Blackout, Cybercrime, Spionage

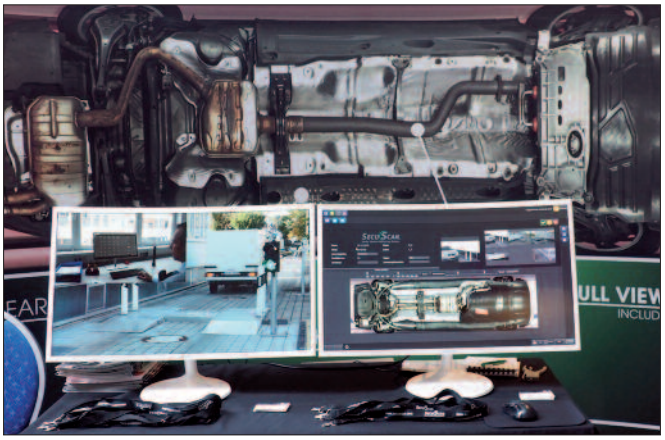
Unter dem Motto „Sicherheit auf dem richtigen Weg – Mensch-Organisation-Technik“ fand am 14. und 15. Mai 2019 in Potsdam der Jubiläumskongress 25 Jahre Verband für Sicherheitstechnik (VfS) statt.

Vor den rund 400 Teilnehmern, die sich zum Jubiläumskongress des „Verbands für Sicherheitstechnik e.V.“ *(VfS; www.vfs-hh.de)* im Kongresshotel Potsdam am Templiner See eingefunden hatten, gab Wilfried Joswig, einer der beiden Geschäftsführer, einen Überblick über die Historie des Vereins. Dieser hatte sich ab 1994 mit sicherheitstechnischen Problemen in Bereichen befasst, die einem erhöhten Bedarf an Sicherheit genügen mussten, wie etwa Justizvollzugsanstalten. Mit der dabei entwickelten Expertise wurden nach und nach weitere Bereiche wie öffentliche Einrichtungen, Logistikunternehmen, Banken, Einkaufszentren, Krankenhäuser, Flughäfen, erschlossen.

In Fachtagungen, wie auch dem jährlich abgehaltenen VfS-Kongress, werden Erfahrungen ausgetauscht und technische Lösungen für Probleme vorgestellt. Vom Verein herausgegebene Handbücher betreffen Videotechnik, Perimeterschutz, Gefahrenmanagementsysteme und elektroakustische Alarmierungseinrichtungen.

Etwa 50 Unternehmen der Sicherheitsbranche waren während des Kongresses mit Ausstellungsständen vertreten. An den beiden Veranstaltungstagen wurden in drei Panels parallel zueinander insgesamt 30 Vorträge abgehalten. Neben jenen, über die nachstehend berichtet wird, auch über Sicherheitsforschung, Terrorismus und Strafvollzug.

Blackout. Der Minister des Innern und für Kommunales des Landes Brandenburg, Karl-Heinz Schröter, bezog sich in seiner Eröffnungsansprache darauf, dass etwa drei Monate zuvor, am 19. und 20. Februar 2019, in Berlin/Köpenick von einer Minute auf die andere etwa 30.000 Haushalte und rund 2.000 Betriebe über 30 Stunden lang von einem Stromausfall betroffen waren. Der Stromausfall wurde hervorgerufen durch Bauarbeiten an einer Brücke, bei denen durch eine Horizontalbohrung eine wichtige Stromleitung sowie die etwa einen Meter entfernt auf gleichem Niveau verlegte Ersatzleitung zerstört worden waren.



Fahrzeugunterboden-Kontrollsystem: Erkennt etwaige Fremdkörper oder Schwachstellen auf der Fahrzeugunterseite.

Vorsorge. Kommunikation und ein Zusammenspiel aller Akteure sei im Krisenfall entscheidend. Der Digitalfunk müsse auch bei Stromausfall funktionieren. Die in Betracht kommenden Funkmasten wurden mit Netzersatzanlagen auf der Basis von Brennstoffzellen versehen, wodurch sie auch im Fall eines Blackouts weiter betrieben werden könnten. Wichtig sei auch die Treibstoffversorgung. Zumindest jene Unternehmen, die für die Daseinsvorsorge wichtig sind, müssten entsprechende Vorkehrungen treffen. Zudem müsse im Radius von 30 km zumindest eine Tankstelle mit Notstromaggregaten Treibstoff auch dann liefern können, wenn das Stromnetz ausfällt.

