Focus on Security

Ausgabe 06, Juni 2016

SECURITAS

Inhalt

Anlagensicherheit

Benjamin Fiene, Communication Interfaces, befasst sich in der Ausgabe 5-2016 der Zeitschrift GIT Sicherheit, S. 76/77, mit **Funktechnologie im Ex-Bereich**. Auch in der Prozessindustrie komme der drahtlosen Signalübertragung eine stetig steigende Bedeutung zu. Denn in vielen Bereichen der prozesstechnischen Anlagen lasse sich der Kosten- und Zeitaufwand durch den Einsatz von Funktechnologie deutlich reduzieren. Allerdings seien bei der Installation insbesondere der Antennen einige Punkte zu beachten. Der Autor behandelt Nachteile bestehender Lösungen, die Verwendung von Standard-Antennen und -leitungen, die Kommunikation über große Entfernungen, den Aufbau verschiedener Netzwerkstrukturen und die Zertifizierung gemäß ATEX und IECEx. Die Antennenbarriere von Phoenix Contact mache die Hochfrequenzausgänge von Funkmodulen eigensicher gemäß der Zündschutzart Ex i. Sie begrenze die Zündenergie im Fehlerfall, sodass Standardantennen in explosionsgefährdeten Bereichen bis Zone 0 eingesetzt werden könnten. Aufgrund seiner Eigenschaften biete sich die Funktechnologie im Prozessumfeld zum Beispiel zur Überwachung von Füllständen und Temperaturen oder zur Detektierung von Störungen an. Die einfach handhabbaren Wireless-Komponenten seien gemäß ATEX und IECEx zertifiziert, sodass sie in explosionsgefährdeten Bereichen installiert werden könnten.

Anschläge

In der Wochenlage vom 27. Mai berichtet das BKA, dass in der Nacht zum 13. Mai das Jeetzel-Einkaufszentrum in Dannenberg/NI aus noch ungeklärter Ursache gebrannt habe. Es sei Sachschaden in Millionenhöhe entstanden. In dem Gebäudekomplex befänden sich sieben Ladengeschäfte, darunter Filialen von **„KiK" und „Takko".** An beiden Filialen seien Farbschmierereien festgestellt worden. Nahezu zeitgleich hätten Unbekannte in Lüchow/NI ein Jobcenter und eine weitere „KiK"-Filiale massiv mit Eisenrohren und blauer Farbe beschädigt. Die globale Textilindustrie mit Firmen wie „KiK" und „Takko" liege bereits seit Jahren im Zielspektrum linker Straftäter, da die linke Szene deren Geschäftspraktiken als ausbeuterische Unterdrückung ansehe.

Arbeitsschutz

Die FAZ weist am 3. Mai darauf hin, dass die Firma UVEX unter der Bezeichnung RX goggle die erste **Vollsichtbrille mit Korrektionsschutzscheiben** vorgestellt habe. Sie ähnele einer Motorradbrille und erfülle die Anforderungen der Festigkeitsklasse „B" nach der Norm für Schutzbrillen EN 166. Für den Arbeitsschutz im Betrieb seien zertifizierte Materialien notwendig. Die Brille werde deshalb als Einheit von Gestell und Gläsern verkauft. Je nach Fehlsichtigkeit und Material der Kunststoffgläser könne die RX goggle allerdings mehr als 100 Gramm wiegen. Es gebe sie für knapp 100 Euro im Fachhandel. Hinzu kämen die individuellen Gläser.

GIT Sicherheit stellt in Ausgabe 5-2016, S. 87/88, **Otoplastiken mit Filtern** der neuesten Generation vor. Für den Schutz des Gehörs seien maßgeschneiderte Otoplastiken herkömmlichen Einweg- oder Standardlösungen deutlich überlegen. Das belege eine Langzeitstudie der Berufsgenossenschaft Holz und Metall eindrucksvoll. Unter dem Markennamen Forsec gebe es jetzt Otoplastiken mit neu entwickelten Filtern, die auch bei wechselnden Lärmpegeln Schutz bieten, während Warnsignale hörbar blieben. Ein Filter aus Silikon eigne sich vor allem für alle Anwender, die in unterschiedlichen Lärmbereichen arbeiten. Signale, etwa im Gleisoberbau könnten ebenso wahrgenommen werden wie im öffentlichen Straßenverkehr. Der Träger

nehme die individuell angepasste Otoplastik nicht als Fremdkörper in der Ohrmuschel wahr. Das erhöhe die Sicherheit.

GIT Sicherheit befasst sich in der Ausgabe 5-2016, S. 88/89, mit der Technischen Regel für Gefahrstoffe 401 „**Gefährdung durch Hautkontakt**: Ermittlung – Beurteilung – Maßnahmen". Erst wenn technische und organisatorische Schutzmaßnahmen für einen ausreichenden Schutz nicht genügen, kämen persönliche Schutzmaßnahmen zum Einsatz. Dargestellt werden in dem Fachbeitrag der Schutz durch Handschuhe und Hautschutzmittel, die Hautreinigung und die sachgerechte Anwendung von Hautschutzmitteln. Hautschutzmittel sollten so hautschonend wie möglich ausgewählt werden. Reibemittelhaltige Hautreinigungsmittel sollten so selten wie möglich genutzt werden. Bei bestimmten hautbelastenden Tätigkeiten müsse der Unternehmer eine arbeitsmedizinische Pflichtvorsorge durchführen lassen bzw. eine Angebotsvorsorge organisieren.

Aufzugssicherheit

Die FAZ weist am 4. Mai auf den **Anlagensicherheitsbericht 2016 des TÜV** hin. Demnach seien bei 60 Prozent der geprüften Aufzüge in Deutschland Mängel festgestellt worden. 13 Prozent hätten erhebliche Schwachstellen, zum Beispiel defekte Notrufanlagen oder Korrosion an den Tragseilen. 0,6 Prozent würden nach der Prüfung als gefährlich gelten, weil Tragseile verschlissen waren oder Fangvorrichtungen nicht funktionierten. 145.000 Anlagen seien von ihren Betreibern noch nie zur gesetzlich vorgeschriebenen Prüfung angemeldet worden. Die Hersteller blieben dabei, dass Aufzüge trotz der jüngsten Zahlen so etwas wie das sicherste Verkehrsmittel hierzulande seien. Wartung und Reparatur seien Sache der Betreiber. 50 Prozent des Anlagenbestands seien 20 Jahre und älter. Das spreche zwar für die Qualität der Aufzüge, mache aber regelmäßige Wartung nötig, da sie nicht mehr auf dem heutigen Stand der Technik sein könnten. Der Verband gehe von einer Dunkelziffer von 100.000 Anlagen aus, die nicht regelmäßig gewartet werden. 2015 habe es vier tödliche Unfälle gegeben, allerdings nicht durch Abstürze, sondern durch Stolpern beim Einsteigen an der Aufzugskante oder verbotene Ausflüge in den Aufzugsschacht.

