief in Vorgänge und Systeme schauen. Gab es irgendwas im Netz oder auf den Rechnern, was sich womöglich anders als üblich verhalten hat? Tauchen Daten auf, wo sie nicht hingehören? Oder gab es Mitarbeiter, die kurz vorher gekündigt und mit Daten hantiert haben? Aus diesem Puzzle von Einzelteilen können wir uns schon am Tatort oder in unserer Laboranalyse ein sehr gutes Gesamtbild machen.

Das heißt, es geht um mehr als nur Hardware?
Korrekt, Hardware allein sichert nicht. Die Sicherheitsarchitektur aus Hardware, Software, Services, Organisation und Planung ist der eigentliche Tatort, an dem wir suchen. Denn oft ist der Mitarbeiter, dessen Rechner wir als Angriffswaffe enttarnen, selbst das Opfer.

alexander.schinner@t-systems.com
www.t-systems.de/video/interview-schinner

Fotos: Dominik Pietsch, Foto Sexauer

Quantensprung mit Risiko.

Quantencomputer könnten viele Bereiche der Forschung revolutionieren. Die Entwicklung treibt Sicherheitsexperten jedoch Sorgenfalten auf die Stirn: Der neue Megarechner, den Wissenschaftler schon in absehbarer Zeit erwarten, könnte viele Verschlüsselungen im Handumdrehen knacken. Unternehmen droht der Verlust sensibler Daten.

Illustration: Knut Niehus/ddp images

TEXT —— Jan Ungruhe

Das Szenario ist düster: Mit einer enormen Rechenleistung knackt ein Quantencomputer in wenigen Augenblicken viele etablierte Verschlüsselungsmethoden, wozu herkömmliche Computer heute noch Milliarden Jahre Rechenzeit benötigen. Auch in der Adresszeile des Browsers steht dann das s im Kürzel https nicht mehr für sicher, sondern für schutzlos. Passwörter und andere sensible Daten im Internet zu übertragen, etwa beim Onlinebanking, könnte zum Hochsicherheitsrisiko werden – für Privatpersonen und Unternehmen gleichermaßen.

Aussichten, die in ferner Zukunft liegen? Mitnichten, sagen zahlreiche Wissenschaftler. Bislang existiert ein solcher Megarechner zwar lediglich in der Theorie. Die Forscher halten es aber durchaus für möglich, dass der Internetkonzern Google seinen Quantenchip mit 50 Qubits schon Ende 2017 vorstellt.

Security-Forscher suchen daher fieberhaft nach einem Gegenmittel gegen die neuen Superhacker. Und die Fahndung wird umso dringlicher, da offenbar auch die NSA (National Security Agency) bereits an einem Megarechner tüftelt, der die Quantenmechanik nutzt und Spähangriffe selbst auf Regierungen oder Behörden ermöglichen würde. Das berichtete die „Washington Post“ unter Berufung auf den ehemaligen Angestellten des US-Geheimdienstes Edward Snowden bereits 2014.

Datenverkehr heute schon gefährdet

Wissenschaftlern zufolge sollten Unternehmen möglichst bald auf neue Verschlüsselungsverfahren der Post-Quanten-Kryptografie umsatteln. Denn bereits der heutige Datenverkehr ist womöglich gefährdet. So könnten Hacker sensible Informationen jetzt verschlüsselt abfangen und speichern, um sie dann in zehn Jahren – oder früher – durch einen Quantencomputer nachträglich knacken zu lassen. Weit hergeholt ist das nicht: Die NSA zum Beispiel darf verschlüsselte Daten so lange aufbewahren, bis sie sie knacken kann.

Eine abwartende Haltung könne für Unternehmen teuer werden, warnt Dr. Enrico Thomae, Post-Quantum-Experte der operational services GmbH, eines Joint Venture von Fraport und T-Systems. „Unternehmen sollten kritische Assets identifizieren und die Anforderung der Langzeitsicherheit in ihre Risikoanalyse aufnehmen, um Informationen mit einem Geheimhaltungshorizont von fünf bis 15 Jahren zu schützen.“ Ignorierten Unternehmen diese Gefahr, könne es für Systeme mit langer Lebensdauer wie Autos oder Kühlschränke zu teuren Nachrüstungen oder Rückrufaktionen kommen.

Größere Schlüssellängen erforderlich

Der Kryptografieexperte empfiehlt, für symmetrische Algorithmen wie AES (Advanced Encryption Standard) eine Länge von 256 Bit zu wählen. Auch bei asymmetrischen Algorithmen verschaffen größere Schlüssellängen einen zeitlichen Puffer. Spezialisten zufolge ist eine Renaissance des Verschlüsselungsverfahrens RSA (Rivest, Shamir und Adleman) mit sehr großen Schlüssellängen möglich. Denn um diese zu knacken, müssten wiederum entsprechend größere Quantencomputer entwickelt werden. Unternehmen könnten künftig aber auch hybride Verfahren einsetzen, also eine aktuelle Verschlüsselungsmethode mit einem neuen Post-Quantum-Algorithmus kombinieren.

Damit der Datenverkehr im Quantenzeitalter nicht entschlüsselt werden kann, wird die Suche nach kryptografischen Verfahren weltweit vorangetrieben. Die EU-Kommission fördert etwa das 2015 gestartete Projekt PQCrypto (Post-Quantum Cryptography) mit 3,9 Millionen Euro. Beteiligt sind Universitäten und Unternehmen aus elf Ländern, darunter die Ruhr-Universität Bochum und die TU Darmstadt. Die Forscher prüfen bekannte Post-Quantum-Algorithmen auf ihre Sicherheit und Anwendbarkeit und optimieren sie zum Beispiel für das TLS-Protokoll. Mit finalen Ergebnissen wird Ende 2018 gerechnet. Parallel dazu startete die US-Bundesbehörde NIST (National Institute of Standards and Technology) einen öffentlichen Auswahlprozess, für den Wissenschaftler noch bis Ende 2017 Algorithmen einreichen können.

Für Attacken neuer Art will auch Google gerüstet sein und experimentiert in seinem Webbrowser Chrome mit einem Post-Quantum-Algorithmus, der auf den Namen New Hope getauft wurde. Die Deutsche Telekom hat derweil gemeinsam mit der südkoreanischen SK Telecom eine Initiative für eine sichere Kommunikation in Zeiten des Quantencomputers angestoßen und die Quantum Alliance gegründet. Die Telekommunikationsunternehmen testen sowohl Post-Quantum-Algorithmen als auch neue Kryptoalgorithmen, die ausschließlich auf Quantencomputern laufen. „Mit der Quantum Alliance setzen wir uns an die Spitze einer technischen Entwicklung, die die IT revolutionieren wird: Wir sorgen mit dafür, dass Kommunikation sicher bleibt, wenn in der Quantenforschung der Durchbruch gelingt und die ersten Rechner auf den Markt kommen“, sagt Claudia Nemat, Vorstand Technologie und Innovation der Deutschen Telekom.

Forschung profitiert

Von einem Megarechner würden vor allem viele Bereiche der weltweiten Forschung nahezu aller Disziplinen profitieren. So ließen sich zum Beispiel medizinische Forschungsprogramme massiv forcieren, Optimierungsprobleme lösen, Suchalgorithmen beschleunigen und große Datenbestände schnell durchforsten. Die Schreckensszenarien des Missbrauchs durch Hacker blieben damit wieder einmal das, als was sie sich in zahlreichen innovativen Technologiefeldern entpuppen: Randerscheinungen – mit einem jedoch nicht zu unterschätzenden Gefährdungspotenzial.

enrico.thomae@o-s.de
www.t-systems.de/telekom/quantum-alliance
www.t-systems.de/verschluesselung
www.t-systems.de/loesungen/verified-security

638

Ziffern lang ist der öffentliche PayPal-Schlüssel. Das entspricht 2048 Bit.

Achillesferse Digitalisierung

Für einige Kliniken war es wie eine Reise in die Vergangenheit: Anfang 2016 legte ein Computervirus mehrere Krankenhäuser in Nordrhein-Westfalen fast vollständig lahm. Statt mit dem Rechner arbeitete das Klinikpersonal plötzlich wieder mit Papier und Bleistift. Dabei erwischte es ausgerechnet Einrichtungen, die als Vorreiter in Sachen Digitalisierung gelten.

KLEINER VIRUS – GROSSE WIRKUNG

Die Krankenhäuser, die Anfang 2016 Opfer des Ransomware-Angriffs wurden, arbeiten weitgehend digital. Mithilfe moderner und innovativer IT-Lösungen optimieren sie die Klinikprozesse und bieten gleichzeitig ihren Patienten eine bestmögliche Versorgung. Doch ausgerechnet diese weitgehende Digitalisierung machte die Einrichtungen zum Angriffsziel: Cyberkriminelle hatten Schadsoftware über den E-Mail-Server eingeschleust, die nach und nach die komplette IT der betroffenen Kliniken lahmlegte. Mit fatalen Folgen: Innerhalb weniger Stunden waren die hoch digitalisierten Einrichtungen nahezu handlungsunfähig.

TEXT —— Silke Kilz

Doch genau da liegt der Hund begraben: Mit der zunehmenden Vernetzung und Mobilität wächst auch die Angriffsfläche für Cyberkriminelle. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stuft die Gefährdungslage durch Erpressungstrojaner (Ransomware) als hoch ein. Zwar gibt es bisher kaum offizielle Zahlen, doch in einer Umfrage haben 78 von 89 befragten Gesundheitseinrichtungen im Jahr 2016 derartige Angriffe verzeichnet.

Unterschätztes Sicherheitsrisiko

Wirklich überraschend ist das nicht. Denn um im Klinikalltag reibungslose und effiziente Abläufe zu ermöglichen, sind Themen wie Mobile Computing, Cloud-Anwendungen oder das Internet der Dinge auch aus dem Gesundheitsbereich inzwischen nicht mehr wegzudenken. So gehen die Ärzte und Pflegekräfte des Robert-Bosch-Krankenhauses in Stuttgart schon lange nicht mehr mit Papierakten zur Visite. Stattdessen tragen sie iPad mini bei sich, auf denen sie alle diagnose- und pflegerelevanten Daten sofort aus dem zentralen Krankenhausinformationssystem (KIS) iMedOne® abrufen können. Direkt am Krankenbett erklären die Ärzte ihren Patienten den Behandlungsverlauf, rufen Untersuchungsergebnisse ab oder erfassen neue Informationen, beispielsweise Änderungen in der Medikation. Mit einem ähnlichen System arbeitet auch das Universitätsklinikum Jena. Hier hat die Telekom eine mobile Variante des KIS i.s.h.med von Cerner installiert. Eine andere mobile Lösung ist am St. Joseph Krankenhaus in Berlin im Einsatz. Hier vereinbaren die Patientinnen der Geburtshilfe ihre Termine nicht mehr telefonisch, sondern online über das sichere Patientenportal der Telekom.

Was viele Kliniken allerdings unterschätzen: Wer solche digitalen Lösungen einsetzt, muss sie auch entsprechend absichern. „Meist verfügen die Krankenhäuser über den Grundschutz mit Anti-Viren-Programmen und Firewall, aber nicht sehr viel mehr“, sagt Thorsten Holz, Professor für Systemsicherheit an der Ruhr-Universität Bochum, in einem Gespräch mit der Wochenzeitschrift „Die Zeit“. Neben dem fehlenden Risikobewusstsein scheuen Krankenhäuser oft auch die Mühen und Kosten einer Sicherheitslösung.

27 %

aller Hackerangriffe im ersten Halbjahr 2016 galten dem Gesundheitswesen (computerwelt.at).

Mehr als Firewall und Virenschutz

Dabei muss ein wirksamer Schutz gegen Cyberangriffe weder komplex noch teuer sein. Das zeigt das Beispiel des Robert-Bosch-Krankenhauses. Hier haben die IT-Verantwortlichen gemeinsam mit den Experten von T-Systems ein Sicherheitsinformations- und Ereignis-Management (SIEM) des Telekom-Partners AlienVault installiert. „Die SIEM-Lösung dient dazu, mögliche Gefahren frühzeitig zu erkennen – und zwar bevor das Kind in den Brunnen gefallen ist“, erklärt Sascha Müller, stellvertretender IT-Leiter des Stiftungskrankenhauses. Dazu sammelt das System an verschiedenen Stellen Millionen von sicherheitsrelevanten Log- und Eventdaten, setzt diese miteinander in Beziehung und erkennt daraus in Echtzeit bestimmte Trends und Muster. Sobald auffällige Abweichungen vom Normalzustand auftreten, löst das System einen Alarm aus. Auf diese Weise haben die IT-Experten die Chance, bereits zu einem sehr frühen Zeitpunkt Gegenmaßnahmen zu ergreifen. Müller verdeutlicht die Funktionsweise anhand eines Beispiels: „Wenn im Active Directory, dem Verzeichnisdienst von Microsoft Windows Server, ein neuer Admin-User angelegt wird und gleichzeitig der Netzwerkverkehr zunimmt, könnte das ein Indiz für einen zielgerichteten Angriff sein.“

HANDLUNGSDRUCK DURCH IT-SICHERHEITSGESETZ

Nach dem seit Juli 2015 gültigen Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) müssen Betreiber kritischer Anlagen künftig ein Mindestniveau an IT-Sicherheit einhalten. Der erste Teil der Kritis-Verordnung zur Umsetzung des IT-Sicherheitsgesetzes ist am 3. Mai 2016 in Kraft getreten. Er richtet sich an die Sektoren Energie, Informationstechnik und Telekommunikation, Wasser sowie Ernährung. Im Frühjahr 2017 wird nun auch der zweite Teil der Verordnung erwartet. Dieser betrifft die Sektoren Transport und Verkehr, das Finanz- und Versicherungswesen sowie den Gesundheitssketor und stellt damit auch an Krankenhäuser erhöhte Sicherheitsanforderungen. Unter anderem werden Kliniken dann verpflichtet sein, ihre IT nach dem Stand der Technik angemessen abzusichern und diese Sicherheit mindestens alle zwei Jahre überprüfen zu lassen. Erhebliche IT-Störungen sind künftig umgehend an das BSI (Bundesamt für Sicherheit in der Informationstechnik) zu melden.

Bewährungsprobe bestanden

Ein anderer Fall aus der jüngeren Vergangenheit des Krankenhauses zeigt, dass sich die SIEM-Lösung bereits bewährt hat. Über eine Website hatten ein oder mehrere Angreifer versucht, auf das IT-System des Robert-Bosch-Krankenhauses zuzugreifen. Diese Website war noch auf keiner Blacklist registriert und wies auch keine gesperrten Protokolle auf, sodass sie von der Firewall des Klinikums nicht als kritisch beurteilt wurde. Das SIEM-System stellte fest, dass die besagte Seite erst Stunden zuvor registriert worden war, es sich also möglicherweise um einen Botnetz-Betreiber handelte. Ein Abgleich mit der Open Threat Exchange Community, einer offenen Datenbank digitaler Bedrohungen, zeigte, dass es sich nach Auswertung und Vergleich dieser „indicators of compromise“ tatsächlich um einen Angriff handelte.