Mehr Befugnisse. Schröter wies in seinem Referat auch darauf hin, dass im Grenzbereich zu Polen die Schleierfahndung bis zur Staatsgrenze ausgeweitet worden sei, um Kriminalität zu bekämpfen. Beamte dürfen Personen und Fahrzeuge kontrollieren. Die Erweiterung der polizeilichen Befugnisse erfolge in einer Balance zwischen Freiheitsrechten und dem Sicherheitsbedürfnis. Die fortschreitende Digitalisierung erfordere eine Zusammenarbeit mit der Wirtschaft und fließe auch in die kriminalistische Ausbildung der Polizeibeamten ein. Im neuen Masterstudiengang Kriminalistik sei ein Modul Cybercrime vorgesehen.

Cybercrime. Dr. Ole Diehl, zum Zeitpunkt des Referats Vizepräsident des Bundesnachrichtendienstes, wies auf die stetige Zunahme von Cyber-Angriffen hin. Die Angriffsflächen würden durch die stärkere Vernetzung immer größer. Diehl unterschied zwischen nicht staatlichen Angreifern, die etwa aus krimineller Gewinnsucht („Hacking as a service“) oder Geltungsbedürfnis („Skript Kiddies“) handeln; Akteuren im Auftrag eines Staates, hauptsächlich zu Propagandazwecken, und staatlichen Akteuren. Von diesen gehe die größte Gefahr aus. Ihnen stünden große Mittel zur Verfügung; sie könnten auf spezielle Ziele zugeschnittene Software einsetzen. Ziele seien unter anderem politische Einflussnahme, Ausbau der eigenen Machtposition, Mobilisierung der eigenen Wirtschaft.

Künstliche Intelligenz. Als weitere Herausforderung bezeichnete Diehl die künstliche Intelligenz (KI), wobei es nicht nur um selbstfahrende Autos gehe. Noch sei der zivile Sektor Schrittgeber in der Entwicklung dieser Technologie, und nicht das Militär. Die Entwicklung autonomer Waffen könnte die KI zur strategischen Frontlinie der Zukunft machen. Autonom entscheidende Waffensysteme könnten die Hemmschwelle zu ihrem Einsatz absenken. Es sollte zu einem globalen Rahmenvertrag zur Kontrolle dieser Systeme kommen, ähnlich den Rüstungskontrollabkommen.

Spionage. Zwei Drittel der Spionagefälle seien laut Dr. Burkhard Even, Abteilungsleiter Spionageabwehr beim Bundesamt für Verfas-

Fotos: Kurt Hickisch

sungsschutz, auf Innentäter zurückzuführen. Das Verschulden reiche vom Vorsatz bis zur Ahnungslosigkeit. Einfallstore seien menschliche Schwächen wie Neugierde, Gleichgültigkeit oder Verführbarkeit. Über gefakte Profile werde in sozialen Medien von Nachrichtendiensten gezielt Wirtschaftsspionage betrieben, die politische Meinung beeinflusst oder Diffamierungskampagnen betrieben. „Die Wirtschaftsspionage ist von der Wirtschaftssabotage nur einen Mausklick entfernt“, warnte Even. Fake News würden sich viral verbreiten. Die Sicherheitsbehörden müssten sich darauf einstellen.

Investitionen von Ausländern in Wirtschaftsunternehmen seien zwar grundsätzlich wünschenswert, doch habe sich in den letzten Jahren gezeigt, dass sich ausländische Investoren verstärkt

Referenten beim VfS-Kongress in Potsdam: Matthias Hagner, Karl-Heinz Schröter, Sascha Puppel.

in bestimmte Bereiche der Hochtechnologie einkaufen, was einen unerwünschten Abfluss von Know-how nach sich ziehen könnte. Dem müsste durch entsprechende wirtschaftspolitische Maßnahmen begegnet werden. Zudem müssten bei der Entwicklung neuer Technologien Sicherheitsaspekte schon von Anfang an berücksichtigt werden.

Ad-Fraud. „Bei der Werbung im Internet geht es darum, dass sie überhaupt gesehen wird (Viewability); in einem Umfeld erscheint, das der Marke nicht abträglich ist (Brand Safety) und dass letztlich das für die Werbung ausgelegte Geld nicht betrügerisch hinterzogen wird (Ad-Fraud)“ – mit Letzterem machte Friederike Pries, *Integral Ad Science – IAS (www.integralads.com),* auf eine neue Kriminalitätsform im Internet aufmerksam.