Bahnsicherheit

350 Mio. Euro zahlt die Deutsche Bahn Jahr für Jahr für Inspektion und Reparaturen der Gleise, berichtet die WirtschaftsWoche am 6. Mai. Dieser Wartungsaufwand ließe sich sparen, wenn etwa **Weichen** drohende Störungen selbst meldeten. Genau das ermöglichten vernetzte Hightechsensoren und eine Big-Data-Analyseplattform des Start-ups Konux. Das System erfasse Erschütterungen und Bewegungen an Weichen und leite daraus den Wartungsbedarf ab. Bis Jahresende 2016 solle die Technik rund 800 Weichen digital überwachen, bis 2019 mehrere Zehntausend.

Biometrie

Der Behörden Spiegel befasst sich in der Mai-Ausgabe mit der biometrischen Erkennung von Personen im Hochsicherheitsbereich. Ein Forschungsprojekt der Hochschule Bonn Rhein-Sieg setze auf **Nahinfrarotwellen**. Die Haut jedes Typs unterscheide sich im nahinfraroten Bereich signifikant von anderen Materialien, zum Beispiel Masken, sodass Fälschungen deutlich leichter zu erkennen seien. Die Intensität der für das System zur Gesichtserkennung verwendeten Nahinfrarotstrahlung betrage rund ein Zehntel dessen, was bei normaler Infrarotstrahlung üblich ist. Auch für die Augen sei die Methode unge-

fährlich. Sobald das Projekt ausgereift sei, könne es unter anderem in Form sogenannter E-Gate-Systeme an neuralgischen Punkten wie Grenzübergängen oder Fußballstadien eingesetzt werden. In einem anderen neuen Forschungsprojekt solle ein dreidimensionaler Fingerscanner entwickelt werden, mit dessen Hilfe auch Kinder und Jugendliche, z. B. im Rahmen der Flüchtlingsregistrierung, eindeutig identifiziert werden könnten. Der Fingerscanner erfasse nicht nur die oberste Hautschicht, sondern den gesamten Finger.

Brandschutz

Sicherheit.info stellt am 27. Mai die **Ansaugrauchmelder SecuriRAS ASD** und die linienförmigen Wärmemelder SecuriSENS ADW von Securiton vor, die zuverlässige Branderkennung gerade auch in schwierigen Umgebungen garantierten. Bisher hätten Techniker die Meldegeräte mit ihrem Laptop persönlich besuchen müssen, um sie zu konfigurieren und zu warten. Damit sei jetzt Schluss. Der Komfort- und Effizienzgewinn durch Config over Line sei kostenlos. Nach dem Gratis-Update der Securifire-Studiosoftware und der Gerätesoftware stünden praktisch sämtliche Funktionen der Config-Tools für die Fernbedienung der Melder zur Verfügung. Der Datenaustausch zwischen den Sonderbrandmeldern und der Brandmeldezentrale erfolge über die bestehende Securiline-Extended-Ringleitung mittels Tunneling-Technologie. Für den Fernzugriff seien somit keine zusätzlichen Kabelinstallationen nötig. Config over Line ermögliche einen schlankeren und besseren Service mit hoher Effizienz, Wirtschaftlichkeit und Bedienerfreundlichkeit.

Business Continuity

Albert Indrist, Mobiliar Protekta Risiko-Beratungs AG, und Dr. Heiner Eichenberger, Safrima AG, befassen sich in der Zeitschrift Sicherheitsforum, Ausgabe 2-2016, S. 58/59, mit Business Continuity Management. Sie thematisieren die Risikoanalyse, die Business Impact Analyse (BIA) und die Business Continuity-Planung (BCP). Die BIA zeige auf, welche maximal tolerierbare Ausfallzeit (MTA) je Geschäftsprozess für die Wiederherstellung nach einem Ausfall oder für die Überbrückung der MTA angenommen werden muss. Im Ernstfall zeige sich leider meistens, dass sich die verschiedenen Einflussbereiche – finanzielle Auswirkungen, Reputationsschäden, rechtliche Konsequenzen, betriebliche Auswirkungen – gegenseitig erheblich beeinflussen und nicht zuletzt gegenseitig verstärken. Nicht alles, was wichtig ist, sei auch zeitkritisch. Bei der BCP liege der Fokus auf zeitkritischen Prozessen und Ressourcen mit einer kurzen MTA. Mindestens zeitkritische Geschäftsprozesse, die sofort aus dem Stand funktionierende Überbrückungs- und/oder Ersatzlösungen brauchen, müssten auch regelmäßig getestet werden.

Drohnen

DHL habe ein positives Fazit ihrer Versuche mit einer neuartigen **Paketdrohne** in Oberbayern gezogen, meldet silicon.de am 10. Mai. Der Schwerpunkt des Testlaufs für die dritte Generation des sogenannten Paketkopters von Januar bis März in Reit im Winkl sei es gewesen, die Einbindung der Lieferdrohne in logistische Abläufe der Paketzustellung zu erproben. Konkret sei es dabei um die automatisierte Be- und Entladung des Paketkopters mittels einer speziell dafür entwickelten Packstation, dem Parcelcopter SkyPort, gegangen. Darüber hätten Privatkunden Pakete versenden und empfangen können. Im Rahmen des Projekts seien laut DHL 130 derartige autonome Be- und Entladungen durchgeführt worden. Für eine Lieferung über die acht Kilometer lange Strecke benötige der Paketkopter unter günstigen Bedingungen lediglich acht Minuten.

Dr. Wolfgang Koch, Fraunhofer Institut FKIE, nimmt in der Mai-Ausgabe des Behörden Spiegel zur **multisensoriellen Drohnenabwehr** Stellung. Drohnen seien schon zur Spionage bei Industrieanlagen oder Kritischen Infrastrukturen, zum Mitschnitt sensitiver Gespräche durch fliegende Richtmikrophone und vieles mehr missbraucht worden. Zur raschen und zuverlässigen Erkennung von Drohnen seien leistungsfähige Sensoren wesentlich, die unterschiedliche Aspekte anfliegender Drohnen erfassen. Zu einem Drohnenerkennungssystem würden Sensoren aber erst durch leistungsfähige Algorithmen der Multisensordatenfusion. Aufgrund seiner Reichweite und Allwetterfähigkeit sei drohnenoptimiertes Radar zentral. Von Drohnen reflektierte Echos würden analysiert, um Orts- und Geschwindigkeitsdaten sowie den Typ zu schätzen. Radardaten seien mit Datenströmen bildgebender Sensoren zu fusionieren, die typischerweise mehrere Spektralbereiche erfassen. Ferner machten Eigenemissionen Drohnen detektierbar, etwa durch Funkfernsteuerung. Durch Auswertealgorithmen würden die Drohne und ihr Pilot lokalisierbar. Ebenfalls vielversprechend seien akustische Emissionen. Die Bedeutung der Multisensordatenfusion sei evident. Bei allem Gefährdungspotenzial hätten „Jedermann-Drohnen" den Vorteil, dass sie kaum elektronischen Selbstschutz bieten. „Soft kill" könne daher ihre Funktionalität einschränken. Teilweise könnten Methoden der elektronischen Kampfführung eingesetzt werden, etwa um Fernsteuerungen zu übernehmen. Sehr einfach sei dies bei WLAN-basierten Ansätzen. Bei „Kamikaze"-Drohnen wäre an Abfangdrohnen zu denken, die etwa durch ein Netz versuchten, die Bedrohung zu neutralisieren.