Sicherheitspaket aus der Box

„Mit der Lösung von T-Systems und AlienVault haben wir quasi ein vorkonfiguriertes Sicherheitspaket aus der Box gebucht“, sagt Müller. Sensoren und SIEM-Lösung wurden im Rechenzentrum des Robert-Bosch-Krankenhauses installiert und konfiguriert. T-Systems-Cybersicherheitsexperten überwachen von einem Security Operations Center (SOC, siehe Beitrag Seite 22) aus rund um die Uhr alle Systeme, bewerten die Signale bezüglich ihrer Kritikalität und initiieren – wenn nötig – Gegenmaßnahmen. „All das könnten wir mit unserer IT-Abteilung hier vor Ort gar nicht leisten“, so Müller. Ein weiterer Vorteil: Regeln und Aktualisierungen müssen vom Krankenhaus nicht selbst erarbeitet werden, sondern gelangen aus der Kooperation von Telekom und der Community mit Open Threat Exchange auf die Plattform. „So steht das Wissen um aktuelle Sicherheitsbedrohungen rasch auch anderen Unternehmen zur Verfügung“, sagt Müller.

bernd.koenig@t-systems.com
www.t-systems.de/telekom-healthcare/cyber-defense

Keine Chance für Autohacker.

Lange Zeit war es eine der letzten Bastionen der nicht vernetzten Welt. Heute fährt das Auto als rollender Rechner mit Internetzugang über die Straße. Damit gerät es auch ins Visier von Hackern. Die Automobilindustrie hat die Gefahr erkannt – und rüstet ihre Produkte gegen Cyberangriffe auf.

TEXT —— Yvonne Nestler

Mitten auf dem Highway funktioniert das Gaspedal nicht mehr. Fluchend schaltet Andy Greenberg das Warnlicht an, während sein Jeep Cherokee immer langsamer wird und die Autos an ihm vorbeirauschen. Der „Wired"-Redakteur kann nichts tun – sein Fahrzeug ist Opfer einer Hackerattacke. Die beiden Hacker, Charlie Miller und Chris Valasek, sitzen zehn Meilen entfernt vor einem Laptop – und haben den Jeep unter ihrer Kontrolle: Erst dröhnte das Radio los, dann vernebelte die Scheibenwaschanlage die Sicht, und jetzt kann Greenberg nicht mehr beschleunigen. Erst als er den Wagen neu startet, ist der Spuk beendet.

Obwohl das Ganze nur ein Experiment und Greenberg vorgewarnt war, erregte die Aktion im Juli 2015 weltweit Aufmerksamkeit. Denn sie zeigte erstmals deutlich die Kehrseite vernetzter Autos: Ohne vernünftigen Schutz können Cyberkriminelle sie auch aus der Ferne knacken und übernehmen. Bisher mussten Hacker zum Beispiel dem Autofahrer eine Musik-CD mit einem Trojaner unterjubeln oder aus ein paar Meter Entfernung die ungesicherte Bluetooth-Verbindung kapern. Heute jedoch sind viele Autos direkt ab Werk mit dem Internet vernetzt und bieten Einfallstore für die Gefahr aus dem Cyberspace. Laut Beratern von Roland Berger galt das bereits 2015 für ein Drittel aller Neuwagen. Allerdings weiß kaum ein Autofahrer, dass er bereits heute in einem fahrenden Rechenzentrum sitzt: Ein modernes Fahrzeug verfügt über mehr als 100 kleine Computer in Form von Steuergeräten.

Money, Money, Money

Die Ziele hinter Cyberattacken sind vielfältig. Ein Krimineller möchte ein Auto stehlen, ohne Türen und Fenster mit Gewalt zu öffnen. Ein anderer möchte über die SIM-Karte eines fremden Autos kostenlos im Internet surfen. Und ein dritter macht Fahrzeuge zu Geiseln: Er legt bestimmte Automodelle aus der Ferne lahm und fordert Lösegeld vom Hersteller. Selbst die Geheimdienste strecken ihre digitalen Fühler nach dem Auto aus: Die Enthüllungsplattform WikiLeaks veröffentlichte Anfang März 2017 ein Dokument, laut dem die CIA im Oktober 2014 überlegte, Autos und Lastwagen zu infizieren. Vielleicht um die Position

Foto: Navid Baraty

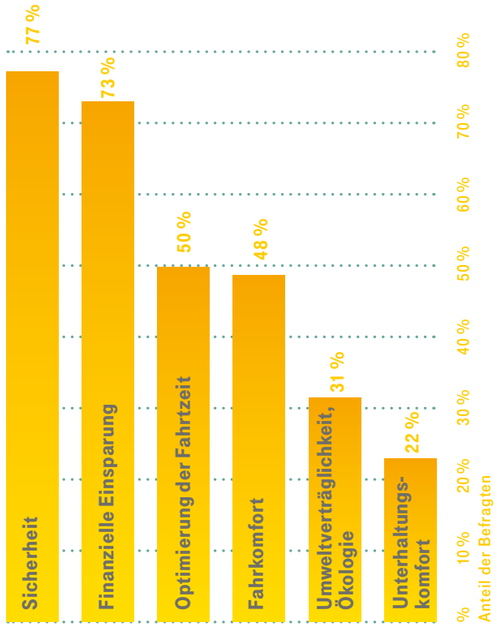
einer Zielperson zu überwachen oder deren Gespräche während Autofahrten abzuhören.

„Am beunruhigendsten ist die Möglichkeit, dass sich Terroristen in autonome Antriebssysteme hacken könnten und Unfälle verursachen, die eine bestimmte Einzelperson oder viele Menschen töten“, schreibt das Beratungshaus PricewaterhouseCoopers (PwC) in seiner „Connected Car Study 2015“. Noch ist das nicht geschehen. Bisher gehen die meisten Autohacks auf das Konto von White-Hat- oder Grey-Hat-Hackern, die sich mit ihren Ergebnissen nur profilieren oder die Technik voranbringen wollen. Dennoch: Sicherheit des Menschen geht nicht mehr ohne Cybersicherheit.

Der Blick fürs Ganze

Deswegen arbeitet die Automobilindustrie bereits daran, ihre Barrieren gegen Cyberkriminalität möglichst hoch zu ziehen. „Wenn Industrieentscheider an Informationssicherheit denken, fokussieren sie in der Regel auf In-Car-Systeme als Schwachstelle“, warnt PwC. „Aber die Bedrohung geht weit über die Dashboard-Oberfläche hinaus.“ Die Devise lautet also: nicht nur an das Fahrzeug denken, sondern auch an seine Mobilfunkkommunikation sowie die Backends des Herstellers und möglicher dritter Service-Provider. T-Systems entwickelt deswegen Security-Lösungen für die gesamte IT- und Telekommunikationsinfrastruktur rund um das vernetzte Fahrzeug – und setzt erste Lösungen bereits mit großen Automobilherstellern um.

Um Ende-zu-Ende-Security zu erreichen, sei es besonders wichtig, IT-Sicherheit und Datenschutz bereits in der Planung neuer Fahrzeugmodelle, -bauteile und -software zu berücksichtigen, gemäß dem Grundsatz „Security und Privacy by Design“, sagt Thomas Fischer von T-Systems. Das gilt auch für die Zulieferer – und für die Zulieferer der Zulieferer. Trotz aller Prävention gilt es auszuschließen, dass Hacker Schwachstellen im Umfeld des vernetzten Fahrzeugs entdecken. Deswegen empfiehlt es sich, hinter der Prävention eine zweite Verteidigungslinie im Auto zu etablieren: Detektionssysteme, die sozusagen als „Wachhunde“ dienen und bei Angriffen Alarm schlagen.



WELCHE DREI KRITERIEN SOLLTE EIN VERNETZTES AUTO VOR ALLEM ERFÜLLEN?

Für Autokäufer auf der ganzen Welt ist Sicherheit die wichtigste Eigenschaft vernetzter Fahrzeuge. Entscheidende Voraussetzung hierfür ist IT-Security.

Quelle: Automobilbarometer 2016, Commerz Finanz

82 %

der US-Amerikaner würden nur zögernd oder sogar nie bei einem Autohersteller kaufen, der gehackt wurde.

(Quelle: KPMG AG)

Digitaler Wachhund im Auto

T-Systems hat eine solche Lösung für das Auto entwickelt. ESLOCKS (Embedded Security Locks) heißt der digitale Schnüffler, der direkt im Herzen des Bordnetzes sitzt, im Gateway zwischen den Feldbussen. Dort prüft das Intrusion Detection System alle Nachrichten auf Anomalien. Dabei fiele zum Beispiel auf, wenn der Airbag bei voller Fahrt ausgelöst werden soll. Wie das Fahrzeug auf eine Auffälligkeit reagiert, legt T-Systems gemeinsam mit dem Autohersteller fest – zum Beispiel, dass der Fahrer eine Warnung erhält oder das Fahrzeug manipulierte Funktionen abschaltet. Das Detektionssystem meldet alle Anomalien an ein Backend, das die Daten mit modernen Machine-Learning-Algorithmen untersucht. Die Erkenntnisse fließen an die Systeme in allen Fahrzeugen zurück.

Einen zweiten Wachhund setzt T-Systems auf die Mobilfunkkommunikation von Autos an. „Die Mobilfunkschnittstelle zwischen dem Fahrzeug und dem Fahrzeug-Backend zusätzlich abzusichern stellt einen wichtigen Bestandteil der Ende-zu-Ende-Security-Lösung dar“, sagt Christian Olt von T-Systems. Beispielsweise könnten Kriminelle durch sogenannte Fraud-Attacken die SIM-Karte eines vernetzten Fahrzeugs unrechtmäßig ausnutzen – und Telefonnummern anrufen, die dafür nicht vorgesehen sind. Ein solcher Vorfall ist immer ein starkes Indiz für einen Cyberangriff, denn das Auto besitzt keine Wähltastatur. Also muss es jemand technisch manipuliert haben. Deswegen entwickelt T-Systems derzeit eine Fraud-Detektions-Lösung für Fahrzeuge.

Grenzenlose Security

Für jeden Automobilhersteller analysieren die Security-Experten dafür zunächst, welche Risiken bestehen und wie sich diese detektieren lassen. Dementsprechend passt T-Systems die technische Lösung an: Das Fraud-Erkennungssystem analysiert die Verbindungsdaten der Fahrzeuge mithilfe vordefinierter Regeln, welche Vorfälle als „ungewöhnlich“ einzustufen sind. Ruft ein Auto etwa eine unbekannte Rufnummer an, erhält der Hersteller automatisch eine Benachrichtigung. Parallel dazu steht der Verdachtsfall in einem Onlineportal zur Verfügung. Damit verfügt der zuständige Servicemitarbeiter des Herstellers über alle Informationen, um zu entscheiden, welche Gegenmaßnahme er einleitet. Beispielsweise könnte der Autobesitzer informiert, die SIM-Karte gesperrt oder rechtliche Schritte könnten eingeleitet werden. Welche Daten ein Automobilunternehmen für den Dienst Fraud Detection as a Service rechtlich nutzen darf, vereinbart die Telekom Security in enger Abstimmung mit dem Hersteller und dem Telekom-Datenschutzbereich.

Das vernetzte Auto hat viele Gesprächspartner: sein Backend, andere Fahrzeuge, das Smart Home, die Verkehrsinfrastruktur, Inhalteanbieter, Smartphones und Tablets – nicht zu vergessen die Kommunikation zwischen den im Fahrzeug verbauten Steuergeräten. Gerade die Elektromobilität erhöht die Zahl der Gesprächspartner, etwa zur Ladeinfrastruktur. Um kritische Kommunikation abzusichern, wird diese verschlüsselt und die Gesprächspartner werden authentifiziert. Hierfür benötigt das Auto – heißt: seine relevanten Steuergeräte – eine digitale Identität. Diese besteht aus zwei Schlüsseln, einem öffentlichen und einem privaten, also geheimen. Die Schlüssel hängen mathematisch zusammen. Schickt nun etwa das Backend Daten an das Auto, generiert es mit seinem privaten Schlüssel eine digitale Signatur (quasi seinen Ausweis), die das Auto mit dem öffentlichen Schlüssel des Backends prüft. Damit ist klar, dass die Daten nicht von einem Hacker stammen, also korrekt sind.

1 300 000

Deutsche besaßen 2016 einen Pkw mit einer fest eingebauten Internetverbindung.

Quelle: Institut für Demoskopie Allensbach

Achtung, Quantencomputer!

Für einen Hacker bieten sich bei diesem Vorgehen zwei Angriffspunkte an. Erstens: der mathematische Zusammenhang zwischen den Schlüsseln. Kennt ein Angreifer diesen, kann er aus dem öffentlichen Schlüssel den privaten Schlüssel erzeugen. Daher muss auch die Automobilindustrie den Stand der Technik ständig im Auge behalten und sich – bei Entwicklungszyklen von drei bis fünf Jahren und einer Lebensdauer des Fahrzeugs von 15 bis 30 Jahren – heute schon den Kopf über die Cyberangriffe von morgen zerbrechen. Eine echte Herausforderung, immerhin kündigen sich für die kommenden Jahre bereits neue Supercomputer an, die Quantencomputer, mit denen sich bisherige kryptografische Verfahren wie RSA und elliptische Kurven knacken lassen.

Zweitens: das Fälschen von Schlüsseln. Die Public-Key-Infrastruktur (PKI) der Automobilhersteller schützt den Autofahrer vor solchen Angriffen. Der Autohersteller nutzt seine eigene digitale Identität, um die öffentlichen Schlüssel des Fahrzeugs als echt zu bestätigen.