In Deutschland werden die Ausgaben für Digital Marketing 2019 etwa 7,7 Milliarden Euro erreichen und bis 2023 auf 10,5 Milliarden Euro steigen. Werbetreibende kaufen Werbung nach bestimmten Kriterien (Zielpublikum) bei Agenturen ein, die ihrerseits Publisher mit der Platzierung der Werbung beauftragen. Abgerechnet wird nach der Anzahl der Aufrufe der Werbung (Impressions), wobei sich der Preis nach der Qualität der aufgerufenen Websites richtet, auf denen die Werbung erscheint. Die Einspeisung auf die Publisher-Sites erfolgt automatisiert; „das Ganze ist ein riesiger vollautomatischer Marktplatz“, wie Pries die Vorgänge umschrieb.

Wo so viel Geld ist, sind auch Betrüger nicht weit. Pries wies darauf hin, dass nach Feststellungen von *IAS* von 100.000 Euro Werbegeld lediglich 50.000 effektiv genützt werden. 10 Prozent gehen durch Ad-Fraud

FOTOS: KURT HICKISCH

verloren, weitere 12 bis 15 Prozent erscheinen als Werbung entweder nicht oder in einem schädlichen Umfeld und 25 Prozent der eingekauften Werbung wird aus eher technischen Gründen nicht gesehen.

Ad-Fraud sei leicht zu machen, äußerst lukrativ und lasse sich nur schwer nachvollziehen. Bei Ad-Fraud wird für Werbung ausgegebenes Geld auf betrügerische Websites umgeleitet. Bei dem von Fries geschilderten „Bot-Ad-Fraud“ schickt der Hacker Bots aus, die in weiterer Folge unbemerkt auf Premium-Seiten surfen, von dort Cookies sammeln und sich dadurch für das Internet attraktiv machen. Danach surfen die Bots auf eine zum Empfang von Werbung (Ads) vom Hacker eingerichtete Site, die dieser hat registrieren lassen. Aufgrund der vielen von den Bots abgelegten Cookies wird die Website des Fraudsters für die Agenturen interessant. Es werden ständig Ads über Netzwerke auf die Betrugsseite geschickt, an die das Werbegeld ausbezahlt wird. Mit verschiedenen Methoden, wie eingehenden Analysen von statischen und dynamischen Features in Browsern und auf Devices oder auch durch Kontakte mit der Hackerszene, spürt das Unternehmen derartige Internetseiten auf.

Werbeumfeld. Es kommt auch auf das Umfeld an, in dem Werbung platziert wird. Neben einem Bericht auf einer News-Seite über einen Flugzeugabsturz wirkt die Anzeige eines Reiseveranstalters deplatziert und entfaltet nicht ihren Werbewert (Brand-Suitability). Werbung für Spielsachen verträgt sich nicht mit solcher für Alkohol. In solchen Fällen blockt das Unternehmen die Anzeige. Die für sie vorgesehene Stelle bleibt leer.

Türkommunikationssystem: Klingel ist mit Smartphone des Bewohners verbunden.

Der Werbetreibende braucht nicht für Werbung zu bezahlen, die für ihn allenfalls sogar abträglich wäre.

Bodycams. „Der Einsatz von Bodycams ist keineswegs mehr auf die Polizei beschränkt“, sagte Dr.-Ing. Matthias Hagner und richtete den Blick auf Bahnpersonal, die Bediensteten von Sicherheitsunternehmen, auf Flughäfen und in Freizeitparks. Wenn die Daten live an eine Zentrale mit Experten gesendet werden, können sie die Feuerwehren beim Identifizieren vorgefundener Chemikalien unterstützen, dem Teledoktor bei der Diagnose helfen oder im Umweltschutz Situationsbilder beim Durchstreifen eines Geländes liefern.

„Bodycams einzuführen ist ein Projekt und nicht bloß die Einführung eines Produkts“, wies Hagner auf die vielfältigen Anforderungen hin. Soll die Cam ein Display haben? Die Polizeien im Norden Deutschlands sind eher dafür, im Süden setzt man auf kleinere Geräte ohne Display. Weiters bedarf es des Einsatzes modernster Kommunikations- und Positionstechnik. Durch Verschlüsselung und Wasserzeichen muss Gerichtsverwertbarkeit sichergestellt sein und datenschutzrechtlich der Konflikt zwischen

Zutrittskontrolle: Torsonde zum Detektieren von Mini-Handys.

den öffentlichen/privaten Sicherheitsinteressen und den Persönlichkeitsrechten der Betroffenen gelöst werden. Da Daueraufnahmen nicht erlaubt sind – ab wann darf Prerecording eingeschaltet werden, um, zum einen, eine deeskalierende Wirkung zu erzielen, zum anderem, um die Zusammenhänge bei sich aufschaukelnden Ereignissen zu erfassen.