Einbruchskriminalität

Sicherheit.info weist am 25. Mai darauf hin, dass Daten aus der Notrufzentrale von Securitas Deutschland eine **Fortsetzung des Anwachsens von Wohnungseinbrüchen auch im Jahr 2016** signalisieren. Im ersten Quartal 2016 hätten die Einbruchalarme um 5,7 Prozent zugenommen. Auffällig stark betroffen seien Baustellen, Logistik, Drogerien sowie Schulen und Kitas. Bei den versuchten Einbrüchen (40 Prozent) falle auf, dass Banken (22 Prozent), private Haushalte (11 Prozent), Einzelhändler (11 Prozent) und Drogeriemärkte (8 Prozent) besonders stark betroffen seien. Für einen effektiven Einbruchschutz seien mehrere Komponenten nötig: mechanischer Schutz an Fenstern und Türen, Alarmanlagen, die an eine ständig besetzte Notrufleitzentrale aufgeschaltet sind, ein zertifiziertes und anerkanntes Sicherheitsunternehmen, das im Alarmfall sofort intervenieren kann sowie eine intakte und aufmerksame Nachbarschaft.

Ermittlungen

Der Behörden Spiegel weist in seiner Mai-Ausgabe darauf hin, dass das BKA seit dem 22. Februar nach richterlicher Anordnung eine neue Software zur Überwachung der Telekommunikation einsetzen darf. Der **neue Trojaner** funktioniere nur auf Windows-Rechnern und sei daher nur in einem sehr engen Rahmen einsatzfähig. Produkte von Apple und auch Messenger-Dienste wie Whats App könnten mit der aktuellen Version nicht abgehört werden. Die Überwachung mobiler Endgeräte sei mit der Software, die das BKA drei Jahre lang entwickelt habe, generell nicht möglich. Das BKA werde künftig zwei verschiedene Arten von Trojanern einsetzen dürfen: einen, der nur die Telekommunikation eines Verdächtigen überwacht, und einen weiteren, der keine Kommunikation überwacht, sondern eine heimliche Onlinedurchsuchung eines Computers durchführt.

Gebäudesicherheit

Es gebe kaum eine Gebäudekomponente, bei der Planer heute nicht auf passende Daten des **Building Information Modeling** (BIM) zurückgreifen könnten, schreibt GIT Sicherheit in der Ausgabe 5-2016, S. 26/27. Es sei daher naheliegend, auch die Sicherheitstechnik in das BIM zu integrieren. Mit den BIM-Daten sei ein echter technischer Mehrwert verbunden. So enthielten die Dateien für die Videokameras auch detaillierte Angaben zum Sichtfeld der einzelnen Modelle, sodass schon in einem sehr frühen Planungsstadium eine Optimierung der Überwachung möglich ist. Dabei könnten sogar die Kameraeinstellungen simuliert werden. Zudem stünden über die BIM-Dateien Funktionen der intelligenten Videoanalyse schon während der Planung zur Verfügung. Gerade bei Gebäuden mit hohem Gefährdungspotenzial würden schon die Raumaufteilung und die Gestaltung von Zu- und Abwegen stark von Sicherheitsaspekten beeinflusst, und angesichts der globalen Sicherheitslage werde dies in immer mehr Neuentwicklungen der Fall sein. Eine frühzeitige Einbindung der Sicherheitstechnik führe zur Berücksichtigung teilweise sehr komplexer Abhängigkeiten und Wechselwirkungen zwischen der Sicherheitstechnik und dem Gebäudedesign schon bei der Planung. Eine Herausforderung für die gesamte Industrie stelle derzeit noch der geringe Standardisierungsgrad bei BIM dar.

IT-Sicherheit

Mit dem **Stand der IT-Sicherheitsforschung** in Deutschland befasst sich die FAZ am 4. Mai. Seit Cyberkrieger 2015 selbst in die Server der renommierten Sicherheitsfirma Kaspersky eindrangen und IT-Experten ein geknacktes Auto mit seinem hilflosen Fahrer in den Straßengraben beförderten, scheine in der vernetzten Welt nicht mehr viel sicher. Cloud, Big Data, Internet der Dinge und Industrie 4.0 potenzierten die Gefahren. An den Schnittstellen der Systeme öffneten sich überall neue Sicherheitslücken. Um die Angriffsflächen zu minimieren, fordere der IT-Sicherheitsforscher Michael Backes auch Investitionen in eigene Infrastrukturen. Bei Betriebssystemen und Prozessoren sei technologische Autarkie angesichts des Rückstands zu den USA utopisch, Microcontroller für die vernetzte Industrie und Router sollte Europa aber (wieder) selbst entwickeln. Eine systematische Sicherheitsforschung habe sich in Deutschland, das wegen seiner starken Industrie ein beliebtes Ziel von Hackerangriffen sei, seit einem knappen Jahrzehnt entwickelt. Auf die gewachsene Gefahr habe das BMBF vor fünf Jahren mit der Gründung von zwei großen Kompetenzzentren in Saarbrücken und Darmstadt und einem kleineren in Karlsruhe geantwortet. Dem Ministerium liege besonders am Schutz der kritischen Infrastrukturen.

Am Darmstädter „Center for Research in Security und Privacy" (Crisp), das Bund und Land derzeit mit sechs Mio. Euro im Jahr fördern, forschten über 400 Wissenschaftler der beiden Darmstädter Hochschulen und des Fraunhofer Instituts für Sichere Informationstechnologie (FIS). Die Forschung konzentriere sich auf gebrauchsfertige Produkte wie die für 2016 angekündigte „Volksverschlüsselung" oder den „Appicaptor", eine Prüfsoftware für Apps. Das Saarbrücker „Center for IT-Security, Privacy and Accountability" (Cispa) bilde mit zwei Max-Planck-Instituten, einem Exzellenzcluster und dem Deutschen Zentrum für Künstliche Intelligenz einen stärker auf Grundlagenforschung gerichteten Forschungsverbund. Die meisten Produkte im Internet der Dinge seien für Hacker leichte Beute. Das größte Sicherheitsrisiko sei aber immer noch der sorglose Umgang der Bürger mit ihren persönlichen Daten. Man werde sich auf geringerem Sicherheitsniveau einrichten müssen, in der Hoffnung, dass die Forschung die größeren Lücken schließt.

Wie silicon.de am 9. Mai meldet, hat das Unternehmen Trustwave eine Sicherheitslücke in der von Lenovo auf nahezu allen von ihm ausgelieferten PCs, Notebooks und Tablets vorinstallierten **Software Lenovo Solution Center** entdeckt. Sie sei unter anderem zur Verwaltung von Sicherheitsfunktionen gedacht und gebe Nutzern einen Überblick über den Zustand von Software, Hardware und Netzwerkverbindungen. Die Schwachstelle erlaube die unautorisierte Ausweitung von Benutzerrechten. Angreifer könnten so unter Umständen die Kontrolle über einen der Lenovo-Systeme übernehmen sowie Malware einschleusen und ausführen. Betroffen seien wahrscheinlich mehrere Millionen Nutzer. Das Unternehmen biete bereits ein Update auf Version 3.3.002 an. Die Kunden müssten die Software manuell starten und würden erst dann aufgefordert, die Aktualisierung zu installieren.