Zentrum des Vertrauens

Sobald ein Auto mit Fahrzeugen anderer Hersteller, mit Ampeln und Bahnschranken spricht, stellt sich eine neue Herausforderung: Die Gesprächspartner müssen sich auf eine gemeinsame, herstellerunabhängige Vertrauensinstanz (Trust Center) einigen, die ihre digitalen Identitäten bestätigt und somit für sichere Kommunikation sorgt. „Die Deutsche Telekom hat seit 1994 ein Trust Center, das von der Bundesnetzagentur akkreditiert ist“, sagt Mark Großer von Detecon. „Dort betreiben wir Public-Key-Infrastrukturen zum Beispiel für Industrieunternehmen, Behörden und Länder.“

Gartner[1] prognostiziert für 2020, dass weltweit etwa 61 Millionen vernetzte Neuwagen – entweder mit eingebauter Konnektivität oder über verbundene Mobilgeräte – gebaut werden. Für die Automobilbranche hat das Thema IT-Sicherheit aber bereits heute hohe Priorität. Das zeigen Initiativen wie AUTOSAR und EVITA, die an Standards für Steuergerätesoftware und sichere Bordnetze arbeiten sowie für erste Prämienprogramme von Autoherstellern für gemeldete Sicherheitslücken.

thomas.fischer@t-systems.com
www.t-systems.de/whitepaper/car-security
www.t-systems.de/connected-car-security

[1] Gartner Press Release: „Gartner Says Connected Car Production to Grow Rapidly Over Next Five Years“, September 2016, http://www.gartner.com/newsroom/id/3460018

Fix ohne Handbuch. Im Innovation Center verproben Experten wie Wearables als Smart Watch, Sensorhandschuh, Scanner und AR-Brille Servicetechniker durch eine Reparatur führen.

Irgendwie naheliegend.

Eine Hightech-Werkstatt voll mit Freiräumen, Spielräumen, Denkräumen. Wie Kunden des Innovation Center München gemeinsam mit T-Systems und deren Partnern aus Wirtschaft und Forschung Lösungen, Ideen und Projekte prototypisieren und weiterentwickeln.

TEXT —— Thomas van Zütphen

Wo entstehen bei der Telekom und T-Systems eigentlich Innovationen? In der Design Gallery in Bonn natürlich, den futuristischen Showrooms für die Kommunikationsmöglichkeiten von morgen. Oder den T-Labs in Berlin, die mit ihrer ICT-Forschung dem Hier und Jetzt von Unternehmensproblemen immer ein Stück voraus sind. Aber hier, abgelegen in der nördlichen Peripherie von München? Was aussieht wie ein schlichter Zweckbau mit fast 200 Meter langer Fassade, beherbergt neben einem Rechenzentrum tatsächlich die Geschäftskunden-Innovationsschmiede Nummer eins – etwas bescheidener und präziser: ein Center für die Verbesserung von Geschäftsprozessen mit den neuesten verfügbaren ICT-Lösungen.

Low Latency Mixed Reality ist so eine Lösung zum Beispiel. Darum geht's: Augmented Reality (AR) erweitert die Realität durch multimediale Inhalte, die Datenbanken passend bereitstellen. Anwendungsbeispiel sind zum Beispiel Wartungsprozesse, die Techniker nach festgelegten Schritten ausführen müssen. Erfasst ein Servicetechniker etwa der Automobil- oder der Luftfahrtindustrie mit der Kamera einer AR-Brille ein relevantes Teil, wird dieses auf dem Display farblich hervorgehoben und mit 3D-Animationen, Videos, CAD-Daten oder Textdokumenten unterlegt. So führt ihn die AR-Lösung Schritt für Schritt durch den gesamten Wartungsprozess. Beispielsweise blendet das System dem Mechaniker das passende Werkzeug ein. Ist es mit einem Ersatzteil-Bestellsystem verknüpft, werden benötigte Teile automatisch geordert.

Mithilfe des 5G-Netzwerks, der dort möglichen anwendungsbezogenen Bereitstellung von Datenraten, Geschwindigkeiten und Kapazitäten (Network Slicing) sowie einer cloudbasierten Plattform entwickelte das Innovation Center daraus einen funktionalen Prototyp eines Wartungsunterstützungssystems. Das ermöglicht, Anwendungen schnell und effizient durchzuführen und zugleich dass deren Daten direkt in der Cloud gespeichert werden können. Die Plattform lässt sich in die Prozesslandschaft von Unternehmen jeder Branche integrieren.

Touch & Feel von Innovationen

Greifbar, getreu dem Motto „Wir wollen Innovation erlebbar machen", werden solche Lösungen im Innovation Center – mitunter buchstäblich spielerisch – in leicht verständliche Showcases übersetzt, in diesem Fall von der Reparaturanweisung einer spezifischen Servicesituation in die Bedienungsanleitung für einen Segway. Wenn zum Beispiel Novizen im Umgang mit den immer beliebter werdenden Personal Transportern mit der Kamera eines iPads den Segway abfahren, werden verschiedene Elemente wie Ladevorrichtung, Höhenverstellung und Cockpit farblich markiert und lassen sich per Fingertipp aktivieren. In Video, Audio, Text und 3D-Animation werden dann die jeweiligen Funktionen über das iPad erklärt.

Das ist nur ein Beispiel dafür, was Intention, Angang und Zielgruppe des Innovation Center ausmachen. „Vielen Unternehmen mangelt es nicht an guten Ideen, sondern an deren Umsetzung, denn in PowerPoint gibt es keine technischen Probleme", so Dr. Stephan Verclas, Leiter T-Systems Innovation und Chef des Innovation Center. „Vor allem deswegen haben wir das Innovation Center in München gebaut, wo wir Innovationen mit unseren Kunden und Partnern mittels Rapid Prototyping entwickeln, in unserem Innovation Data Center betreiben und in Innovationsworkshops das Feedback unserer Kunden einholen."

Dabei ist die Herangehensweise der Innovations-Scouts gewissermaßen prototypisch, geht sie doch immer von der Frage aus: „Was passiert gerade am Markt?" Dazu beobachten Experten des Innovation Center gesellschaftliche Trends, um entdeckte „Business Customer Needs" mit zugleich aufkommenden technologischen Möglichkeiten in Korrespondenz zu setzen. Ob im Bereich Security, Netze, Cloud oder IoT – dieses Brückenbauen zwischen Technologie und Business macht das Innovation Center aus.

Disruption

So hat zur diesjährigen CeBIT das Team um Stephan Verclas in enger Zusammenarbeit mit der Digital Division von T-Systems die Logistiklösung des im Silicon Valley beheimateten Start-ups Roambee in einem Blockchain-Demonstrator für eine industrielle Fertigungslinie abgebildet. Und das Exponat als Blick über den Tellerrand klassischer Bitcoin-Finanztransaktionen hinaus zur Hannover Messe Industrie (HMI) noch einmal auf eine komplette Supply-Chain ausgebaut – inklusive des Features Smart Contracts. So disruptiv wie Blockchain für die gesamte Finanzwirtschaft ist, zeigt die Verknüpfung mit Roambee in einem Blueprint, welches Disruptionspotenzial die Lösung für die gesamte Fertigungsindustrie entwickeln kann. Denn dort haben Nachweisbarkeit und Verlässlichkeit einer permanent rollenden Logistikkette mit Blick auf Just-in-time-Fertigung herausragende Bedeutung. Insofern ist es kein Wunder, dass erste Unternehmen unterschiedlichster Branchen schon mit der Bitte um Teststellungen bei T-Systems „angeläutet" haben.

Für eine höhere Transaktionssicherheit in industriellen Lieferketten verknüpfte das Innovation Center die Logistiklösung Roambee erstmals mit dem Datenbanksystem Blockchain.

Konzernübergreifende Kooperation

Detecon, T-Labs, Multimedia Solutions, hub:raum – nicht nur mit den unterschiedlichsten Entwicklungseinheiten des eigenen Konzerns arbeitet das Innovation Center übergreifend eng zusammen. Die Kooperation erfolgt auch mit Analysten, Industrie- und Forschungspartnern, Universitäten und Start-ups, vor allem aber auch mit allen Divisionen der T-Systems (IT Division, TC Division, Digital Division und Security) und dem jeweiligen Kunden selbst.

Ziel sei es, so Stephan Verclas, „Design Thinking als Ansatz zum Lösen von Problemen und zur Entwicklung neuer Ideen in ein Unternehmen zu führen und dabei Lösungen zu finden, die aus Kundenanwendersicht überzeugen". Die Roadmap der gemeinsamen Arbeit des Innovation Center mit seinen Kunden und Partnern aus Forschung und Industrie folgt dabei modernen, agilen Entwicklungsmethoden wie Scrum.

Bis zu 150 Design- und Innovationsworkshops führt das Innovation Center jährlich durch. Ziel ist es, gesellschaftliche und technologische Entwicklungen gemeinsam mit Kunden auf deren Geschäftsfälle zu übertragen und durch die Entwicklung konkreter Produkte zu einer Wertschöpfungssteigerung zu führen.

Fotos: Dominik Gigler

INTERVIEW

„Innovation live erleben.“

Dr. Stephan Verclas, Leiter T-Systems Innovation und zugleich Chef des Innovation Center, über Abstraktion, Analogien und Adaption als Schlüssel zur businessnahen Anwendung neuer Softwarelösungen im strategischen Kundeneinsatz.

TEXT —— Thomas van Zütphen

Herr Dr. Verclas, was ist die Grundidee des Innovation Center?
Auslöser war vor acht Jahren die Frage, warum wir auch damals schon zwar als erfahrener ICT-Dienstleister und Infrastrukturanbieter galten, dabei draußen jedoch nicht unbedingt als innovativ wahrgenommen wurden. Ergebnis unserer Analyse war, dass wir als Service-Provider naturgemäß immer erst neue Softwareprodukte und Hardwaretechnologien abwarten müssen, um dann neue, innovative Services darauf aufzusetzen, also in gewisser Weise intrinsisch arbeiten. Zweiter Grund war, dass wir keine Anlaufstelle hatten, an der wir Kunden unsere Kreativität und Kompetenz konzentriert an einem Ort zeigen konnten.
Es gab zwar seitens der Telekom die T-Gallery im Sinne eines Showrooms der Kommunikation der Zukunft – aber ohne den Fokus auf Geschäfts- und ICT-Servicekunden, sondern eher aufs Consumergeschäft. Zugleich sind unsere T-Labs als Forschungs- und Entwicklungseinheit aktuellen Businessmodellen in der Regel weit voraus. Das heißt: Hier hatten wir einen Gap. Diese Lücke – das war die Konsequenz daraus – mussten und wollten wir schließen mit einem Center, das unser innovatives Portfolio vor Ort dem Kunden präsentieren kann.

Wenn man so will also: Innovation erlebbar machen?
Ganz genau. Dieses Liveerleben in den Vordergrund zu stellen war schon so etwas wie der Grundgedanke, weil wir eben ein doch sehr schwieriges, komplexes Portfolio haben. Viele unserer Services und Ideen, die bestimmte Prozesse elementar verbessern, sind oft nicht sichtbar – oder wenn doch, dann nur über langweilige Eingabemasken. Das ist nicht unbedingt spannend.

Wie kam es dann zur Standortwahl unter dem Dach eines Rechenzentrums?
Unser damaliger Produktionschef hatte hier in München das Projekt „Data Center 2020“, das den Betrieb eines Rechenzentrums unter energetischen Aspekten erforschte. Da bot es sich einfach an, Innovationen dort zu zeigen, wo uns der Markt ohnehin schon herausragende Kompetenz bestätigt hatte. Tür an Tür mit einem Rechenzentrum der Zukunft. So kam die Sache ins Rollen, und im September 2010 wurde das Innovation Center eröffnet.

Damit hatten Sie eine Plattform. Aber wie haben Sie die eigentliche Botschaft „T-Systems kann auch Innovation“ dann mit Leben gefüllt?
Zunächst war es wirklich mehr ein Showroom. Aber relativ schnell haben wir festgestellt, wen beziehungsweise was es damit eigentlich zu adressieren galt, nämlich die Umsetzungsproblematik der Kunden, aber auch unserer eigenen Kollegen in Sales und den Accounts. Denn oft ist es doch so: Es gibt ein neues Produkt, eine Software, aber so recht hat niemand eine Idee, wie das, was sie leistet, in den eigenen Geschäftsfall oder bestimmte Anwendungszwecke einzusetzen sein könnte. So kam es zur Überlegung, im Innovation Center nicht nur Workshops durchzuführen, sondern hier wirklich Innovationen zu entwickeln, diese auch zu betreiben und sich über Workshops dann erst die Feedbackschleife einzuholen. Diese Dialogform mit dem Kunden haben wir vor drei Jahren sogar mobilisiert und können heute mit einem digitalen Innovation Center auch auf Messen gehen oder mit einer kleineren Version als „Innovation2Customer“ direkt zum Kunden.

Wenn Sie Innovationen für Kunden entwickeln, haben Sie es mit unterschiedlichsten Branchen zu tun. Woher kommt das Know-how, das Sie brauchen, damit Ihre Lösung einem Unternehmen in seinem jeweiligen Markt, Geschäftsfeld und der individuellen Kundenanforderung wirklich hilft?
Wir haben ein sehr breites und tiefes ICT-Know-how, aber wir sind keine Branchenexperten, sondern zunächst einmal Generalisten, das stimmt. Den jeweiligen erforderlichen Deep Dive vollziehen wir nach dem Cross-Industry-Prinzip A3, das heißt, für bestehende Basisinnovationen aus einer anderen Branche auf Abstraktion basierend Analogien zu finden und dann die Adaption vorzunehmen für das Kundenproblem, um das es konkret geht. Das funktioniert ausgezeichnet.

Wie sieht das konkret aus? Wie machen Sie Innovationen?
Das ist auch eine Frage, die nahezu jeder Kunde in einem Innovationsworkshop stellt. Zunächst beschreiben wir unsere Zusammenarbeit mit den anderen Einheiten des Konzerns, denn wir können hier auf 450 Quadratmetern – handwerklich, wenn man so will – natürlich nicht alles selber machen.
Aber so wird deutlich, dass wir sowohl im strategischen und prozessualen Innovationsmanagement Expertise haben als auch in der Umsetzung und wie wir am Ende des Tages die komplette Kette abdecken. Vom Identifizieren einer möglichen Innovation über das Scouten mittels Technologieradar bis hin zur praktischen Entwicklung, zum Coaching, zu der Projektleitung und zuletzt der Vermarktung. Entweder als Transfer ins Portfolio oder als Kompetenzaufbau für unsere Systems Integration oder die Kollegen der Multimedia Solutions.

Wer hat am Ende eigentlich die Rechte an einer Innovation, beziehungsweise was ist, wenn das Ergebnis Ihrer Arbeit einer schon vorhandenen Lösung im Markt sehr nahekommt?
Das ist eine wichtige Frage. Das Intellectual Property Right muss tatsächlich geklärt sein, wenn ich mit einem Kunden strategisch an Innovationen zusammenarbeite. Etwa in der Automobilindustrie spielen Patente – eines Wettbewerbers zum Beispiel auf eine vergleichbare Lösung – eine wichtige Rolle. Aber auch dieses IPR-Management übernehmen wir als Service des Innovation-Managements für den Kunden.