Da in Konfliktsituationen möglicherweise auf das Einschalten der Kamera vergessen wird, könnte eine technische Lösung darin bestehen, dass beispielsweise das Ziehen des Schlagstocks die Bildaufnahmen auslöst. Dies wäre etwa über eine Bluetooth-Verbindung realisierbar.

Träger von Bodycams werden lernen, so Hagner, dass Bodycams ihnen das Leben leichter machen. Immerhin können die Aufnahmen auch als Beweismittel für das richtige Verhalten des Trägers der Cam gesehen werden.

Sicherheitstechnik. Mit dem Überwinden von Sicherheitstechnik, im Besonderen von Bewegungsmeldern, beschäftigte sich Sascha Puppel, Sachverständiger für Sicherheitstechnik im Elektrotechnikerhandwerk. Abgesehen von Planungs- und Installationsfehlern, zeige sich, dass die Täter dazulernen. „Die Taktrate zwischen neuen technischen Entwicklungen bis zu deren Überwindung wird immer kürzer“, stellte Puppel fest, wozu auch das Internet beiträgt, über das sich entsprechend Interessierte „schlau machen“ können. Abdecken oder Besprühen von Bewegungsmeldern ist bereits überholt. Der Trend geht dahin, der technischen Eigenart dieser Melder entsprechend, die Körperwärme nach außen nicht in Erscheinung treten zu lassen – was zu auch kuriosen, von Überwachungskameras aufgezeichneten Verhaltensweisen der Täter geführt hat.

Videoüberwachung. Die Regelung der Videoüberwachung wurde von der DSGVO der nationalen Gesetzgebung (in D § 4 BDSG, in Ö §§ 12 und 13 DSG) zur Regelung überlassen, führte Tanja Albert, *Dresdner Institut für Datenschutz; www.dids.de)* aus. Allerdings sind allgemein die Grundsätze der DSGVO als unmittelbar geltendem Recht zu beachten.

Die Videoüberwachung muss (Art. 6 Abs. 1 lit. f DSGVO) erforderlich sein in dem Sinn, dass das festgelegte Ziel nur durch eine Videoüberwachung erreicht werden kann und es kein anderes Mittel gibt, das bei gleicher Wirkung weniger in die Rechte der Betroffenen eingreift, etwa der Einsatz von Sicherheitspersonal; der Wahrung berechtigter Interessen dienen, also zum Schutz vor konkreten Gefahren, nicht jedoch zur abstrakten Gefahrenvorsorge (Abschreckung) und es hat eine Abwägung zwischen den Interessen des Verantwortlichen und denen des Betroffenen zu erfolgen.

Die Frage dabei ist, ob ein objektiver Dritter in der konkreten Situation vernünf-

Fotos: Kurt Hickisch

tigerweise erwarten kann, überwacht zu werden bzw., ob Videoüberwachung im Anlassfall typischerweise akzeptiert oder abgelehnt wird (ErwG 47). Nicht akzeptiert wird Videoüberwachung in Räumen zur Erholung oder zur Freizeitgestaltung, im Umkleidekabinen, Arztpraxen. Besonders schutzwürdig sind Kinder (Schwimmbad). Sollten beispielsweise über eine Gesichtserkennungssoftware biometrische Daten verarbeitet werden, kommt auch Art. 9 DSGVO zum Tragen.

Die Videoüberwachung ist datenschutzfreundlich zu gestalten (zeitliche und räumliche Einschränkung; Art. 25 DSGVO). Die Verarbeitung muss sicher sein (Art. 32). Den umfangreichen Transparenzpflichten (Art. 13 Abs. 1) wird wohl nur so nachgekommen werden können, dass die wichtigsten davon in Form eines Aushangs vor dem überwachten Bereich bekanntgegeben werden und in weiterer Folge auf die entsprechende Internet-Adresse verwiesen wird oder diese durch einen QR-Code aufgerufen werden kann.

Das bloße Piktogramm nach DIN 33450 mit der weißen Kamera auf blauem Grund genügt nicht, zeigte Albert auf. Es sind noch zusätzliche Angaben etwa über den Verantwortlichen, den Zweck der Verarbeitung, deren Rechtsgrundlage, über Speicherdauer und Datenempfänger sowie über die Betroffenenrechte erforderlich.

Weiters ist noch die Pflicht zur unverzüglichen Löschung zu beachten, wenn die Zweckbindung nicht mehr gegeben ist (Art. 17 Abs. 1 lit. a DSGVO). Formell erfordert die Videoüberwachung ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO sowie eine Datenschutz-Folgenabschätzung nach Art. 35, wenn die Videoüberwachung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

Edelstahl-Seilnetz: Eignet sich für die Drohnenabwehr und verhindert das Einbringen etwaiger Tatmittel aus der Luft.