Smartphone-Hersteller müssen US-Behörden peinliche Fragen zu ihrer **Update-Politik** beantworten, berichtet silicon.de am 10. Mai. Die acht Firmen sowie mehrere Mobilfunkanbieter in den USA sollten der Federal Trade Commission (FTC) und der Federal Communications Commission (FCC) erklären, nach welchen Kriterien sie entscheiden, „ob sie eine Sicherheitslücke eines bestimmten mobilen Geräts schließen", welche Schwachstellen diese Geräte hätten sowie ob und wann diese Schwachstellen beseitigt würden. Als Herausgeber des Mobilbetriebssystems Android stelle Google zum Beispiel in der Regel einmal pro Monat Sicherheitsupdates zur Verfügung. Bei Samsung seien die zugesicherten Updates auf wenige Spitzenmodelle beschränkt. Apple habe keinen festen Zeitplan, um Lücken in iOS zu schließen.

Mit **Cyberrisiken für die Industrie 4.0** befasst sich der Behörden Spiegel in seiner Mai-Ausgabe. Eine im Auftrag des BMWi entwickelte Studie eines Konsortiums unter Führung von Rohde & Schwarz komme zu dem Ergebnis, dass die autonome Gerätekommunikation neue Sicherheitslücken für Hacker und andere Cyberkriminelle schaffe. Es fehlten klare gesetzliche Regularien und ein technisches Gesamtkonzept zum Schutz der vernetzten Industrie. Hersteller technischer Lösungen sollten geeignete Hard- und Softwarekomponenten zur Umsetzung des Szenarios „Secure Plug & Work" entwickeln, hardwarebasierte Sicherheitsanker in allen Endgeräten bereitstellen sowie Integritätsprüfungen der eigenen Firmware, Anwendungen und Konfigurationsparameter während des Bootens und zur Laufzeit ermöglichen. Aber auch neue intelligente und adaptive Anomalie-Erkennungssysteme seien künftig erforderlich. Eine weitere technische Anforderung: Modelle und Tools müssten langfristig in der Lage sein, auch komplexe Prozesse abzubilden. Nur so könnten Entscheidungsträger rationale und fundierte Entscheidungen im Zusammenhang mit organisatorischen IT-Sicherheitsmaßnahmen treffen.

Nach einem Bericht von zeit.de vom 24. Mai hat Google auf der Entwicklerkonferenz I/O eine Idee vorgestellt**, Passwörter abzuschaffen**. Bis Ende 2016 sollen alle Android-Entwickler sogenannte Trust Scores in ihre Apps integrieren können. Jeder Besitzer eines Android-Smartphones bekomme einen **individuellen Trust Score**. Dieser setze sich aus verschiedenen Datenpunkten zusammen, die direkt über das Gerät ermittelt würden. Dazu zählten etwa der Standort via GPS, Gesichtserkennung und Fingerabdruck, aber auch das Tippverhalten, wie oft bestimmte Apps gestartet werden und selbst wie das Smartphone behalten wird oder mit welchen Netzwerken und anderen Geräten es verbunden ist. Künftige Android-Apps könnten statt Passwörtern den Trust Score nutzen. Ein gestohlenes Smartphone sei derzeit in den meisten Fällen bloß durch eine PIN oder einen Fingerabdruck gesichert. Ein Trust Score, der zusätzlich weitere biometrische Verfahren und das Nutzerverhalten verwendet, könnte es Dieben weiter erschweren, sich unerlaubten Zugriff zu verschaffen.

Heise.de meldet am 24. Mai, beim BSI sollten „**Mobile Incident Response Teams**“ eingerichtet werden, die bei schweren Hackerangriffen betroffenen Firmen schnell zu Hilfe eilen sollen. Dabei sei ein enger Austausch und eine vertrauensvolle Zusammenarbeit zwischen Staat und Wirtschaft unabdingbar, um Cybersicherheit in Deutschland auf hohem Niveau zu gewährleisten.

Silicon.de berichtet am 23. Mai, der Sicherheitsanbieter Duo Security warne vor einer bereits seit Längerem bekannten Schwachstelle in Android, die womöglich bis zu 60 Prozent aller Geräte mit Googles Mobilbetriebssystem betreffe. Der Bug finde sich in der Sicherheitsfunktion Secure Execution Environment des Chipanbieters Qualcomm, von dem rund 80 Prozent aller **Central Processing Units** für Android-Geräte stammten. Schadsoftware, die die Sicherheitslücke ausnutzen kann, werde über infizierte Apps verbreitet, die laut den Forschern auch schon erfolgreich Googles Sicherheitskontrollen für den Play Store überlistet hätten. Im Anschluss könne ein Angreifer dann Sicherheitsfunktionen aushebeln und auf diese Weise unter Umständen die komplette Kontrolle über ein System übernehmen. Die Anfälligkeit in der Qualcomm-Sicherheitsfunktion führe konkret dazu, dass sich besonders heikle Operationen wie die Verwaltung kryptografischer Schlüssel nicht mehr getrennt vom übrigen Betriebssystem in einem geschützten Bereich ausführen lassen.

IuK-Kriminalität

Ransomware gehöre zu den hinterhältigsten und gemeinsten Maschen, die Cyberkriminelle im Gepäck haben, schreibt die FAZ am 3. Mai. Es handele sich um Schadsoftware, die Computernutzer von ihrem eigenen Gerät ausschließt. Sie verschlüssele Dateien oder sperre den Zugang komplett. Nur wer zahlt, sehe seine wertvollen Dokumente und kostbaren Familienfotos irgendwann mal wieder, so die Drohung der Malware-Programmierer. In einer Online-Umfrage der BSI hätte ein Drittel der Unternehmen bekundet, in den vergangenen sechs Monaten ein Opfer von Ransomware geworden zu sein. Drei Viertel der Infektionen seien auf infizierte E-Mail-Anhänge zurückzuführen. Auch sogenannte Drive-by-Angriffe, verursacht durch das Surfen auf infizierten Hompages, spielten eine wichtige Rolle. 70 Prozent hätten angegeben, dass einzelne Arbeitsplatzrechner befallen waren. In jedem fünften der betroffenen Unternehmen sei es sogar zu einem erheblichen Ausfall von Teilen der IT-Infrastruktur gekommen. 11 Prozent hätten wichtige Daten verloren. Das BSI beobachte immer neue Wellen von Ransomware-Angriffen. Fast alle Unternehmen – 86 Prozent – hätten zusätzliche Maßnahmen getroffen, um sich besser vor Ransomware zu schützen. Sie sensibilisierten ihre Mitarbeiter und verstärkten die Abwehr, unter anderem durch eine bessere Virenerkennung für die Computer oder durch zusätzliche Datensicherungen. Das Problem Ransomware dürfte sich so schnell nicht lösen lassen. Denn ein attraktives Profil kennzeichne das kriminelle Geschäftsmodell: niedriges Risiko für die Entwickler, verbunden mit hohen möglichen Erträgen. „Seit Mitte September 2015 hat sich die Bedrohungslage durch Ransomware deutlich verschärft“, konstatiere das BSI in einer Analyse.