Wer sind Ihre Besucher?
Von Groß bis Klein. Konzerne bis zu KMUs. Und bei jedem folgt unsere Arbeit dem Mindset „Think big, start small and learn fast“.

stephan.verclas@t-systems.com
www.t-systems.de/video/interview-verclas

„Bei jeder neuen Software fragt man sich doch als Erstes: Was könnte sie für meinen Geschäftsfall leisten? Und genau diese Umsetzungsproblematik adressiert das Innovation Center.“

DR. STEPHAN VERCLAS
Leiter T-Systems Innovation und Chef des Innovation Center

Fotos: Dominik Gigler, T-Systems

Dabei kann es durchaus sein, dass Unternehmen mit dem Wunsch zum Innovation Center kommen, die Möglichkeiten der Digitalisierung über innovative Lösungen primär auf Kostenreduktion abzuklopfen. Doch schwenkt die Diskussion dann zum Beispiel auf das Thema Augmented Reality im Kontext des eigenen Maintenance-Bereichs, ergibt sich oft, dass eine Steigerung der Prozesseffizienz tatsächlich reizvoller und der eigentliche Schlüssel zur Problemlösung sein könnte.

Denn von IoT über Smart Robotics zu Machine Learning bis hin zu Software-Defined Anything: „Zwischen Hype und Marktadaption schwirren einfach zu viele neue Trends und Buzzwords durch ständig neuere Technologiedebatten, als dass man auch auf Anhieb in Gänze überblicken könnte, welche Möglichkeiten die Digitalisierung mir als Kunde und meinen individuellen Geschäftsmodellen unter Umständen konkret bietet“, so Verclas. „Im Ergebnis kann beim besten Willen dann kaum noch jemand in der Lage sein zu definieren, was seine Herausforderung ist.“

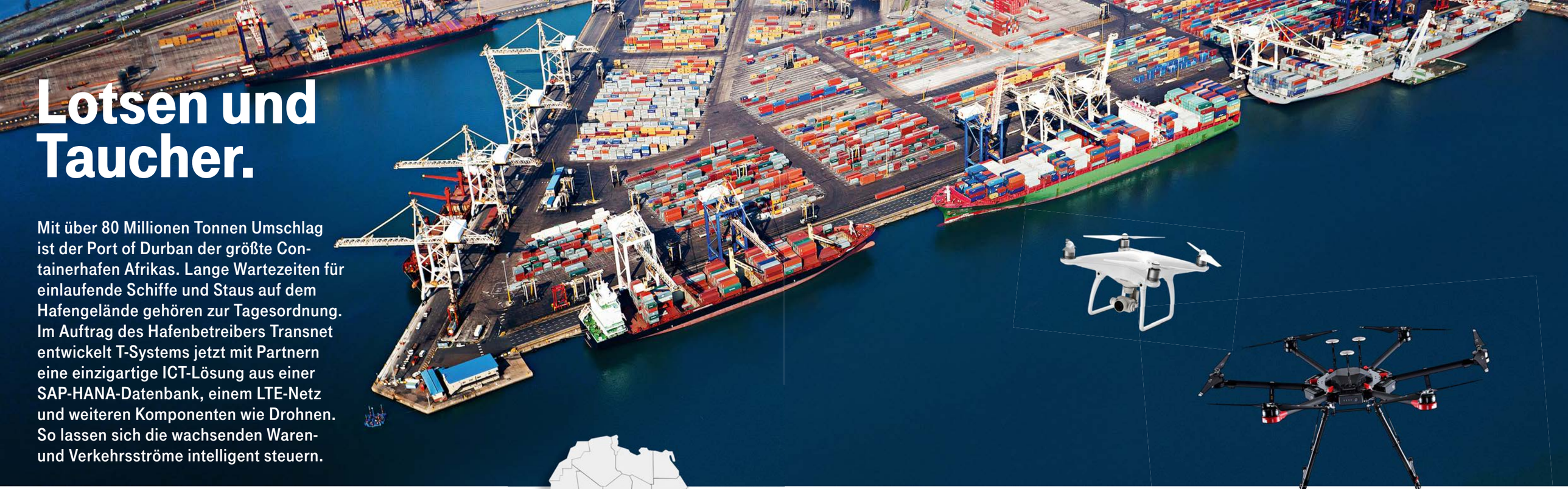
Bremsklötze auf dem Weg zur Innovation
150 Workshops dieser Art hat das Innovation Center für Kunden von T-Systems und Telekom Deutschland im vergangenen Jahr durchgeführt. Jeweils individuell vorbereitet von verantwortlichen Innovationsmanagern, die die Projekte treiben. Dazu gehört auch ein strategisches Coaching für den Umgang von Unternehmen mit den eigenen Innovationseinheiten. Denn „Innovation hat eine sehr emotionale Komponente und tut sich naturgemäß schwer, weil sie in jedem Betrieb das Bestehende stört und droht, etwas anders zu machen“, so die Erfahrung von Stephan Verclas. Das jeweilige Beharrungsvermögen anzugehen entpuppt sich regelmäßig als eine Kernaufgabe der Berater des Innovation Center.

„Auch in dieser Rolle versteht sich das Innovation Center in erster Linie als Dienstleister unseres Konzerns. Darum wird bei uns in München auch kaum jemand wirklich direkt klingeln. Kunden, die den Wunsch nach Innovation bei uns adressieren wollen, sprechen unser Team auf Messen wie der Hannover Messe Industrie an oder wenden sich an ihren T-Systems-Accounter beziehungsweise unser Servicemanagement“, so Stephan Verclas. „In diesem Sinne sind wir als Innovationsplattform natürlich einerseits ein handfestes Tool, zugleich aber Richtung Kunde auch eine stehende Einladung, mögliche neue ‚Opportunities‘ gemeinsam anzugehen.“ Ist ja auch naheliegend.

stephan.verclas@t-systems.com
www.t-systems.de/innovation-center
www.t-systems.de/innovation-management
www.t-systems.de/video/roambee-blockchain

Lotsen und Taucher.

Mit über 80 Millionen Tonnen Umschlag ist der Port of Durban der größte Containerhafen Afrikas. Lange Wartezeiten für einlaufende Schiffe und Staus auf dem Hafengelände gehören zur Tagesordnung. Im Auftrag des Hafenbetreibers Transnet entwickelt T-Systems jetzt mit Partnern eine einzigartige ICT-Lösung aus einer SAP-HANA-Datenbank, einem LTE-Netz und weiteren Komponenten wie Drohnen. So lassen sich die wachsenden Waren- und Verkehrsströme intelligent steuern.



Durban, Südafrika

TEXT —— Thorsten Rack

Dieser Markt hebt richtig ab: Die Produktionszahlen von Drohnen für den privaten und kommerziellen Gebrauch steigen rasant. Einer Prognose von Gartner zufolge wird „der weltweite Umsatz 2017 um 34 Prozent auf 6 Milliarden US-Dollar ansteigen. Bis 2020 wird erwartet, dass das Marktvolumen mehr als 11,2 Milliarden US-Dollar erreicht“.* PwC schätzt den Gesamtmarkt für Drohnen und dazugehörige Geschäftsanwendungen gar auf stattliche 127 Milliarden Dollar**. Das größte Potenzial steckt demnach im Infrastruktursektor, in der Landwirtschaft und der Transport- und Logistikbranche.

Drohnen zu Wasser und in der Luft

Welchen Mehrwert Drohnen im geschäftlichen Umfeld bieten, zeigt ein Pilotprojekt, das von der Transnet National Ports Authority initiiert und von T-Systems und ihren Technikpartnern Huawei und LOTS Operations im Port of Durban umgesetzt wurde. In Afrikas größtem Containerhafen helfen unbemannte Fluggeräte wie die DJI Phantom 4, etliche Arbeitsabläufe effizienter zu gestalten. Sie ermöglichen der Transnet als Hafenbetreiber eine Überwachung des gesamten Areals in Echtzeit. Dazu werden die Kamerabilder live ins Kontrollzentrum übertragen. Sie orten Bojen und kontrollieren deren Zustand. Sie erfassen Temperatur, Windgeschwindigkeit und sonstige Wetterdaten. Und sie erleichtern die Kommunikation mit den Frachtschiffen: „Indem Drohnen statt Boote die Einfuhrpapiere von den Schiffen abholen und zurückbringen, beschleunigen sie das Löschen der Ladung“, sagt Ronald Salis, verantwortlicher Projektleiter von T-Systems Südafrika.

Doch nicht nur in der Luft sind die autonomen Helfer unterwegs. Unter Wasser übernehmen Drohnen die Inspektion von Kaimauern und Schiffsrümpfen. Da sie im Gegensatz zu Tauchern unabhängig von der Wasserqualität arbeiten können, sinkt der Zeitaufwand auf etwa ein Drittel. Selbst die Umwelt profitiert vom Drohneneinsatz. Der mit Solartechnik angetriebene „Waste Shark“ beseitigt dank Geofencing und Kollisionsvermeidung vollkommen autonom Abfälle aus dem Hafenbecken. Und bei starker Verschmutzung kann der „intelligente Hai“ selbstständig weitere Drohnen zur Unterstützung anfordern.

„Egal ob zu Wasser oder in der Luft – die Drohnen spielen eine wichtige Rolle in unserem Smart-Port-Projekt“, betont Salis. „Und wir haben noch mehr mit ihnen vor. Künftig sollen sie den Kapitänen helfen, ihre Frachtschiffe einfach und sicher in den Hafen zu navigieren – ohne menschliche Lotsen. Dafür kombinieren wir die Drohnen mit Sensoren, 3D-Karten und Virtual-Reality-Anwendungen.“ Schon bald soll dieses weltweit einzigartige Lotsensystem im Hafen von Durban erprobt werden.

SAP-HANA-Datenbank ist Herzstück

In der intelligenten Hafenlösung, die T-Systems als Generalunternehmer für Transnet aufgebaut hat, sind die Drohnen aber nur der sichtbare Teil. Herzstück ist eine SAP-HANA-Datenbank, die im Hintergrund läuft. Daran sind alle Hafensysteme, Überwachungskameras, Sensoren, Trackingtools und auch die Drohnen via LTE-Mobilfunk angeschlossen. Eine Business-Intelligence-Lösung wertet die eingehenden Daten in Echtzeit aus und bringt sie im Kontrollzentrum auf die Bildschirme. Von hier aus werden die aufbereiteten Informationen – teils vollautomatisch – an die Zielgruppen im Hafen verteilt. Das vernetzte System bedeutet für Transnet einen Quantensprung. Bislang existierten nur Einzelanwendungen.

In 18 konkreten Anwendungsfällen hat die Smart-Port-Lösung bereits den Betriebsablauf im Hafen vereinfacht und/oder beschleunigt. Dazu gehören die Zugangs- und Zufahrtskontrollen, das Container- und Lkw-Tracking, diverse Arbeitsabläufe auf dem Wasser sowie im Kundenservice. „Wenn ein Schiff an unsere Küste kommt, muss der Kapitän wissen, wann er den Hafen erreicht und ob es genügend freie Kapazitäten gibt, um einzufahren und die Ladung zu löschen“, erklärt Lentle Mmutle, CIO von Transnet. „Wir wollen rund um solche Ereignisse eine umfassende Transparenz schaffen, um lange Wartezeiten zu vermeiden und den Handel zu vereinfachen.“

Die ICT-Technik von T-Systems schafft nicht nur einen vernetzten Überblick der Prozesse im Hafen und optimiert die Verkehrsströme. Durch den beschleunigten Warenumschlag steigen auch die Umsätze. Während die Lkw bislang oft Tage oder gar Wochen auf ihre Lieferung warten mussten und die Zufahrten blockierten, lässt sich die Beladung jetzt viel genauer steuern. Rund 5000 Smartphones und Tablets erleichtern die Kommunikation zwischen Spediteuren und Hafenbetreiber. Die Fahrer können eigene Verspätungen melden und erhalten umgekehrt automatische Warnungen, wenn es auf ihrer Route oder bei der Ankunft des Frachtschiffs zu Verzögerungen kommt. Mittels Geolokalisierung übermitteln die On-Board-Units jederzeit den genauen Standort der Lkw ans Kontrollzentrum und erfassen die Verweildauer auf dem Gelände. So sind situationsgerechte Umleitungen möglich.

PwC schätzt den Gesamtmarkt für Drohnen und dazugehörige Geschäftsanwendungen auf

127 Milliarden $.

„Zentrales Nervensystem“ für den Hafen

Dr. Stefan Bucher, operativer Leiter der IT-Division von T-Systems: „Unser Ziel ist es, das ‚zentrale Nervensystem‘ des Hafens zu entwickeln. Die Smart-Port-Lösung soll es der Transnet erlauben, mehr und mehr Betriebsabläufe zu vereinfachen und Echtzeit-Datenanalysen in die Geschäftsprozesse zu integrieren. So können die Hafenressourcen effizienter gesteuert und zugewiesen werden. Das steigert die Produktivität erheblich.“

Auch der Transnet-CIO ist zuversichtlich, dass das Projekt die Waren- und Verkehrsströme im Port of Durban nachhaltig optimieren wird. „Wenn jeder dieselben Informationen hat, können wir besser planen“, so Mmutle. „Die neue Lösung ermöglicht es uns, die Kapazitäten intelligenter zu steuern, genauere Informationen zu verteilen und Warnungen zu versenden, wenn Unterbrechungen in der Wertschöpfungskette drohen.“ Gut möglich daher, dass der Smart Port Durban als Blaupause für weitere Häfen dienen wird. Schließlich ist die Transnet National Ports Authority für alle acht südafrikanischen Seehäfen verantwortlich.

ronald.salis@t-systems.com

www.t-systems.de/news/smart-port-durban
www.t-systems.de/loesungen/sap-hana
www.transnetnationalportsauthority.net/OurPorts/Durban
www.t-systems.de/video/smart-port-durban

* http://www.gartner.com/newsroom/id/3602317

** http://press.pwc.com/News-releases/global-market-for-commercial-applications-of-drone-technology-valued-at-over-127-bn/s/ac04349e-c40d-4767-9f92-a4d219860cd2

Security by Design –

7 Goldene Regeln.

Bei der Entwicklung neuer Softwareprodukte fällt ein wichtiger Aspekt immer noch zu oft unter den Tisch: die Sicherheit. Und das in einer Zeit, in der Experten täglich etwa 380 000 neue Varianten von Schadprogrammen registrieren. In der Folge verzeichnen schon heute große Konzerne mehrere Tausend Attacken pro Tag.