Produkte. Mit dem *Secuscan Fahrzeugunterboden-Kontrollsystem (www.secuscan.com)* kann der Unterboden eines Fahrzeugs optisch auf Fremdkörper (Sprengstoffe, Schmuggelgut) oder auch Sicherheitsmängel (Rost) kontrolliert und videotechnisch erfasst werden, wobei das Fahrzeug mit einer Geschwindigkeit bis zu 40 km/h über den Linienscanner fahren kann. Das System kann fest in die Fahrbahn eingebaut oder mit Auffahrtsrampen auch mobil eingesetzt werden.

Die Videosysteme von *Hikvision (www.hikvision.com/de)* erkennen Kraftfahrzeuge nicht nur anhand des Kennzeichens, sondern auch nach Farbe und Typ. In Parkhäusern ermöglichen sie das Auffinden eines Fahrzeugs an Hand des Kennzeichens. Das Unternehmen stellt auch Ultra-Lowlight-Kameras und Thermokameras her. Vom Unternehmen entwickelte Verfahren zur Gesichtserkennung werden für Casinos oder in Kaufhäusern eingesetzt.

Forteza (www.forteza-eu.de) hat als Neuheit ein mobiles Radarsystem vorgestellt, mit dem ein Gelände rasch abgeschirmt werden kann, etwa für Hubschrauberlandungen, zur VIP-Sicherung oder für Events. Dringt jemand in den abgeschirmten Bereich ein, erfolgt eine akustische Warnmeldung.

Bei entsprechender rechnerischer Einengung der Radarkeule kann auch vor Gebäuden ein schmaler Schutzvorhang ausgebildet werden. Die Reichweite zwischen zwei Geräten beträgt 50 m. Bis zu 20 Bereiche können an die Zentrale angeschlossen werden.

Securiton (www.securiton.de) bietet mit dem *Wingman* ein tragbares Drohnen-Alarmsystem mit einer Detektionsweite bis auf etwa 2 km. Wesentlich größer, aber immer noch mobil einsetzbar ist das System Aartos mit einer Reichweite von 5 bis 7 km. In beiden Fällen handelt es sich um Passivgeräte, die die Steuerungs- und Videosignale eines UAV auffangen. Im Videomanager kann die Flugrichtung der Drohne sichtbar gemacht werden. Für Behörden hat das Unternehmen Jammer im Angebot.

Das *X-Tend Edelstahl-Seilnetz* der Fa. *Carl Stahl Gitter (www.carlstahl-architektur.com),* das horizontal oder vertikal über freie Flächen gespannt wird, stellt, über architektonische Zwecke hinaus, von sich aus eine passive Drohnenabwehr dar und verhindert auch das Einbringen etwaiger Tatmittel aus der Luft.

Die Comlab AG (www.comlab.ch) bietet Jammer an, die beispielsweise in Justizvollzugsanstalten die Kommunikation über Handys stören. Einzelne Handys, etwa die von Vollzugsbeamten, können dabei ausgenommen werden. Ein anderer tragbarer Jammer verhindert durch Überlagerung der in Betracht kommenden Frequenzen, dass über Funksignale IEDs gezündet werden können.

Die *CEIA GmbH (www.ceia.net)* hat als Neuheit eine Torsonde zum Detektieren von Mini-Handys vorgestellt. Zwar könnten auch die bisher üblichen Torsonden derartige Kleinsttelefone (die von den Abmessungen her auf eine Handfläche passen) entdecken, doch müsste die Empfindlichkeit so hoch eingestellt werden, dass Falschalarme häufig würden.

Die *Multicomsystem OHG (www.multicomsystem.de)* bietet einen in Elektrogeräte wie Verteileranlagen, Waschmaschinen, Fernseher eingebauten Brandschutz an, der einen Entstehungsbrand direkt im Gerät selbst bekämpft. Es handelt sich dabei um Thermoampullen, die bei definierter Temperatur ein Löschmittel (Novec) freisetzen. Bei Anschluss an eine Brandmeldeanlage kann optional auch eine Fernauslösung durch ein elektrisches Signal erfolgen.

Die Fa. *Ognios aus Salzburg/Wals (www.ognios.at)* hat ein Türkommunikationssystem entwickelt, bei dem man beim Anklingeln bei der Haus/Wohnungstür mit dem Handy des Wohnungsinhabers verbunden wird, gleichgültig, wo dieser sich befindet. *Kurt Hickisch*

FOTO: KURT HICKISCH