Silicon.de weist am 2. Mai auf einen aktuellen Bericht von Kaspersky Lab zu **DDoS-Attacken** im ersten Quartal 2016 hin. Cyberkriminelle bedienten sich offenbar wieder vermehrt der http-DDoS-Angriffsmethode. Zur Umsetzung solcher Attacken sollen sie immer häufiger das DNSSEC-Protokoll nutzen. Im Allgemeinen sei die Zahl der Verstärkungsattacken gegenüber dem Vorjahr etwas zurückgegangen, dafür habe sich ihre Durchschlagskraft vervierfacht.

Wie die FAZ am 18. Mai meldet, warnt Kaspersky vor der neuen Version einer

Schadsoftware, mit deren Hilfe Hacker die **Kontrolle über Geldautomaten** übernehmen und auf diese Weise Karteninformationen stehlen könnten. Das Programm erlaube es ihnen auch, sich den gesamten Geldbestand in dem Automaten auszahlen zu lassen. Die Kriminellen gingen unauffällig vor, sodass Jahre vergehen könnten, bis eine Infektion bemerkt wird. Möglich werde der Angriff dadurch, dass viele Geldautomaten noch mit dem 15 Jahre alten Microsoft-Betriebssystem Windows XP laufen, für das diverse Sicherheitslücken bekannt seien. Die Kriminellen erlangten Zugriff entweder über das Netzwerk der Bank oder den USB-Anschluss des Automaten. Die Schlösser der Maschinen ließen sich zum Teil mit einem Kugelschreiber öffnen. Die bisher übliche Vorgehensweise sei es gewesen, am Kartenschlitz des Geldautomaten kleine Lesegeräte, sogenannte Skimmer, zu platzieren, mit denen Daten des Magnetstreifens der Karten ausgelesen wurden. Mit der neuen Variante werde der Geldautomat selbst zum Skimminggerät.

Wieder einmal seien Antivirenprodukte prominenter Hersteller von schweren Sicherheitslücken betroffen, meldet golem.de am 18. Mai. Angreifer könnten Systeme mit Norton- und Symantec-Software zum Absturz bringen, bei Windows-Rechnern soll es besonders schlimm sein. Die Sicherheitsfirmen Symantec und Norton hätten mehrere kritische Sicherheitslücken in ihren Produkten gepatcht. Die Schwachstelle betreffe die **Scan-Engine von Symantec**, die auch von Norton verwendet werde. Würden der Engine Dateien mit einem manipulierten PE-Header untergeschoben, könnten damit Speicherfehler provoziert werden. Nach Angaben von Tavis Ormandy sind alle Versionen der Software betroffen – also unter Windows, Mac OS X, Linus und Unix.

Nach einer Meldung in der FAZ am 14. Mai warnt der Verfassungsschutz vor **russischen Cyberangriffen**. Der Cyberraum ist nach den Worten des BfV-Präsidenten ein Ort hybrider Kriegsführung. Er eröffne neue Operationsräume für Spionage und Sabotage. Russische nachrichtendienstliche Cyberangriffe seien Teil mehrjähriger international ausgerichteter Operationen. Inzwischen zeigten russische Nachrichtendienste auch Bereitschaft zur Sabotage. Eine Kampagne zur Cybersabotage trage den Namen „Sandworm". Sie ziele neben Regierungsstellen auf Telekommunikationsunternehmen, Energieversorger oder Hochschul- und andere Bildungseinrichtungen.

Knapp vier Jahre nach einem Hackerangriff habe das Internet-Netzwerk Linkedin seine Nutzer zu einem Passwort-Wechsel aufgefordert, berichtet die FAZ am 20. Mai. Bei dem Angriff seien damals die Login-Daten von mehr als 100 Mio. Mitgliedern gestohlen worden. Betroffen seien offenbar E-Mail-Adressen und Passwörter. Als Sicherheitsmaßnahme habe Linkedin die Passwörter aller Nutzerkonten für ungültig erklärt, die vor 2012 angelegt worden seien. Zudem informiere das Netzwerk einzelne Nutzer, die ihr Passwort ändern müssten.

Munich Re bekämpft die Cyberkriminellen, titelt die FAZ am 23. Mai. Gemeinsam mit dem Versicherer von Cyberhaftungsrisiken Beazley will Munich Re großen Konzernen eine umfassende Absicherung für ihre digitalen Vermögenswerte und IT-Infrastrukturen anbieten, und zwar mit einer Deckungssumme bis 100 Mio. Euro. Nach einer Lloyd's Schätzung werde der Weltmarkt für Cyberversicherungen in diesem Jahr bereits 2,5 Mrd. Dollar ausmachen und bis 2020 auf rund acht Mrd. Dollar steigen. Künftig sollten auch zunehmend mittelständische Unternehmen ihre Cyberrisiken über speziell erweiterte Haftpflichtpolicen abdecken können. Deutlich weniger als 5 Prozent der vereinbarten Haftungssumme soll Firmen der Schutz kosten.

Heise.de weist am 23. Mai auf einen Bericht der Melde- und Analysestelle Informationssicherung (Melani) hin, wonach bei einem Hackerangriff auf den staatseigenen Schweizer

Rüstungskonzern RUAG **mehr als 20 Gigabyte Daten entwendet** worden seien. Eine Serie von Hackerangriffen gegen die RUAG habe bereits im Dezember 2014 begonnen und sei über ein Jahr lang unentdeckt geblieben. Für den Angriff hätten die Angreifer eine seit mehreren Jahren im Umlauf befindliche Schadsoftware der Turla-Familie benutzt.

Magnetfeld-Sensoren

Einbrecher gehen naturgemäß gern unbeobachtete Wege. Nach einem beherzten Sprung über den Gartenzaun hätten sie mehr Zeit und Ruhe für die Arbeit im Verborgenen, schreibt GIT-Sicherheit.de am 5. April. Dass solche Manöver nicht unbemerkt ablaufen, dafür könne ein dünnes Kabel sorgen, das Physiker der Saar-Universität ursprünglich zur Sicherung großer Flughafen-Gelände entwickelt hätten. **Sensible Magnetfeld-Sensoren**, die im Kabel aneinandergereiht sind, nähmen jede noch so kleine Änderung des Erdmagnetfeldes wahr, das sie umgibt, erklärt Professor Uwe Hartmann. Das könnten die Erschütterungen der Drahtmaschen sein, wenn jemand über den Zaun klettert, oder der Reißverschluss an der Jacke dessen, der nichts Gutes im Schilde führt. Geht dieser etwa über das im Boden der Einfahrt eingelassene Kabel, stelle auch dies für die Sensoren eine Abweichung von den vorherigen Messwerten und Signalmustern dar. Die kleinen Messfühler seien vernetzt und meldeten jede noch so kleine Störung in die zentrale Auswerteeinheit, die in einem winzigen Microcontroller untergebracht sei. Dort werde die Meldung weiterverarbeitet und automatisch von Fehlalarmen unterschieden, die etwa durch harmlosen Wind am Zaun ausgelöst wurden. „Die Signalmuster unterscheiden sich je nach Art der Störung. Durch unsere bisherigen Forschungen können wir etliche Arten von Erschütterungen und Änderungen des Magnetfeldes einzelnen Störungen zuordnen, also erkennen, ob sie von einem Menschen, von Wind, einem Auto oder einem Tier herrühren", so Hartmann. Daher könne das System auch erfassen, ob Weidetiere oder der Hund das Gebiet verlassen, auf dem sie bleiben sollen – ein kleines Metallstück am Halsband genüge. Damit die „Zentrale" von selbst Übertritte ihrem Verursacher zuordnen könne, simulierten die Physiker Störungen an Testzäunen. Mit ihren Ergebnissen lernten sie das System für typische Ereignisse an, indem sie diese mathematisch modellieren und die Auswerteeinheit entsprechend programmieren. Das System gebe genau an, wo die Störung gemessen wurde, was vor allem bei großen Grundstücken interessant sei. Die Sensoren seien nahezu verschleißfrei, und die Messung sei unabhängig von der Witterung. Regen oder Nebel könnten ihnen nichts anhaben.