TEXT —— Jan Ungruhe

Das Problem ist: 95 Prozent der erfolgreichen Angriffe basieren auf schlecht programmierter, schlecht gewarteter oder schlecht konfigurierter Software“, sagt Thomas Tschersich, Leiter Internal Security & Cyber Defense Deutsche Telekom. Dieses Problem ließe sich aber lösen, indem Security zu Beginn der Überlegung direkt berücksichtigt würde – „anstatt erst ein Pflaster über das Produkt zu kleben, wenn es bereits zusammengebaut wurde“, sagt Tschersich. Der Fachbegriff dafür lautet: Security by Design.

Security by Design vermeidet Fehler frühzeitig

Berücksichtigt ein Entwickler Sicherheitseigenschaften als Designkriterium, lassen sich Systemfehler von vornherein vermeiden. „Ein Softwareingenieur arbeitet dann auch ganz anders, denn er arbeitet Spezifikationen ab. Gehört Security nicht zu den Designkriterien, arbeitet er es auch nicht ab“, erklärt Tschersich. In diesem Fall könne der Entwickler nur hoffen, dass alles gut geht. „Meistens sehen wir aber: Es geht nicht gut.“

Im Idealfall ist das Thema Security bereits ein fester Bestandteil in der Ideenphase: Lässt sich die Idee unter Sicherheitsgesichtspunkten überhaupt realisieren? Wie muss die funktionale Sicherheitsanforderung aussehen? So fließt der Sicherheitsaspekt bereits bei der Erstellung des Prototyps mit ein – und wird durch alle Produktionsstufen mitgetragen. „Beim Abnahmetest wird das fertige Produkt dann bestenfalls nur noch durchgewinkt“, sagt Tschersich.

Angriffsfläche um mehr als 95 Prozent reduzieren

Security-Experte Tschersich empfiehlt Unternehmen, sich an sieben Grundregeln zu orientieren. „Setzt man diese ‚Goldenen Regeln‘ um, reduziert man die Angriffsfläche um mehr als 95 Prozent.“

Security by Design verringert Haftungsrisiko

Dem Security-Experten zufolge verringert ein Unternehmen mit Security by Design zudem sein Haftungsrisiko. „Hersteller müssen künftig damit rechnen, dass sie dafür haften, wenn sie die Sicherheit nicht von Anfang an vernünftig eingebaut haben.“ Könne das Unternehmen keinen Nachweis für ausreichende Sicherheit erbringen, habe es schon bald „ein signifikantes finanzielles Problem“, so Tschersich.

thomas.tschersich@telekom.de
www.t-systems.de/video/interview-tschersich

1. ANGRIFFSFLÄCHE KLEINHALTEN
Die Angriffsfläche lässt sich deutlich minimieren, indem Überflüssiges deaktiviert wird. Deaktivierte, nicht benötigte Softwareprogramme und Komponenten auf IT-Systemen können auch nicht angegriffen werden. Tschersich: „Wer im Haus nur eine Haustür braucht, baut auch nur eine ein.“

2. GEEIGNET AUTHENTIFIZIEREN
Vertrauliche Informationen und Informationssysteme sollten nur für die gewünschten Kommunikationspartner zugänglich sein. „Wer sicherstellt, dass nur authentifizierte Nutzer oder Systeme auf etwas zugreifen können, schließt mit einer hohen Wahrscheinlichkeit alle nicht identifizierten aus“, sagt Tschersich.

3. EINGABEN ÜBERPRÜFEN
Jede Eingabe sollte auf zulässige Zeichen, insbesondere Sonderzeichen, und auf die maximal zulässige Eingabelänge geprüft werden. Ein Beispiel: Bei der Bestellung auf einem Webportal sind im Feld für das Geburtsdatum des Nutzers nur Zahlen und möglicherweise noch Punkte erforderlich. „Ein Angriff kann verhindert werden, indem alles außer Zahlen und Punkten ignoriert wird“, sagt Tschersich.

4. SYSTEME TRENNEN
Nach einem erfolgreichen Angriff auf ein System versuchen Angreifer häufig, von dort nach und nach Zugriff auf weitere Systeme zu erhalten. Systeme sollten daher voneinander getrennt werden. „Wenn ein Angreifer dann etwa den Webserver hackt, ist er noch lange nicht auf der Datenbank“, sagt Tschersich.

5. VERTRAULICHES VERSCHLÜSSELN
Der Zugang zu Systemen der Datenspeicherung, -verarbeitung und -übermittlung liegt meistens nicht vollständig in der Hand des eigenen Unternehmens, etwa wenn Clouddienste genutzt werden. Umso wichtiger ist es, vertrauliche Informationen zu schützen. Tschersich erklärt: „Selbst wenn Angreifer ein System hacken, können sie auf verschlüsselte Daten nicht zugreifen.“

6. REGELMÄSSIG AKTUALISIEREN
Systeme sind schutzlos, wenn sie nicht stets auf einen aktualisierten Versionsstand gebracht werden. Nur so wird verhindert, dass Angreifer bekannte Sicherheitslücken nicht ausnutzen. Neue Versionsstände enthalten zum Beispiel oftmals Abwehrmechanismen gegen bekannt gewordene Sicherheitslücken der Vorgängerversionen.

7. SICHERHEIT KONTINUIERLICH TESTEN
Der Zustand der Systeme muss im Hinblick auf ihre Sicherheit und Angreifbarkeit kontinuierlich durch Security-Checks kontrolliert werden. „Systeme leben und entwickeln sich weiter. Zudem werden immer neue Schwachstellen bekannt“, erklärt Tschersich.

Illustration: Alex Freund/thelicensingproject.com

Cybersecurity made in Sachsen.

T-Systems-Tochter Multimedia Solutions überführt Cyber-Defense-Forschungslösung HoneySens des Freistaats Sachsen in den Produktivbetrieb und übernimmt die Vermarktung.

TEXT —— Thomas van Zütphen

Für eine funktionierende öffentliche Verwaltung sind Informationssicherheit und Datenschutz unabdingbar. Denn was immer Bürger und Unternehmen „aufs Amt" führt– von der simplen Adressänderung über die Gewerbeanmeldung, Fragen des Technologietransfers bis zum Schutz von Patenten –, könnte nicht nur die Aufmerksamkeit von Stadt, Land oder Bund auf sich ziehen. Mitunter auch die von Hackern.

Beispiel Sachsen: Mehr als 1400 direkte Angriffe auf sein Verwaltungsnetz (SVN) konnte allein der Freistaat im vergangenen Jahr detektieren und abwehren – eine Steigerung im Vergleich zu 2015 um 63 Prozent. In den 26 Millionen eingegangenen E-Mails der Landesverwaltung wurden 75 723 Schadprogramme gefunden, fast dreimal so viele wie im Jahr zuvor. „Unsere Netze können auch zum Ziel für Hacker werden, das können wir nicht verhindern", so Karl-Otto Feger, Beauftragter für Informationssicherheit des Landes. „Was wir aber verhindern können, ist, dass Cyberspione erfolgreich sind." Dabei sind die IT-Systeme der Sächsischen Landesverwaltung nicht nur Bedrohungen aus dem Internet ausgesetzt, sondern können ebenso Ziel von Angriffen aus dem internen Netzwerk werden. Ausgangspunkt sind typischerweise mit Schadsoftware befallene Rechner. Aber auch unbemerkt ins Netzwerk vorgedrungene Angreifer oder Mitarbeiter, die sich – oft irrtümlich – über Sicherheitsbestimmungen hinwegsetzen, stellen Gefahrenquellen dar. Klassische Sicherheitsmaßnahmen wie zentrale Firewalls und Anti-Virus-Systeme können diese Gefahrenquellen jedoch nicht oder nur ein wenig reduzieren.

Der Freistaat Sachsen initiierte daher 2014 das Forschungsprojekt HoneySens, um Hacker und Malware künftig schneller aufspüren zu können. Das im Ergebnis gemeinsam mit der TU Dresden entwickelte Softwaresystem lässt Sensoren im Netz verwundbare – für Angreifer attraktive – Schwachstellen simulieren. Die „Honigtöpfe" zeichneten zunächst in ausgewählten Teilnetzen des SVN alle verdächtigen Netzwerkaktivitäten oder Datenpakete auf und leiteten sie an einen Zentralserver zur Prüfung und Alarmierung weiter. „Durch die Sammlung und Auswertung wertvoller Informationen soll unser gesamtes IT-System mit insgesamt 28 Unternetzen und rund 40 000 PC-Arbeitsplätzen gegen unbefugte Zugriffe von außen gestärkt werden", erklärt Karl-Otto Feger.

Für den Sprung von einem reinen Entwicklungsprojekt zu einem dauerhaften, flächendeckenden Einsatz in der Landesverwaltung suchte der Freistaat Sachsen einen Industriepartner. Der sollte den Prototyp in den Produktivbetrieb des SVN überführen und das Softwaresystem zu einem eigenen, zugleich vermarktungsfähigen Produkt weiterentwickeln. Der Freistaat entschied sich aus mehreren Gründen für die T-Systems-Tochter Multimedia Solutions GmbH (MMS). Neben der jahrelangen Erfahrung von T-Systems in ihrer eigenen weltweiten Honeypot-Landschaft und deren Weiterentwicklung „werden wir laut Vertrag gewährleisten, dass die Softwareentwicklung auch für andere Nutzer günstig einsetzbar bleibt und es parallel zum angestrebten vereinbarten Produktivbetrieb auch eine dauerhaft frei nutzbare Open-Source-Version der Software geben wird", erklärt Marcel Wallbaum, der das Projekt aufseiten der MMS verantwortet.

In gewisser Weise jedoch, daraus macht Karl-Otto Feger kein Geheimnis, „kam bei der MMS auch der Standortvorteil Dresden zum Tragen. Mit der Wahl eines sächsischen Unternehmens haben wir bis zum vorgesehenen Launch des Produkts Ende 2017 kurze Wege und gewährleisten anschließend, dass die Vermarktung durch unseren Industriepartner wiederum auch dem Land Sachsen zugutekommt."

marcel.wallbaum@t-systems.com
https://www.egovernment.sachsen.de/1935.html
www.t-systems.com/solutions/cyber-security

Im Produktivbetrieb wird HoneySens das IT-System der Sächsischen Landesregierung mit 40 000 PC-Arbeitsplätzen flächendeckend gegen unbefugte Zugriffe von außen stärken.

Wenn das Haus mit dem Auto spricht.

Connected-Car-Ideen gibt es viele. Doch richtig zum Tragen kommt die Technologie erst, wenn auch ein tatsächlicher Austausch stattfindet und die Maschinen miteinander interagieren.

TEXT —— Sven Hansel

Bahn frei, Gang rein, laufen lassen. Manchmal kann Auto fahren so angenehm sein – bis einem plötzlich wie ein Blitz durch den Kopf schießt: „Habe ich die Terrassentür tatsächlich geschlossen?", „Ist der Herd ausgeschaltet, oder brennt die Küche bereits?" Und natürlich beunruhigen diese Fragen, wenn man sich und sein Kurzzeitgedächtnis bereits 100 Kilometer weit von zu Hause entfernt hat.

Nicht nur vor diesem Dilemma können sich schon bald zumindest die Besitzer eines Volkswagens schützen: Noch im Laufe dieses Jahres werden die Car-Net-Dienste des Autobauers im ersten Schritt über die Technologie Mirror-Link mit der herstellerunabhängigen Telekom-Smart-Home-Plattform QIVICON verbunden. Analog zu Mirror-Link werden dann im späteren Verlauf weitere Anbindungstechnologien folgen. Damit lassen sich Funktionen wie Licht, Heizung oder Innen- und Außenkamera komfortabel aus dem Auto heraus abrufen und steuern. Dafür benötigt der Fahrer kein Smartphone, sondern greift auf alle Funktionen über das Autodisplay zu – ganz einfach so wie auf sein Navi.

Drei gute Gründe für das vernetzte Auto

Ob Wasserschaden oder Rauchentwicklung – die Haussteuerung meldet besondere Vorkommnisse im Fahrzeug.

Display statt Smartphone – wie beim Navi greift der Fahrer auf die Funktionen via Touchscreen zu.

Kein Stress – alles darf auch während der Fahrt bedient werden.

Der Clou an dem neuen Modul sind jedoch nicht allein dessen Funktionen, sondern deren Integration. Denn das vernetzte Haus und das smarte Auto agieren keinesfalls autonom, sondern gemeinsam. „Wenn Sensoren im Haus beispielsweise einen Wasserschaden oder Rauchentwicklung erkennen, bekommt der Fahrer diese Informationen proaktiv auch während der Fahrt angezeigt. Er kann dann sofort über die Kamera einen Blick in sein Zuhause werfen und, wenn nötig, umgehend telefonisch Hilfe organisieren", erläutert Rainer Feldkamp, Leiter Strategische und Innovative Projekte bei T-Systems. Dieses Miteinander gilt nicht nur für den Ernstfall, sondern auch im Alltag. Anhand der Entfernung des Fahrzeugs erkennt die Steuerung im Haus die wahrscheinliche Ankunftszeit und kann daraufhin die Heizung entsprechend regeln. Das ist komfortabel und spart zugleich Heizenergie. Ebenfalls lassen sich die Rollläden öffnen, die Alarmanlage aktivieren oder das Licht einschalten. Das geht auch während der Fahrt, denn das System ist jederzeit StVO-konform.

„Wir als Mobilitätsdienstleister und T-Systems als Kommunikations- und IT-Experte bringen das Beste aus beiden Welten zusammen", fasst Dr. Marcus Heitmann, Geschäftsführer des Volkswagen-Geschäftsbereichs Car-Net, die Stärke des neuen Angebots zusammen. Wie richtig die beiden Partner damit offenbar liegen, zeigt eine repräsentative Forsa-Studie im Auftrag des Versicherers CosmosDirekt. So kennen mittlerweile bereits 86 Prozent der Bundesbürger Smart-Home-Systeme, und mehr als jeder zweite erhofft sich davon etwa höhere Sicherheit. Denn bei einem Einbruch übernehmen inzwischen einige Hausratversicherungen die Wiederbeschaffungskosten für gestohlene Gegenstände, wenn ein Smart-Home-Alarmsystem installiert ist. Zudem erstatten sie die Kosten für aufgebrochene Fenster, Türen – alles dank der Tatsache, dass das Haus mit dem Auto spricht.

rainer.feldkamp@t-systems.com
www.t-systems.de/blickwinkel/connected-car

Fotos: Haus E, Chemnitz; [2011] Bigstock.com, Volkswagen AG

Craftbier aus dem intelligenten Regal.

Welche Entwicklung nimmt der Lebensmitteleinzelhandel mit seinen aktuell – allein in Deutschland – 35 000 Geschäften? Vor zehn Jahren waren es noch mehr als 51 000. Fest steht: Sukzessive erobert die Digitalisierung auch die letzte Bastion des hierzulande noch weitgehend onlinefreien Handelssegments.

