Helmut Reimer

Report

BSI aktualisiert Ausweissimulator PersoSim

Der im Auftrag des BSI entwickelte Ausweissimulator PersoSim steht seit Ende Juni 2020 in der Version 0.15 zum Download bereit. PersoSim ermöglicht die Simulation von Personalausweisen für die Entwicklung und Erprobung von Komponenten und Diensten mit der Online-Ausweisfunktion. Das Programm dient somit als Ergänzung zur Nutzung von Testmusterkarten. Eine missbräuchliche Nutzung von derart simulierten Ausweisen an Wirk-Systemen ist hierbei nicht möglich.

Zusätzlich zu den vorgefertigten Profilen für Personalausweise stehen nun auch Profile für die eID-Karte für EU-BürgerInnen und Angehörige des Europäischen Wirtschaftsraums bereit, sodass Entwickler und Anbieter ihre Systeme vorbereiten können. Die eID-Karte ergänzt ab November 2020 das Portfolio von Personalausweis und elektronischem Aufenthaltstitel und ermöglicht so die direkte Nutzung der Online-Ausweisfunktion auch für EU/EWR-Bürger.

Daneben wurden in PersoSim die vorhandenen Personalausweisprofile aktualisiert und der zugehörige Editor mit neuen Funktionen erweitert. Simulator und Editor laufen nun auch unter Java 11. Zudem skaliert die neue grafische Oberfläche jetzt besser über unterschiedliche Bildschirmauflösungen.

Hier steht der Ausweissimulator zum Download zur Verfügung: *https://persosim.secunet.com/de/downloads/*

17. Deutscher IT-Sicherheitskongress und Feierlichkeiten zum 30-jährigen Bestehen des BSI

Das BSI lädt vom 2. bis 4. Februar 2021 zum 17. Deutschen IT-Sicherheitskongress und den Feierlichkeiten zum 30-jährigen Bestehen des BSI im World Conference Center Bonn ein.

Hier finden Sie in Kürze Informationen zu dem Call for Papers sowie über Neuigkeiten zum Programm und den Inhalten. Sobald wir unser Anmeldeportal freischalten, können Sie sich darüber für die Veranstaltung anmelden.
Anmeldung zur Vorab-Information: *https://www.bsi.bund.de/DE/Service/Aktuell/Veranstaltungen/IT-Sicherheitskongress/IT-Sicherheitskongress_node.html*

EN 303 645 bringt mehr Sicherheit ins Smart Home

Mehr Sicherheit für vernetzte Geräte im Smart Home – dafür liefert der Europäische Standard (EN) 303 645 nun die Grundlage. Als Cyber-Sicherheitsbehörde des Bundes war das Bundesamt für Sicherheit in der Informationstechnik (BSI) maßgeblich an der Entwicklung des am 30. Juni 2020 durch die europäische Normungsorganisation ETSI (European Telecommunications Standards Institute) veröffentlichten Standards beteiligt.

„Immer mehr Menschen in Deutschland nutzen die Möglichkeiten der Digitalisierung und Vernetzung des eigenen Zuhauses. Jedes neue internetfähige Gerät eröffnet aber auch Cyber-Kriminellen neue Angriffsmöglichkeiten. Daher hat das BSI gemeinsam mit Herstellern, Prüfinstituten und internationalen Regierungsorganisationen die Entwicklung des neuen Standards vorangetrieben. Es gilt, vernetze Geräte als Teil des täglich wachsenden Internets der Dinge (IoT) auf eine sichere Basis zu stellen. Mit dem neuen EU-Standard ist dies gelungen, für die Informationssicherheit und Privatsphäre der Verbraucherinnen und Verbraucher in Deutschland und Europa ist dies ein Meilenstein", erklärt BSI-Vizepräsident Gerhard Schabhüser.

Der neue, weltweit anwendbare Mindestsicherheitsstandard EN 303 645 dient als Empfehlung für die sichere Entwicklung (Security by Design) von IoT-Geräten. Er baut auf dem vorherigen Standard TS 103 645 auf und auch der vom BSI mitentwickelte deutsche Sicherheitsstandard DIN SPEC 27072 ist in die Erstellung des neuen europäischen Standards eingeflossen.

Unzureichend geschützte IoT-Geräte sind ein Risiko für die Informationssicherheit und Privatsphäre der Nutzerinnen und Nutzer und daher ein beliebtes Ziel von Cyber-Angreifern. Kompromittierte Geräte können missbraucht werden, um an persönliche Daten der Besitzer zu gelangen oder um großflächige Cyber-Angriffe auf Infrastrukturen Dritter durchzuführen. Um diesen Bedrohungen zu begegnen, beinhaltet der Standard verpflichtend umzusetzende Anforderungen. Hierzu gehören sichere Authentisierungsmechanismen, ein angemessenes Updatemanagement und die Absicherung der Kommunikation.