Maritime Sicherheit

Der ASW weist im Newsletter vom 20. Mai auf einen Hintergrundbericht der Result Group GmbH zur maritimen (Un)Sicherheit in Westafrika hin. Weltweit seien in den vergangenen zwölf Monaten **gewalttätige Angriffe auf Schiffe zurückgegangen**. Die Zahl der gemeldeten Übergriffe auf Schiffe überwiege im südostasiatischen Raum (Straße von Malakka). Am Horn von Afrika liege die Zahl der Lösegelderpressungen auf dem tiefsten Stand seit Jahren, ganz im Gegensatz zu Westafrika, wo die Bandbreite der kriminellen Übergriffe im Golf von Guinea sogar gewachsen sei. Der mittlerweile zu einem Wirtschaftszweig entwickelte Rohöldiebstahl sei um die Deliktsbereiche Menschen- und Drogenschmuggel und Piraterie expandiert. Die hohe Gewaltbereitschaft in den westafrikanischen Gewässern stelle ein großes Problem dar. Zwei Drittel der weltweit registrierten Entführungen fänden in den Küstengewässern von Nigeria und der Elfenbeinküste statt. Weil die Anrainerstaaten am Golf von Guinea regelmäßig die Einfahrt von Schiffen mit

ausländischem Sicherheitspersonal an Bord verbieten, könne eine Übertragung der am Horn von Afrika erfolgreichen Strategie der Kombination aus staatlicher Seeraumüberwachung und privatwirtschaftlichen Schutzmaßnahmen nicht umgesetzt werden. Die EU habe eine Expertenkommission ins Leben gerufen. Auf der Grundlage ihrer Arbeitsergebnisse möchte sich die EU verstärkt um die lokalen und regionalen Akteure bemühen und versuchen, diese zusammenzubringen. In der Arbeitsgruppe seien drei übergeordnete Ziele definiert worden: die Stärkung der legislativen, judikativen und exekutiven Rahmenbedingungen, die Stärkung von operativen Fähigkeiten und die Einführung von Kommunikationssystemen zum verbesserten Austausch zwischen den Anrainern.

Maschinensicherheit

Dipl. El. Ing. HTL/Wirtschaftsingenieur Urs Kaufmann thematisiert in der Ausgabe 2-2016 des Sicherheitsforums, S. 60–63, **gesetzliche Anforderungen von verketteten Maschinen**: Was im allgemeinen Sprachgebrauch als Produktionslinie, verkettete Maschine oder komplexe Anlage bezeichnet wird, sei eine Maschine im Sinne der EG-Maschinenrichtlinie 2006/42/EG. Der Autor zeigt auf, wenn es sich um eine Ansammlung von Einzelmaschinen und wann um eine verkettete Maschine handele, und wer welche gesetzlichen Anforderungen beachten müsse. Er beantwortet folgende Fragen: Was ist eine verkettete Maschine? Wer ist Hersteller einer verketteten Maschine? Welche gesetzlichen Anforderungen gibt es? Welche Dokumente sind einzufordern? Was bedeutet die Beurteilung der verketteten Maschine? Welche Validierungen müssen durchgeführt werden? Was passiert, wenn eine Maschine ersetzt oder ergänzt wird? Eine verkettete Maschine sei gegeben, wenn ein produktionstechnischer Zusammenhang gegeben ist, und die einzelnen Maschinen sicherheitstechnisch als Gesamtheit funktionieren. Der Hersteller müsse die gesetzlichen Anforderungen der Maschinenrichtlinie 2006/42/EG erfüllen. Als Hersteller der verketteten Maschine gelte derjenige, welcher die verkettete Maschine aus Maschinen zusammenbaut oder zusammenbauen lässt, wenn vertraglich nichts anderes vereinbart sei. Vor allem müssten bei der verketteten Maschine die sicherheitstechnischen Schnittstellen zwischen den Maschinen überprüft werden und deren Konformität mit der Maschinenrichtlinie als Ganzes mit einer EG-Konformitätserklärung bestätigt werden.

Perimeterschutz

Aspekte einer effektiven und effizienten Perimetersicherung beleuchtet GIT Sicherheit in der Ausgabe 5-2016, S. 58/59. Als ein sehr wirkungsvolles und kosteneffizientes System für die Absicherung von Zäunen habe sich das **Zaunsicherungssystem FlexZone** erwiesen. Es eigne sich für fast jeden Zauntyp und lasse sich durch seine vielfältigen Möglichkeiten der Parametrierung so an die jeweiligen Umgebungsbedingungen anpassen, dass optimale Alarmierungseigenschaften mit geringsten Fehlalarmauslösungen verbunden werden. Bei diesem System sei eine einzige Auswerteeinheit theoretisch in der Lage, Zaunstrecken von bis zu 600 Metern Länge zu überwachen und in bis zu 60 Zonen zu unterteilen. Sollte die Umgebung ein System erfordern, das absolut immun gegen elektronische Störungen ist, böten sich **fiberoptische Systeme** an, die auf dem Prinzip der Übertragung von Lichtwellen arbeiten. Senstar biete mit dem FiberPatrol System ein Produkt an, das in der Lage sei, mit einer Auswerteeinheit Strecken von bis zu 24 km Zaunlänge zu überwachen. Barriereunabhängig gebe es erdverlegte Systeme, die vor, hinter oder ganz ohne physische Barrieren Grundstücke und Objekte absichern könnten. Diese Systeme würden im Boden verlegt und bildeten ein hochfrequentes, unsichtbares Feld.

Mit einer einzigen Auswerteeinheit könnten Strecken bis zu 800 Meter überwacht werden. Alle Systeme könnten zudem miteinander oder mit weiteren Drittsystemen kombiniert werden, um unterschiedlichsten Umgebungsbedingungen und System- und Sicherheitsanforderungen gerecht zu werden.