TEXT —— Roger Homrich

Weit und breit weder Warteschlangen noch Kassen. In Konzeptstores checkt sich jeder Kunde vor dem Einkauf mit seinem Smartphone ein und bezahlt später per App. Die Regale im Shop erkennen automatisch, welche Ware entnommen wird. Der Preis wird dem virtuellen Einkaufskorb hinzugefügt, und der Gesamtbetrag für den Einkauf im Anschluss automatisch vom Konto abgebucht. Schöne neue utopische Einkaufswelt? Nicht ganz.

Wie der Supermarkt der Zukunft heute schon funktionieren könnte, zeigten T-Systems und „Anna“ auf den Messen EuroShop und CeBIT. Aus gutem Grund. Denn nach einer Prognose des Handelsverbands Deutschland (HDE) steigt der Onlineanteil weiter an, wobei er im Lebensmittelbereich erst ein Prozent des Gesamtumsatzes ausmacht. T-Systems-Retail-Experte Dirk Rumler: „Wir glauben an die Zukunft des Omni-Channel. Kunden möchten von den Vorteilen der Digitalisierung profitieren und weiterhin in der Filiale einkaufen.“

So wollen laut HDE drei Viertel der Bundesbürger weiterhin persönlich im Laden einkaufen. Kanalübergreifendes Einkaufen ist laut BITKOM-Expertin Julia Miosga keine Einbahnstraße: „Online- und Offlinehandel könnten sich gegenseitig befruchten, wenn die entsprechenden Services für die Kunden geschaffen würden. Die Zukunft gehörte jenen Händlern, die die Bedürfnisse ihrer Kunden im Laden und im Internet optimal bedienen. Ziel ist es, den Kunden überall abzuholen und ein nahtloses Einkaufserlebnis zu bieten.“ Rund ein Siebtel aller Internetnutzer ab 14 Jahren hat bereits Produkte online bestellt und diese dann im Ladengeschäft abgeholt. Und weitere 42 Prozent können sich vorstellen, das künftig zu machen. „So wird auch Click & Collect wieder zum Frequenzbringer im stationären Geschäft und birgt ein hohes Potenzial, Kunden zu binden“, so Miosga.

Doch konkret zurück zu Anna. Das T-Systems-Testimonial kommt aus Frankfurt, lebt in Stuttgart und liebt Maultaschen. Selbst gekocht hat Anna die schwäbische Spezialität aber noch nie. Jetzt kommt Besuch aus Hamburg, und dann gehören Maultaschen auf den Tisch. Doch es fehlt ein Rezept. Das bekommt Anna vom Lebensmittelhändler um die Ecke samt Zutatenliste auf ihr Smartphone gespielt. Nur noch abholen – Stichwort Click & Collect – muss sie den Einkauf selbst. Als Stammkundin darf sie direkt vor dem Eingang parken. Per Smartphone und Mobile-Identity-&-Access-App schaltet sie eine der Parksperren frei.

14,2 %

Jeder siebte Internetnutzer hat 2016 vom Click-&-Collect-Service des Einzelhandels bereits Gebrauch gemacht.

Regal grüßt Kunden

Mit Betreten des Markts meldet sich ihr Handy direkt beim kostenlosen Hotspot an, und der Händler schickt ihr passend zu Maultaschen als Alternative zu badischem Wein ein Sonderangebot für Craftbier aufs Handy. Am Regal hält Anna ihre Kundenkarte an den Scanner und wird auf einem Bildschirm begrüßt: „Hallo Anna, schön, dass du da bist.“ Sie nimmt sich das passende Bier aus dem Regal, bekommt Zusatzinfos zum Produkt – und ein exklusives Sonderangebot: sechs Flaschen Bier kaufen, eine weitere gratis dazu.

Sobald die Flaschen im Einkaufswagen landen, erfasst der digitale Einkaufskorb den Abrechnungsbetrag. Jetzt will Anna noch saftige, reife Tomaten. Mit einem Minispektrometer scannt sie eine Tomate und bekommt auf ihrem Smartphone den Brix-Score angezeigt: Die Tomaten sind optimal für den Salat zu den Maultaschen. So, jetzt schnell nach Hause. In zwei Stunden kommen die Hamburger Gäste – und dann müssen die Maultaschen fertig sein. Raus mit den Waren an der Kassenschlange vorbei, denn den Einkauf bucht der Händler direkt von ihrem Konto ab.

Kaufverhalten in der Cloud analysieren

„Das alles ist heute kein Hexenwerk mehr. Ob Präzisionswaagen, Bewegungssensoren oder Barcode-Scanner. Alles ist längst auf dem Markt vorhanden“, erklärt Rumler. „Die entsprechende Technologie können Händler schon heute bei uns bekommen.“ Waagen im Inneren des Regals registrieren, ob ein Kunde ein Produkt aus dem Regal nimmt oder gegebenenfalls wieder zurückstellt. Alle Daten landen in der Cloud, wo sie für verschiedene Zwecke analysiert werden. „So bekommen Händler via IoT Informationen zum Kaufverhalten an die Hand, über die bisher nur Onlineshops verfügen, und können an den Regalen neben Produktinfos auch gezielt auf Sonderkonditionen für Stammkunden oder Kampagnen aufmerksam machen“, erklärt Sven Tissen, Smart E-Commerce Consultant bei der T-Systems-Tochter Multimedia Solutions GmbH, die das IoT-Regal entwickelt hat. Selbst externe Daten lassen sich verarbeiten. So ist es möglich, Kunden am Regal darüber zu informieren, wenn am Wochenende Grillwetter zu erwarten ist und welche Barbecue-Spezialitäten gerade im Angebot sind.

Fotos: Lorem ipsum

Fotos: andresr/Getty Images, T-Systems (2)

Via Smartphone werden intelligente Regale zum interaktiven Einkaufsberater und erleichtern Kunden die Orientierung durch die Vielfalt der Auslagen. Zugleich bekommen Händler über IoT Informationen zum Kaufverhalten und können ihre Angebote besser individualisieren.

„Kunden wollen die Vorteile der Digitalisierung auch beim stationären Einkauf nutzen.“

DIRK RUMLER, VP Sales
Center of Excellence Retail bei T-Systems

Per Scan der Kundenkarte (Foto) oder über eine vorinstallierte App erkennt das Regal den Kunden und kann ihn auf dem Digital-Signage-Bildschirm personalisiert ansprechen.

Zusatzservices dank Digitalisierung

Selbst wenn der Lebensmittelhandel eine der wenigen Sparten ist, an denen der Onlineboom bislang weitgehend vorbeiging, könnten Lebensmittellieferdienste wie REWE Digital oder Amazon Fresh den Internethandel mit Lebensmitteln spürbar voranbringen. Immerhin 3,34 Millionen aller Onlineshopper haben 2016 bereits Lebensmittel im Internet eingekauft – dreimal so viele wie 2011. „Daher müssen die Filialisten unter den Lebensmittelhändlern die Chancen der Digitalisierung für sich nutzen und Zusatzservices in den Läden einführen“, sagt Rumler. „Und die beiden für die Retail-Branche wichtigsten Messen des Jahres haben gezeigt, dass die Händler das erkannt haben. Mehr als 20 Unternehmen aus dem Handel haben sich für Anna und unser Einkaufsszenario interessiert und wollen Tests mit uns durchführen.“ Dies wird nicht nur den Verkauf von schwäbischen Maultaschen kräftig ankurbeln.

dirk.rumler@t-systems.com
www.t-systems.de/loesungen/iot
www.t-systems.de/retaile
www.t-systems.de/video/smartes-regal

„Benchmark ohne Kompromisse.“

Franz Schnabl, VP HR Magna Europe, und Hansjörg Tutner, Global Director HR Magna Steyr, im Gespräch mit Michael Böhm, Global Account Executive bei T-Systems, über auditierte Sicherheit, den Wettlauf der Bildungssysteme mit dem IT-Arbeitskräftemarkt und HR als Schnittstelle der Digitalisierung zwischen Mensch und Maschine.

Fotos: David Payr

TEXT —— Thomas van Zütphen

Herr Schnabl, Magna wächst organisch wie strategisch gleichermaßen. Dabei muss der Konzern mit fast 320 Produktionsstätten und 102 Engineering-, Produktentwicklungs- und Sales-Standorten in 29 Ländern immer mehr den Weg vom Manufacturing zur intelligenten Produktion gehen. Wie legen Sie eine hochmoderne Smart Factory der Automobilfertigung an?

Franz Schnabl: Wir sind zu 100 Prozent kundengetrieben, gerade auf dem Weg zur smarten Fabrik. Und um in diesem Sinne effizienter, schneller, qualitätsgetreuer und immer besser am Markt zu sein, ist Innovation für Magna ein permanenter Begleiter. Die Digitalisierung hat so viel Fahrt aufgenommen, dass Innovationszyklen, die früher mitunter 20 Jahre dauerten, heute in sechs Monaten oder noch schneller umgesetzt werden müssen. Deshalb liegt unser Fokus darauf, im Interesse unserer Kunden in Sachen neuester Produktionstechnik und Technologien immer eine Benchmark zu schaffen. Da gehen wir ungern Kompromisse ein.

Hansjörg Tutner: Gleichwohl ist das Thema Digitalisierung ja keine Revolution, sondern eine Evolution. Wir haben schon früh Roboter in der Fertigung eingesetzt. Das Neue ist die Menge und die Vielfalt an Daten, die uns zur Verfügung stehen. Das heißt: Auch wenn wir – wie aktuell gerade am Standort Graz – sechs Produktionsstraßen für neue Modelle umrüsten und dabei quasi keinen digitalen Stein auf dem anderen lassen, ist das zwar ein gewaltiges Projekt, aber es bleibt ein evolutionärer Prozess.

Wie unterscheiden sich dabei die Anforderungen der Einrichtung beziehungsweise Umstellung zwischen Green-Field- und Brown-Field-Anlagen?

Schnabl: Zum digitalen Beplanen und Bespielen sind Green-Field-Projekte natürlich einfacher, weil Sie bei null anfangen können. Die Komplexität der Umstellung aktuell hier in Graz liegt darin, dass die laufenden Projekte bis zum letzten Tag und zur vollen Zufriedenheit der Kunden zu Ende geführt werden. Das bedeutet, parallel zum laufenden Betrieb umrüsten zu müssen. Bei Übernahmen wiederum geht es darum, einem neuen Mitglied in der Magna-Familie nicht einfach Systeme überzustülpen, die wir schon anderswo nutzen, sondern abzuwägen und nach Best Case zu beurteilen.

Tutner: Und dann kommt natürlich noch hinzu, dass wir je nach Standort in Asien, Amerika oder Europa eine jeweils völlig andere Produktionskultur vorfinden. Wenn Sie so wollen: Wie ist mein „Spielermaterial“? Was hab ich für Mitarbeiter? Und wie ist der Ausbildungsstand? Solche Dinge muss man berücksichtigen, wenn man mit jedem Schritt der Digitalisierung seinen Mitarbeitern neue, andere und gegebenenfalls mehr Dinge abverlangt. Also zunächst einmal analysieren, wie sieht die Produktionsumgebung „Mensch“ vor Ort aus.

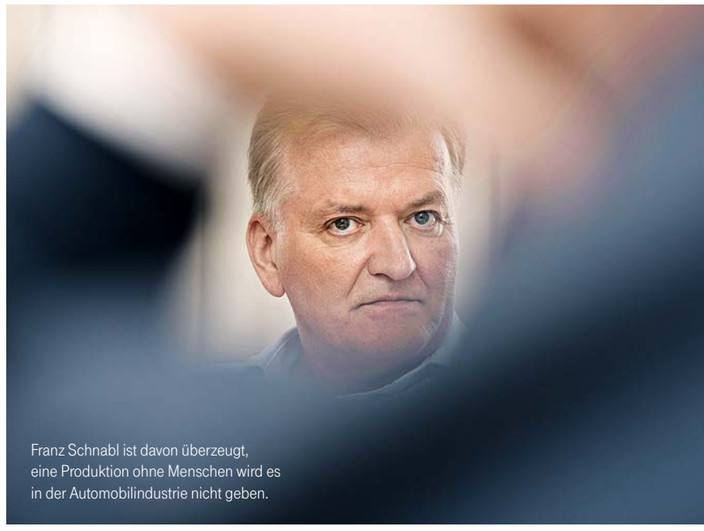
Schon 1999 haben Sie damit begonnen, verschiedene Automodelle auf der gleichen Fertigungsstraße zu bauen. Was hat sich seither getan?

Tutner: Im heute sehr weit automatisierten Rohbau werden Sie nur noch ganz wenige hoch qualifizierte Mitarbeiter finden. Hier hat sich das Verhältnis Mensch-Maschine komplett verschoben. Ähnlich ist es in der Lackierung. In der Montage wiederum braucht die Automobilproduktion sehr viel Flexibilität, die wird noch immer über den Menschen am sinnvollsten abgebildet. Alles über Roboter darzustellen wäre auch nicht wirtschaftlich. Deshalb verringern wir manuelle Wertschöpfung nur da, wo es Sinn macht. Die Kunst ist es, die Grenze zu finden zwischen dem, was technisch möglich ist, und dem, was wirtschaftlich Sinn macht.

Schnabl: Und dabei ist es egal, ob es sich um mobile Fertigungsstraßen handelt oder um sich selbstorganisierende Transportfahrzeuge, um Lagerbestände, deren Regale selbstständig nachordern, oder um Roboter, die von Menschen lernen und neues Wissen an ihre „Kollegen“ weitergeben – diese Grenze folgt in allen Produktionsbereichen immer

„Um effizienter, schneller, qualitätsgetreuer und immer besser am Markt zu sein, ist Innovation für Magna ein permanenter Begleiter.“

FRANZ SCHNABL, VP HR Magna Europe



Franz Schnabl ist davon überzeugt, eine Produktion ohne Menschen wird es in der Automobilindustrie nicht geben.

„Preventive Maintenance erfordert neue Qualifikationslevel und steht für einen permanenten Change-Prozess."

HANSJÖRG TUTNER, Global Director HR Magna Steyr

Ohne immer mehr die Aufgaben von Universitäten zu übernehmen, werden Industriebetriebe für Hansjörg Tutner kaum mit dem technologischen Fortschritt mithalten können.

der Kundenvorgabe: Was müssen wir tun, um jährlich eine Effizienzsteigerung von zwei bis zweieinhalb Prozent im Fahrzeugausstoß zu erreichen, wenn die Mitarbeiterzahl gleich bleibt? Die daraus zwingend resultierende Arbeitsplatzverschiebung erleben wir in allen Bereichen.

Welche Aspekte spielen bei der zunehmenden Digitalisierung aus HR-Sicht eine besondere Rolle?

Schnabl: Die Mitarbeiter müssen sich mit jeder neuen Technologie auseinandersetzen und fit dafür sein. Wenn zum Beispiel die Ablaufgeschwindigkeit bestimmter Prozesse schneller wird, darf die Fehlerhäufigkeit nicht steigen. Bei Magna werden über alle Bereiche hinweg etwa fünf Prozent der Arbeitszeit für Aus- beziehungsweise Fortbildung aufgewendet.

Tutner: Investitionen in Ausbildung und Lernen werden zunehmen. Denn es wird wettbewerbsrelevant, dass wir immer an der Qualifikation unserer Mitarbeiter „dranbleiben". Nur ein Beispiel dafür ist die Instandhaltung unserer Anlagen. Wenn es heute darum geht, im Vorfeld zu erkennen, wann ein Fertigungsteil wie zu ertüchtigen ist, dann müssen Mitarbeiter die entsprechenden Ergebnisse der Auswertung von Daten und Sensoren verstehen und danach handeln. Preventive Maintenance erfordert neue Qualifikationslevel und steht praktisch beispielhaft für einen permanenten Change-Prozess.

Wie lange wird es in der digitalen Fabrik noch menschliche Mitarbeiter geben, und was werden ihre Aufgaben sein?

Schnabl: Eine Produktion ohne Menschen wird es so nicht geben. Das ist unvorstellbar. Einer Prognose von PwC zufolge werden wir 2030 in der Automobilproduktion etwa fünf Prozent weniger direkte Mitarbeiter beschäftigen. Entsprechend werden sich Arbeitsplätze verlagern. Ich persönlich glaube, der Faktor Mensch wird nie ganz wegfallen. Das ist ja für Industrie und Wirtschaft auch ein politisches Gebot von Arbeit und Beschäftigung, sinnstiftend für den Menschen zu sein. Diese Verantwortung auf dem Hochaltar der Digitalisierung opfern zu wollen würde sich sofort gegen die Digitalisierung selbst richten und wäre insofern – quasi automatisch – buchstäblich kontraproduktiv.

Richtig ist: Die Digitalisierung bietet Riesenchancen, Arbeitszeitmodelle anders zu gestalten und die Lebensführung von uns Menschen selbstbestimmter zu machen. Die Kunst ist es, alle Menschen auf dieser Reise rechtzeitig abzuholen und mitzunehmen. Das ist eine Kernaufgabe von HR in der Digitalisierung, die wir – und das gilt für alle Stakeholder des Unternehmens – für aktuell 160 000 Mitarbeiter weltweit auf dem eingeschlagenen Weg in Richtung smarte Produktionsprozesse sehr ernst nehmen. HR als Schnittstelle der Digitalisierung zwischen Mensch und Maschine.

IoT, künstliche Intelligenz, Augmented Reality – was in den hochmodernen Fertigungsstätten von Magna längst „commodity" ist, ist für viele Unternehmen „yet to come". Was ist das „Next Big Thing" in der smarten Fabrik?

Schnabl: „Think global, act local" mit dem Fokus auf Kundenzufriedenheit spiegelt sich heute in unserer Innovationsstrategie wider. Anders gesagt: Die Frage an sich nach dem Next Big Thing kann, glaube ich, niemand beantworten.

Tutner: Das hat natürlich damit zu tun, dass dahinter wiederum in unserer Branche die Frage der Mobilität der Zukunft steht. Und auch das kann niemand beantworten. Für uns als Zulieferer bedeutet das, immer vorne dabei zu sein. Denn sicher ist: Es wird sich signifikant etwas ändern, gerade in der Automobilproduktion. Autonomes Fahren und Elektromobilität werden gewaltigen Einfluss auf uns haben von der Ausbildung über die praktische Fertigung bis zur Organisation.

Gibt es konkrete Technologien, Anwendungen, Devices, von denen Sie sagen, da ist Magna schon sehr weit?

Schnabl: Auf Automobilseite ist es etwa unsere Innovation eines Hybridantriebs aus kombiniertem Elektro- und Wasserstoffantrieb. Was unsere Digitalisierung angeht, erfolgt der aktuell größte Umbruch bei uns in der Logistik, wo wir sukzessive fahrerlose Transportsysteme einsetzen. Die gesamte Steuerung der Logistik wird mit der ständig optimierten Hochverfügbarkeit von Daten sehr spannend. In der Robotic Collaboration ist unser nächster Schritt, dass in ersten Anwendungen die Zäune verschwinden, die heute noch vielerorts in der Fertigung Menschen und Roboter voneinander trennen.

Tutner: Ebenso testen wir Wearables als Brillen beim virtuellen Engineering und in der Ausbildung. In einem anderen Fall kooperieren wir mit dem Innovation Center der T-Systems in München in Anwendungsszenarien, in denen es darum geht, bei Incidents in der Produktion oder Montage die richtigen Spezialisten schnellstmöglich in einem virtuellen Emergency Room zusammenzubringen.

„General wird Sicherheits-Chef bei Magna" titelte „Der Standard" seinerzeit – welche Rolle spielt Sicherheit für Sie in Ihrer aktuellen Rolle heute?

Schnabl: Das hat ja mehrere Facetten. Angefangen damit, dass jede Produktionsbesprechung bei uns mit dem Thema Sicherheit am Arbeitsplatz beginnt. Die sehr sehr positiven Zahlen, wie wir sie hier erzielen, fallen aber nicht vom Himmel. Das heißt, auch hier führt jedes Wissen aus der neuen, gewaltigen Datenverfügbarkeit täglich zu neuen Chancen, und dafür muss man offen sein. Deshalb wird jeder Standort regelmäßig evaluiert und auditiert, um auch in Sachen Sicherheit am Arbeitsplatz immer auf dem neuesten Stand der Technik zu sein. Das bedeutet konkret, dass wir an dieser Stelle versuchen, unsere europäische Kultur und Denkweise zum globalen Standard zu machen.

Aber es geht ja auch um die Sicherheit der Anwendungen, Produkte und Services sowie die Sicherheit nach außen. All das, was wir unter Innovationsschutz summieren, haben wir bewusst dem Risk Management zugeordnet, das verantwortlich für die Integrität von Software und Daten und Intellectual Property ist – sowohl unsererseits als auch kundenseitig. Dieses Feld wird an Bedeutung zukünftig in einem nicht zu unterschätzenden Maß gewinnen.

Nennen Sie einmal ein Beispiel, bitte.

Schnabl: Nehmen Sie – einmal abseits der branchenweit diskutierten Herausforderungen wie Connected Car, autonomes Fahren, Internet of Things & Co. – nur das Stichwort Drohnen. Wenn es um den Schutz vor Industriespionage, zum Beispiel aus der Luft via Drohnen geht, gibt es für uns kundenseitig klare Vorgaben und auch Auditierungen, wie wir bestimmte Bereiche im Entwicklungs- und Produktionsprozess zu schützen haben – inklusive der Drohnenabwehr. Da hat die Branche schon über den VDA (Verband der Automobilindustrie) längst entsprechende Standards vorgegeben.

Aber mit Blick auf den gesetzlichen Rahmen besteht noch Handlungsbedarf – wenn es darum geht, ein theoretisches Recht an Intellectual Property zum Beispiel auch durchzusetzen und in einen verlässlichen Compliance Framework münden zu lassen. Denn zahnlose Tiger nützen niemandem, wenn böswillige Drohnen das eigene Werktor überfliegen.

„Think global, act local" muss sich für Franz Schnabl in der Innovationsstrategie Magnas widerspiegeln.

Damit Unternehmen ihr Recht an Intellectual Property etwa bei Luftaufnahmen von Drohnen durchsetzen können, sieht der Automobilzulieferer Magna (hier das Werk in Graz) gesetzgeberischen Handlungsbedarf.

Flexibilität, Agilität, Vernetzung – Magna versteht Smart Production und die digitale Fabrik nie als Status quo, sondern treibt die digitale Fabrik quasi permanent weiter. Zugleich geht es darum, den Weg vom Virtual Engineering zur realen Fertigung und Auslieferung an den Kunden immer kürzer zu gestalten. Welche Unterstützung erwarten Sie von IT-Dienstleistern wie T-Systems?

Schnabl: Man muss selbstständig über den Tellerrand schauen. Damit sich jeder in den Innovationsprozess einbringt. Von unseren Partnern erwarten wir einen ständigen Interaktionsprozess, und das Dritte ist der Kunden- und Wettbewerbsdruck. Der befeuert den täglichen Verbesserungsprozess – immer entlang der Frage: Warum haben wir einen Auftrag bekommen, einen anderen aber nicht? Die Gründe sind fast immer Innovation und Effizienz.

Tutner: Das führt zu einer Herausforderung, die den Input, den wir in Sachen Digitalisierung und Innovation etwa von Partnern wie T-Systems bekommen, noch verschärft: dass am Ende des Tages der Arbeitsmarkt nicht annähernd die potenziellen Mitarbeiter liefern kann, die von uns zum Beispiel mit Blick auf Virtual Engineering oder Smart Production gebraucht werden. Im Ergebnis müssen Industriebetriebe wie wir immer mehr Aufgaben von Schulen und Universitäten übernehmen, um mit dem technologischen Fortschritt dessen, was in der industriellen Fertigung heute schon möglich ist, Schritt zu halten.

Schnabl: Da sind unsere Bildungssysteme ein brutaler Showstopper der Digitalisierung – so deutlich muss man das sagen. Das ist eine Kritik, die sich besonders an die Politik richtet.

boehmm@t-systems.com
www.magna.com/de
www.t-systems.de/automotive/smart-factory

Fotos: David Payr

Gib Cyberspionen keine Chance.

In der Sicherheitsarchitektur vieler Unternehmen wird häufig ein Aspekt vernachlässigt. Bei den Weitverkehrsnetzen für Daten- und Sprachkommunikation, quasi den Lebensadern der globalen Kommunikation, wird zumeist keine Verschlüsselung eingesetzt. Beim Elektronikkonzern Rohde & Schwarz, mit mehr als 10 000 Mitarbeitern und Standorten in 70 Ländern, beißen sich Cyberspione dagegen die Zähne aus. Die gesamte Kommunikation wird zusätzlich verschlüsselt.

TEXT —— Roger Homrich

Während Rechenzentren Hochsicherheitstresoren gleichen, erreichen die Datenverbindungen im globalen Unternehmensnetz oft nicht annähernd deren Schutzniveau. Um jedoch Entwicklungs- und Kundendaten genauso wie Angebote oder Finanzinformationen davor zu schützen, mit vergleichsweise geringem Aufwand abgezapft zu werden, müssen von IT-Dienstleistern außergewöhnlich hohe Sicherheitsanforderungen bedient werden können.

„2014 haben wir uns für das Produkt EtherConnect von T-Systems entschieden, bei dem bislang getrennte LANs zu einem logischen Netzwerk zusammengeschlossen werden. Damit können wir unsere Anforderungen an hohe Bandbreite erfüllen und zugleich unsere hauseigene Verschlüsselungstechnologie einsetzen“, sagt Andreas Rau, verantwortlich für die WAN-Infrastruktur von Rohde & Schwarz. „Die Lösung ist eine perfekte Erweiterung zu unserer IP-basierten WAN-Infrastruktur.“

Heute betreibt T-Systems für das Unternehmen mit mehr als 10 000 Mitarbeitern im Telekom Designed Network ein IP-Netz für zwölf deutsche Standorte. Die Produktionswerke in Memmingen, Teisnach, Vimperk (Tschechien) und die Entwicklungsstandorte in Berlin und Stuttgart sind mit redundanten Gigabit-EthernetConnect-Verbindungen an die Zentrale in München angeschlossen.

Unternehmenseigene Hochleistungsverschlüsselung

Ein Unternehmen, das zu den innovativsten in Deutschland zählt und für staatliche Institutionen arbeitet, braucht jedoch maximale Sicherheit. Daher verschlüsselt Rohde & Schwarz seinen gesamten Datenverkehr auch über das Ethernet-WAN. Der Clou: Das Unternehmen setzt die hauseigene Hochleistungsverschlüsselungslösung SITLine ETH der Rohde & Schwarz Cybersecurity ein. Diese ist vom Bundesamt für Sicherheit in der Informationstechnik (BSI) geprüft und für den Datenaustausch von Informationen zugelassen, die das Schutzniveau VS-NfD sowie NATO RESTRICTED haben. Die BSI-Prüfung umfasst das ganze System mit sämtlichen Implementierungsdetails, inklusive Krypto-Management, verwendeter Algorithmen, Software und Hardware. Jede Änderung erfordert eine neue Evaluierung.

Mit der Kombination aus eigener Verschlüsselungstechnologie und der EthernetConnect-Netzwerkinfrastruktur von T-Systems nutzt Rohde & Schwarz eine Gesamtlösung, bei der das Beste aus zwei Welten zusammengekommen ist. Das hoch verfügbare, vollständig redundante Netz von T-Systems wird durch die Verschlüsselungslösung zusätzlich gegen neugierige Lauscher abgesichert. Durch die IP-basierte Verschlüsselung waren nur geringe Übertragungsraten möglich, mit der hardwarebasierten Ethernet-Verschlüsselung können große Bandbreiten mit geringen Verzögerungen realisiert werden.

Bis zu 40 Gigabit Verschlüsselungsdurchsatz

Die heutige Lösung von Rohde & Schwarz Cybersecurity erlaubt einen Verschlüsselungsdurchsatz von bis zu 40 Gbit/s pro Gerät. Damit wird Ethernet in Kombination mit Kryptografie interessant, weil nahezu kein Overhead anfällt. Wenn dann noch einfache Administration, getrenntes Netzwerk- und Sicherheitsmanagement, kompakte Bauweise und niedrige Systemkosten dazukommen, steht verschlüsseltem Ethernet für den Einsatz im WAN nichts mehr im Weg. Die Daten werden mittels einer AES-256-Bit-Verschlüsselung gesichert. Die Lösung arbeitet ohne zentralen Schlüsselserver und ist damit sowohl hoch verfügbar als auch wirksam vor entsprechenden Angriffen geschützt.

markus.greiner@t-systems.com
www.rohde-schwarz.de
www.t-systems.de/verschluesselung

Wie.

„Stempeln“ von unterwegs – die mobile Zeiterfassung im Fahrzeug funktioniert so simpel wie die Stechuhr im heimischen Betrieb.

Wann.

Wo.

Einfache Auswertung von Fahrzeugdaten: Die M.Box registriert Geschwindigkeit, Standort, Fahrt- und Ruhezeiten.