Polizeiliche Kriminalstatistik (PKS)

Am 23. Mai haben Bundesinnenminister de Maizière und der Vorsitzende der IMK die PKS 2015 vorgestellt. 6.330.649 Straftaten wurden in Deutschland 2015 polizeilich registriert. Gegenüber dem Vorjahr bedeutet dies einen Anstieg um 4,1 Prozent. Die Häufigkeitszahl (Straftaten pro hunderttausend Einwohner – HZ) erhöhte sich von 7.350 auf 7.797 Fälle. Ohne die strafbaren ausländerrechtlichen Verstöße waren es allerdings nur 5.927.908 und die HZ sank gegenüber 2014 um 0,5 Prozent. Die Gesamtaufklärungsquote lag bei 53,4 Prozent (2014: 53,7 Prozent). Wie in den Vorjahren dominierten auch 2015 die Diebstahlsdelikte, und zwar mit 39,2 Prozent. Besorgniserregend angestiegen sind 2015 wiederum Fälle des Wohnungseinbruchdiebstahls, die schon 2011 um 9,3 Prozent, 2012 um 8,7 Prozent, 2013 um 3,7 Prozent und 2014 um 1,8 Prozent zugenommen hatten. 2015 betrug der Anstieg 9,9 Prozent auf 167.136. Im Durchschnitt wurden damit 2015 mehr als 19 Wohnungseinbrüche stündlich begangen. Signifikant zugenommen haben ferner 2015 gegenüber dem Vorjahr ausländerrechtliche Straftaten (um 157,5 Prozent auf 246.345), Diebstähle aus Verkaufsräumen (um 6,1 Prozent auf 26.834), Waren- und Warenkreditbetrugsfälle (um 4,9 Prozent auf 14.215). Signifikant abgenommen haben Fälle strafbarer Datenveränderung und Computersabotage (um 37,6 Prozent auf 2.130), Tankbetrugsfälle (um 7,8 Prozent auf 6.753), Sachbeschädigungen (um 4 Prozent auf 245.095) und Beleidigungen (um 3 Prozent auf 6.684). Die Kriminalitätsbelastung war 2015 am größten im Land Berlin (HZ 16.414), am geringsten in Baden-Württemberg (HZ 5.761). Unter den Großstädten ab 200.000 Einwohner war Frankfurt am Main am stärksten (HZ 16.950) und Bielefeld am geringsten belastet (HZ 8.499). Eine ausführlichere Zusammenfassung – insbesondere zu den die Wirtschaft besonders belastenden Kriminalitätsphänomenen – findet sich auf der Webseite von Securitas Deutschland (Presse/Sicherheitslage).

Tunnelsicherheit

In Ausgabe 2-2016 der Zeitschrift Sicherheitsforum, S. 15–17, erläutert Catharina Bujnoch, Siemens Schweiz AG, den **Brand- und Evakuierungsschutz des Gotthard-Basistunnels**. Die Tunnelröhren seien alle 325 Meter durch Querschläge verbunden, sodass die Zugpassagiere im Brandfall in die andere Röhre flüchten könnten. An den beiden je 600 Meter langen Nothaltestellen pro Tunnelröhre sei eine Evakuierung von bis zu 1.000 Personen möglich. Dass es dazu gar nicht kommen solle, dafür sei die Anlage mit unzähligen Sensoren, Überwachungseinrichtungen und Steuerungen bestückt, die über Tausende Kilometern Glasfaserkabel mit den beiden Control-Centern am Nord- und am Südportal verbunden sind. Das gelte auch für die Brandorterkennung in den vier Nothaltestellen. Sie erfolge mit drei unterschiedlichen Detektionssystemen und steuere bei einer bevorstehenden Evakuierung direkt die Lüftungsklappen an. Eine Besonderheit sei die Installation der Fibrolaser-Branderkennungstechnik. Ergänzt werde Fibrolaser durch Wärmebildkameras und durch Rauchmelder, die ständig Temperatur und Luft auf Rauchpartikel prüften.

Verkehrssicherheit

Nach einer Meldung von GIT-Sicherheit.de vom 25. April haben Sicherheitsexperten bei Kaspersky Lab herausgefunden, dass **Verkehrssensoren zu leicht manipuliert** werden können. Sollten Kriminelle Zugang zur Verkehrsinfrastruktur einer Smart City erlangen, könnten gemäß der Kaspersky-Studie folgende Probleme auftreten: Beeinträchtigung von Daten, die über Straßensensoren erfasst wurden; Modifizieren, Verfälschen oder Löschen kritischer Daten; Zerstörung von teurer Smart-City-Ausrüstung; Sabotage der Arbeit der zuständigen Behörden. Die Experten von Kaspersky Lab würden zum Schutz vor Manipulationen der Straßensensoren empfehlen: die Kennzeichnung der Hersteller von den Geräten zu entfernen, Standardnamen der Geräte abzuändern und die Media-Access-Control (MAC)-Adressen der Hersteller nach Möglichkeit zu verdecken, für die Bluetooth-Verbindung eine zweistufige Authentifizierung zu nutzen und starke Passwörter zu verwenden sowie in Zusammenarbeit mit Sicherheitsexperten die Geräte auf weitere Schwachstellen zu untersuchen.

Verschlüsselung

Dirk Losse, HID Global, plädiert in Ausgabe 2-2016 der Zeitschrift Sicherheitsforum, S. 36, für starke Authentifizierung. Mit herkömmlichen Authentifizierungsverfahren wie der Nutzung statischer Passwörter könne das Risiko für die Sicherheit unternehmenskritischer Systeme und Daten nicht beseitigt werden, denn sie schützten nicht ausreichend vor Keyloggern oder Phishing-Attacken. In Betracht komme aber die Implementierung einer starken **Zwei- oder Mehrfaktor-Authentifizierungslösung**, die auch den mobilen Zugriff auf Netzwerke und Daten unterstütze. Die darüber hinaus notwendige Benutzerfreundlichkeit biete zum Beispiel die Tap-Authentifizierung, das heißt eine Lösungskombination aus Security-Token zur starken Authentifizierung und NFC-fähigen mobilen Geräten. Anwender müssten bei einer solchen Lösung lediglich ihre Smartcard, und zwar dieselbe Karte, die sie auch für das Öffnen von Türen verwenden, an ihr Smartphone oder Tablet halten, um einen direkten, sicheren Zugang zu Unternehmensdaten oder auch Cloud-Applikationen zu erhalten.

Mit **Hintertüren in verschlüsselter Software** beschäftigt sich heise.de am 18. Mai. Die Debatte über Hintertüren in verschlüsselnder Software könne jahrzehntelang negative Folgen haben, auch wenn sich sichere Verschlüsselung letztlich durchsetzen sollte. Das zeigten die sogenannten Crypto Wars, die eigentlich von den Verschlüsselungsverfechtern gewonnen worden seien. Beispielsweise unterstützten auch 2016 noch immer rund ein Drittel aller Server das Protokoll SSLv2. Das sei 1995 mit dem Netscape Navigator eingeführt worden und enthalte die damals staatlich vorgeschriebenen schwachen Kryptoschlüssel.