Für das Steuern von Fahrzeugflotten ist eine zuverlässige Software heutzutage unabdingbar. Zu wissen, wann und wo der komplette Fahrzeugbestand unterwegs ist und wie er eingesetzt wird, ist das A und O jedes Fuhrparkmanagements. Diese Aufgabe übernimmt zum Beispiel die M.Box von MobilZeit. Die Softwarelösung dient der GPS-Ortung und Datenerfassung in Echtzeit. Als Betriebsumgebung nutzt das Unternehmen Infrastruktur aus der Cloud von T-Systems.

TEXT —— Michael Hermann

Ob Spedition, Pflegedienst, Taxiunternehmen, Handwerker oder Handelsvertreter mit Fahrtenbuch: MobilZeit bedient mit der M.Box Kunden aus allen Branchen, die Fahrzeugflotten betreiben. Mithilfe dieser Softwarelösung können Unternehmen ihre Fahrzeuge zeitnah orten und zurückgelegte Routen der letzten zwölf Monate verfolgen. Die M.Box misst die Geschwindigkeit, ermittelt Haltepunkte und Standorte – und dient darüber hinaus zur Diebstahlerkennung für Fahrzeuge und Baumaschinen.

Seit mehr als 20 Jahren versorgt das Unternehmen aus Winsen an der Aller Kunden mit innovativen Systemen zur Datenerfassung: P.Box für die Personalzeiterfassung, S.Box für die mobile Zeiterfassung und M.Box für die GPS-Fahrzeugortung. Die im eigenen Haus betriebenen Serversysteme erlaubten es jedoch nicht, die M.Box flexibel mit IT-Ressourcen zu versorgen. „Was wir gebraucht haben“, so Geschäftsführer Kurt Fisker, „war eine Betriebsumgebung mit größtmöglicher Flexibilität und Skalierbarkeit.“

Der schwankende „Appetit“ auf mehr – sei es ein lokaler Pizzabringdienst mit fünf Pandas oder ein landesweiter Kurierservice mit 2000 Sprintern: Jede Auslastung von Fahrzeugflotten folgt täglich neuen Kurven. Auch deshalb entschied sich MobilZeit für das Infrastructure-as-a-Service-Angebot DSI vCloud von T-Systems – und dabei konkret für das Nutzungsmodell Committed vDC. Bestehend aus einem festen und einem flexiblen Ressourcenanteil (CPU und RAM) dienen reservierte Rechenressourcen zur Abdeckung der Basislast. Zugleich lassen sich mit abrufbereiten „Burst“-Kapazitäten gegebenenfalls auftretende Lastspitzen stemmen. So passt sich die Unternehmens-IT jederzeit flexibel dem Geschäft an. Hierfür setzt T-Systems Technologie von VMware ein.

Mithilfe des Self-Service-Portals migrierte MobilZeit die Daten von mehreren Tausend Fahrzeugen, die bereits die M.Box installiert hatten, in die sichere und dynamisch skalierbare DSI vCloud eines T-Systems-Rechenzentrums in München. Ob Fahrzeug, Baumaschine oder Trailer – für jedes ihrer Betriebsmittel nutzen die Kunden von MobilZeit seither eine M2M-Datenkarte der Telekom, die im Standardrhythmus von einer Minute, bei Bedarf auch alle zehn Sekunden, die jeweilige Positionsangabe übermittelt. Sind die Daten über das Telekom-Netz in die Telekom-Cloud übermittelt, kann dort jeder Kunde in einem eigenen geschützten Bereich seine individuellen Einsatzszenarien – etwa in der Disposition und Routenanalyse – bearbeiten. Dabei ermöglicht die lokal installierte Client-Software, dedizierte Auswertungen auch in unterschiedlichen Formaten vorzunehmen. Zudem können Kunden virtuelle „Zäune“, sogenannte Geofence-Zonen, einrichten und mit deren Hilfe ermitteln, wann und wie lange Fahrzeuge einen zuvor definierten Bereich verlassen. Dadurch lässt sich jeder Diebstahl im Flottenbestand erkennen: Durchbricht ein Fahrzeug ohne Autorisierung seinen virtuellen Zaun, erhält der Kunde sofort eine Warnung per E-Mail.

Hoch verfügbar und zuverlässig

Für die MobilZeit GmbH und ihre Kunden hat sich der Umzug gelohnt. Denn die Hochverfügbarkeit und die Zuverlässigkeit der Cloud-Lösung schlagen den Eigenbetrieb um Längen. „Allein in Sachen Kundenzufriedenheit zahlt sich das für uns schon aus“, freut sich Kurt Fisker. Zugleich ist die Leistungsfähigkeit von MobilZeit und M.Box nicht länger abhängig vom eigenen Hardwarebestand, sondern kann je nach Bedarf aus der DSI vCloud hinzugebucht oder heruntergefahren werden. Ein Anruf oder eine E-Mail genügt, und T-Systems stellt zusätzliche Rechenleistung oder Speicherplatz anforderungsgerecht zur Verfügung.

martin.bader@t-systems.com
mobilzeit.de
www.t-systems.de/referenz/mobilzeit
www.t-systems.de/loesungen/vcloud
www.t-systems.de/video/vCloud

Fotos: Shutterstock.com, Marcus Jacobs, PR

GO Maut 2.0 spricht europäisch.

Österreichs staatliche Infrastrukturgesellschaft ASFINAG betreibt das interoperable, elektronische Mautsystem GO Maut von 2018 an mit Unterstützung von T-Systems.

Vom schweren Wohnmobil bis zum Sattelschlepper – in Österreich kann die Maut nur über die GO-Box entrichtet werden. 2016 waren es 650 Millionen Transaktionen.

Fotos: Johannes Hauleitner/Gallery Stock, ASFINAG (3)

ASFINAG
Die ASFINAG wurde 1982 gegründet und plant, finanziert, baut, erhält, betreibt und bemautet rund 2200 Kilometer Autobahnen und Schnellstraßen. Seit 1997 besitzt die ASFINAG das „Fruchtgenussrecht" an den im Eigentum des Bundes stehenden Grundstücken und Anlagen des hochrangigen Bundesstraßennetzes. Damit ist das Unternehmen berechtigt, Mauten und Benützungsgebühren einzuheben. Die ASFINAG finanziert sich im Wesentlichen aus den Mauteinnahmen – also ohne Zuschüsse aus dem Staatsbudget. Alle Mauteinnahmen gehen wieder direkt in den Betrieb und Bau des Streckennetzes und damit in die Erhöhung der Verkehrssicherheit.

TEXT —— Roger Homrich

1. Januar 2004, in Österreich startet die Gebührenpflicht für Fahrzeuge über 3,5 Tonnen Gesamtgewicht. Auf allen Autobahnen und Schnellstraßen registriert seitdem eine On-Board-Unit, die GO-Box, zusammen mit den Mautportalen entlang der Autobahnen die Fahrtstrecken der mautpflichtigen Lkw.

Ohne zu stoppen, kommuniziert die GO-Box auf Basis von Mikrowellentechnik automatisch mit den Mautportalen. Der Installationsaufwand für die Lkw-Fahrer ist minimal, die Bedienung einfach: Vor Fahrtantritt müssen sie nur die Anzahl der Achsen des Fahrzeugs per Knopfdruck eingeben. Schon kann's losgehen. Den Rest erledigt die GO-Box fast allein, sie rechnet während der Fahrt die Maut aus. Der Betrag wird abgebucht, oder der Lkw-Besitzer bekommt eine Rechnung. Ein kurzer Piepton, die Mauttransaktion ist erfolgt. Bezahlen können die Lkw-Besitzer ganz nach ihrem Geschmack. Entweder sind die Boxen ähnlich wie bei einem Pre-Paid-Handy mit Guthaben aufgeladen oder die Daten der Fahrstrecke werden automatisch in ein Rechenzentrum übertragen, dort verarbeitet und die Kosten via Postpay in Rechnung gestellt – zum Beispiel mit GO Direkt.

Ein wichtiger Aspekt für die Modernisierung des Systems ist die Interoperabilität der Mautsysteme auf europäischer Ebene. Hier hat die ASFINAG (Autobahnen- und Schnellstraßen-Finanzierungs-Aktiengesellschaft) zusammen mit anderen europäischen Mautbetreibern Pionierarbeit geleistet. GO Maut 2.0 erfüllt den von der Europäischen Kommission vorgelegten interoperablen Standard eines europäischen elektronischen Mautdienstes (EETS). Der gibt vor, dass die Länder in Europa weiterhin selbst über die eingesetzte Mauttechnik entscheiden dürfen, diese allerdings kompatibel zum EETS sein muss. Eine zugelassene On-Board-Unit im Pkw oder Lkw wird dann ausreichen, um die Gebühren in allen angeschlossenen europäischen Erhebungssystemen zu erfassen.

Nächste Mautgeneration ab 2018 am Start

2016 hat die ASFINAG den Aufbau und den Betrieb des Zentralsystems neu ausgeschrieben und an die Telekom-Tochter T-Systems vergeben. Von 2018 an wird damit die Grundlage für ein zukünftiges neues GO-Mautsystem geschaffen. Erstmals wird damit ein großes, flächendeckendes Mautsystem im laufenden Betrieb erneuert. Wie 2004 Neuland für die ASFINAG, die damit am offenen Herz operiert. Ein Systemausfall von nur einem Tag würde einen Schaden in Millionenhöhe bedeuten.

Den Zuschlag für den Aufbau des zentralen IT-Systems und den zehnjährigen Betrieb des hochverfügbaren Rechenzentrums erhielt T-Systems nach einem europaweiten Vergabeverfahren. „Wir setzen seit 2004 ein sehr stabiles und verlässliches System ein. Mit diesem Auftrag können wir dieses Erfolgsmodell fortführen und sicherstellen", sagt ASFINAG-Geschäftsführer Bernd Datler. Für die GO Maut 2.0 modernisiert T-Systems die technische Plattform, zum Beispiel durch Virtualisierung von Systemen. „Damit wollen wir die Komplexität der Systemlandschaft deutlich reduzieren", erklärt Datler. Die Software bleibt während der Umstellung unangetastet. „Wir wollen sicherstellen, dass unsere Kunden nichts von der Umstellung bemerken. Im Gegenteil: Die Kunden werden vom Ausbau der Services profitieren."

Um die bekannten Risiken für den Umzug eines solch komplexen IT-Systems in ein neues Rechenzentrum zu minimieren, hat die ASFINAG im Vorfeld der Ausschreibung sehr genau beschrieben, was das System leisten muss, und dafür die Dokumentation auch extern prüfen lassen. Mit Erfolg: Zur Halbzeit der Transition im April 2017 standen die Ampeln auf Grün.

„Unsere GO Maut 2.0 spricht eine europäische Mikrowellensprache."

BERND DATLER
Geschäftsführer ASFINAG Maut Service GmbH

Verkaufsterminals und Kontrollfahrzeuge

Doch der Auftrag umfasst eine Reihe weiterer Aufgaben. T-Systems Austria ist künftig auch für die Ausgabe der Fahrzeuggeräte zuständig und übernimmt den Betrieb der rund 200 Vertriebsstellen samt Zahlungsterminals. Eine große Herausforderung, immerhin verarbeiten die Systeme der GO Maut rund 650 Millionen Transaktionen pro Jahr.

„Auch die Fahrzeuge des Service- und Kontrolldienstes rüsten wir mit moderner Technologie nach", sagt Dieter Kögler von T-Systems Austria. Obwohl die Zahlungsmoral der Fahrer in Österreich bei der Maut sehr hoch ist, muss die Einhaltung der Mautpflicht aus Gründen der Fairness weiter kontrolliert werden. Dafür setzt die ASFINAG neben dem Dienst auch automatische Kamerasysteme ein, die die korrekte Entrichtung der Maut überwachen.

Nutzer finanzieren Investitionen in die Infrastruktur

Die Einhaltung der Mautpflicht ist ein wesentlicher Eckpfeiler für die ASFINAG. Denn die ASFINAG erhält keine zusätzlichen Geldmittel vom Bund und finanziert sich ausschließlich über die Erlöse aus Vignette und Lkw-Maut. „Jeder, der die Autobahn benutzt, kommt auch dafür auf. Ein faires System, das die ASFINAG zu einem Best-Practice-Modell in ganz Europa macht", bestätigt Datler. Dabei ist außerdem die Kompatibilität mit anderen Mautsystemen, etwa dem GPS-gestützten deutschen System, wesentlich. „Jedes Satellitengerät für Deutschland hat auch eine Mikrowellenschnittstelle an Bord. Die spricht also eine europäische Mikrowellensprache", sagt Datler.

Dieter.Koegler@t-systems.at
www.asfinag.at
www.t-systems.de/loesungen/maut

FRONTBEOBACHTUNG

Neun Fakten zum Cyberwar zwischen Gut und Böse.

Über 92
Milliarden Dollar
betrugen 2016 die weltweiten Ausgaben für Datensicherheit. Für 2020 werden sie auf über 125 Milliarden Dollar geschätzt.

1.792 Hackerangriffe
gab es im vergangenen Jahr, bei denen insgesamt fast 1,4 Mrd. Datensätze kompromittiert wurden.

48 %
der Deutschen
meinen, dass Unternehmen ihre persönlichen Daten illegal nutzen und unerlaubt an Dritte weitergeben.

500
bedrohliche Attacken
auf NATO-Einrichtungen wurden 2016 monatlich abgewehrt.

„Lassen Sie einen Stick in der Kantine oder der Toilette liegen. Einer wird ihn sicher in den Rechner stecken."

Mario Faßbender,
Verfassungsschutz Brandenburg

Etwa 380 000
neue Schadprogramm-varianten
werden täglich gesichtet. Allein bis August 2016 waren insgesamt mehr als 560 Millionen verschiedene Schadprogrammvarianten bekannt.

Um 1270 %
zugenommen hat im ersten Halbjahr 2016 die Anzahl der Spamnachrichten mit Schadsoftware im Anhang gegenüber dem Vorjahr.

Mehr als
225 000
Einwohner
der Ukraine waren 2015 stundenlang ohne Strom, nachdem das Strom-verteilnetz Opfer einer Cyberattacke wurde.

Etwa jeden 2. Tag
erfolgt ein gezielter geheimdienstlicher Cyberangriff auf das deutsche Regierungsnetz.

Fotos: plainpicture/fStop/Caspar Benson, xijian/Getty Images, iStockphoto.com, Patrick Strattner/Getty Images, porcorex/Getty Images, kyoshino/Getty Images, RICOWde/Getty Images, Stuart Minzey/Getty Images, Daniel Sambraus/EyeEm/Getty Images

DIE OPEN TELEKOM CLOUD
EINFACH. SICHER. GÜNSTIG.
MEHR INFOS UNTER CLOUD.TELEKOM.DE

ERLEBEN, WAS VERBINDET.