Videoüberwachung

Sicherheit.info stellt am 24. Mai eine neue Produktserie von Axis Communications vor, eine auf kleine Unternehmen ausgerichtete Lösung zur Videoüberwachung, eine umfangreiche Out-of-the-box-Serie mit einem speziellen Supportkonzept. Das neue Lösungsangebot kombiniere ein umfassendes Produktportfolio – die Companion-Serie – mit einem eigenen Supportkonzept für Errichter und IT-Reseller. Das Herzstück der Serie sei der **Companion-Recorder**, ein Netzwerk-Videorekorder für acht Videokanäle, der mit einem Port-PoE-Switch ausgestattet sei. Die Kameras böten eine große Bandbreite an Funktionen für unterschiedliche Anwendungen, inklusive Videoüberwachung bei Tag und Nacht mit integrierter Infrarotbeleuchtung für Innen- und Außenbereiche.

Sicherheit.info berichtet am 25. Mai über die von Hanwah Techwin Europe vorgestellten Kameras und DVRs der neuen **Serie Wisenet-HD**, die für Endanwender ausgelegt sind, die Full-HD-Aufnahmen erfassen und aufzeichnen möchten, aber nicht auf eine IP-basierte Lösung umsteigen wollen. Unter Einbindung der AHD-Technologie, die HD-Bilder über bereits vorhandene Koaxialverkabelung überträgt, böten die sieben Kamera-Modelle und die drei DVRs der Serie eine kostengünstige Aktualisierungsoption für analoge Altsysteme und neue Installationen. Alle sieben Kameramodelle böten echte Tag/Nacht-Funktionalität mit einem integrierten Infrarotsperrfilter. Weiterhin seien sie ausgestattet mit dualer Stromversorgung und der neuesten Generation der Rauschunterdrückung. Die drei DVRs könnten gleichzeitig über alle Kanäle in Echtzeit aufzeichnen und mehrere Videos über das Netzwerk und an mobile Geräte simultan übertragen.

Zufahrtskontrolle

Mit den **Herausforderungen des Lieferverkehrs und Besuchermanagements** im Firmengelände befasst sich die Ausgabe 5-2016 der Zeitschrift GIT Sicherheit, S. 28–30. Logistische Prozesse müssten minutiös aufeinander abgestimmt, Just-in-Time-Geschäfte durchgeführt und Lieferungen aus der ganzen Welt angenommen und eingelagert werden. Da brauche es intelligente Systeme und sinnvolle Schnittstellen, um Abläufe zu automatisieren, zu beschleunigen und abzusichern. Der Beitrag behandelt vor allem die Voranmeldung, die Pflicht zur Sicherheitsunterweisung von Besuchern, die automatische Kennzeichenerkennung, die automatische Schrankensteuerung, das Pager-System und die Einbeziehung der Lkw-Waage. Grundlegend für ein effizientes System sei die Abdeckung des gesamten Prozesses des Lkw-Managements – von der Voranmeldung über die Anmeldung an der Pforte bis hin zur Ausfahrt. Moderne Systeme verwalteten mehrere Standorte mit mehreren Einfahrten und deckten unterschiedliche Besuchsarten ab.

Zutrittskontrolle

Dipl.-Ing. Werner Störmer, Fachautor, behandelt in der Ausgabe 5-2016 der Zeitschrift GIT, S. 48–50, die Bedeutung der Zugangskontrolle (Einleitung der Nutzung eines IT-Systems oder Kommunikationssystems) und der Zutrittskontrolle für die Unternehmenssicherheit. Er geht dabei auch auf spezifische softwaretechnische Lösungen ein: auf Zutrittswiederhol-Kontrolle, auf Offenzeit-Überwachung und Mehrpersonen-Anwesenheitskontrolle. Höchste Sicherheit bei optimalem Bedienungskomfort bekomme man derzeit mit der **Handvenenerkennung**, die zudem eine hohe Akzeptanz genieße. Das Muster und die Position der Venen blieben zeitlebens unverändert – auch bei Wärme oder Kälte – und seien bei jedem Menschen unterschiedlich. Die Falschakzeptanzrate des Sensors liege bei 0,00008 Prozent. Bis heute sei es noch niemandem gelungen, die Handvenenerkennung zu hacken oder anderweitig so zu manipulieren, dass eine fremde Identität angenommen werden konnte. Die Konvergenz von physischer Zutrittssteuerung mit der Zugangskontrolle zum Rechner sei ein weiterer Schritt für ein umfassendes Sicherheitskonzept.

Im Interview nimmt Dr. Jörg Wissdorf, Interflex, in der Ausgabe 5-2016 der Zeitschrift GIT Sicherheit, S. 52–54, Stellung zu **flexiblen und sicheren Zeiterfassungs- und Zutrittslösungen**. Grundsätzlich müsse der administrative Aufwand gering sein, im Hintergrund laufen und möglichst mobil bearbeitbar sein. Apps seien hier das bevorzugte Mittel. Die Infrastruktur für die im Hintergrund laufenden Programme stecken zunehmend in der Cloud. Entscheidend sei zudem die richtige

Kombination von Zutritt und Zeiterfassung. Komplex werde das System durch das, was im Hintergrund bereit stehe: Regelungen des jeweiligen Arbeitsvertrages, Überstunden, Minusstunden, Urlaub usw. Wichtige Anwendungsfälle gebe es auch für Banken: Hier müssten Mitarbeiter-Skills gemanagt werden – etwa die von Analysten.

GIT Sicherheit stellt in der Ausgabe 5-2016, S. 56/57, die Ausrüstung des „Tower 185" in Frankfurt am Main mit der elektronischen **Schließlösung Smart Air** von Assa Abloy vor. Sie sei ein besonders flexibles und kosteneffizientes Zutrittskontrollsystem, das mit der RFID-Chipkartentechnik Mifare ausgestattet ist und problemlos in vorhandene Systeme integriert werden könne. Es ermögliche eine schnelle Bearbeitung der Zutrittsrechte über die Zugangskarten. Der Vorteil des Update-on-Card-Systems liege darin, dass der Schließplan auf den jeweiligen Benutzerkarten gespeichert werde und Änderungen nicht an der Tür programmiert werden müssten. Neue Türen, zusätzliche Nutzer, veränderte Zugangsberechtigungen und Zeitpläne könnten über die Software jederzeit auf den Karten angelegt, überschrieben oder aktualisiert werden.

Impressum

Focus on Security enthält Informationen zum Unternehmensschutz und wird monatlich herausgegeben. Der Focus on Security erscheint per elektronischem Newsletter, der an 1.800 Abonnenten verteilt wird.

Hinweis der Redaktion:
Sämtliche Personenbezeichnungen im Plural gelten auch ohne ausdrückliche Nennung gleichermaßen für männliche und weibliche Personen.

Herausgeber:
Manfred Buhl, Vorsitzender der Geschäftsführung, Düsseldorf

Verantwortlicher Redakteur:
Bernd Weiler, Leiter Kommunikation und Marketing

Beratender Redakteur:
Reinhard Rupprecht, Bonn

focus.securitas.de

Kontakt
Securitas Holding GmbH
Redaktion Focus on Security
Potsdamer Str. 88
D-10785 Berlin

Sitz: Düsseldorf, Amtsgericht Düsseldorf HRB 33348
Geschäftsführer: Manfred Buhl (Vors.), Jens Müller, Gabriele Biesing
Vorsitzender des Aufsichtsrates: Dr. Carl A. Schade

E-Mail: info@securitas.de