Auf Basis des neuen Standards erarbeitet das BSI mit weiteren Partnern bei der europäischen Standardisierungsorganisation ETSI derzeit bereits eine Prüfspezifikation zu EN 303 645. Diese definiert, wie die Anforderungen aus dem Sicherheitsstandard strukturiert und umfassend getestet werden können.

Deutsche Unternehmen sind beliebtes Ziel für Phishing-Angriffe

Deutsche Unternehmen sind besonders häufig im Visier krimineller Phishing-Angriffe. Dieses Risiko hat sich in der Corona-Pandemie nochmals verstärkt. Das zeigt der am 07. Juli 2020 veröffentlichte Phishing-Report von Cofense. TÜV SÜD, ein führender neutraler Experte für Cyber-Sicherheit, Risk Awareness und Datenschutz, arbeitet als Partnerunternehmen mit Cofense bei der Phishing-Abwehr zusammen.

Seit Beginn der Corona-Pandemie und der damit verbundenen Zunahme von Fernzugriffen sowie deutlich höherem Online-Datenverkehr, ist besonders die Anzahl der Phishing-Versuche stark gewachsen. Diese Angriffsmethode erfreut sich allgemein großer Beliebtheit unter Hackern, umso mehr, weil das Arbeiten im Ho-

meoffice oft schlechter gegen virtuelle Angriffe abgesichert ist als innerhalb eines Unternehmensnetzwerkes.

Aktuelle Zahlen aus dem Phishing-Report von Cofense für das erste Quartal 2020, zeigen, dass die Command-and-Control-Server krimineller Aktionen mit 4,78 Prozent am zweithäufigsten in Deutschland stehen. „Die tatsächliche Position einer Hacker-Gruppe kann sich zwar durchaus an einem anderen Ort befinden", erklärt Stefan Vollmer, CTO bei TÜV SÜD Sec-IT. „Die hohe Zahl der Command-and-Control-Server lässt jedoch ebenfalls auf ein großes Interesse an deutschen Firmen schließen. Denn: Ein deutscher Server, von dem die Malware-Attacken ausgehen, sitzt in einem vertrauenswürdigen Land, weswegen manche Spam-Regeln möglicherweise nicht greifen und die Postfächer der deutschen Unternehmen es gewohnt sind, von dieser Quelle E-Mails zu erhalten."

Außerdem, so Vollmer weiter, bieten deutsche Unternehmen schon allein deshalb grundsätzlich eine gute Angriffsfläche für Phishing Attacken, weil hierzulande einige Weltmarktführer zu Hause sind und dadurch viel Industrie und Know-how gebündelt vorhanden sind. "Kriminelle und erpresserische Angriffe werden dadurch umso lohnenswerter", erklärt Vollmer. „Außerdem können die Informationen eines kleinen oder mittelständischen und schlechter geschützten Weltmarktführers – sogenannter Hidden Champions – interessanter sein, als die eines gut abgeschirmten Großkonzerns."

TÜV SÜD ist Partner im Cofense® Managed Security Service Provider (MSSP)-Program. Gemeinsam bieten die beiden Unternehmen modernste Anti-Phishing-Services für Organisationen an. Da die meisten Angriffe von Cyberkriminellen mit einem versuchten Phishing-Angriff beginnen, sollten Unternehmen über die richtigen Werkzeuge verfügen, um diese Versuche rechtzeitig zu erkennen.

Der aktuelle Cofense Phishing Report ist hier verfügbar: *https://go.cofense.com/...*

Samsung, BSI, Bundesdruckerei und Telekom Security: Personalausweis auf Smartphone

Gemäß einer Pressemitteilung vom 23. Juli 2020 bringen Samsung Electronics, das Bundesamt für Sicherheit in der Informationstechnik (BSI), die Bundesdruckerei (bdr) sowie die Deutsche Telekom Security GmbH den elektronischen Personalausweis auf ausgewählte Samsung Galaxy Smartphones. Geplant ist dies noch im Laufe des Jahres, sobald die mobile eID-Lösung in Deutschland verfügbar ist. Im Rahmen der langjährigen Zusammenarbeit mit den deutschen Behörden bei der E-Government-Initiative hat Samsung gemeinsam mit den genannten Partnern die technischen Grundlagen für den kommenden Roll-out gelegt und eine hardwarebasierte Sicherheitsarchitektur entwickelt. Sie ermöglicht es den Bürgern, den Personalausweis als eID sicher auf dem eigenen Smartphone zu speichern. Nach der ersten Anmeldung wird der Personalausweis an einen sicheren Ort im Gerät übertragen.

Schützen, was wichtig ist

Die eigene Identität ist das höchste persönliche Gut. Um sicherzustellen, dass sie gut geschützt ist und Informationen der Bürger sicher aufbewahrt sind, muss die mobile eID-Lösung die strengen Sicherheitsanforderungen des BSI erfüllen. Deshalb haben die vier Partner eine ganzheitliche Architektur entwickelt, in deren Mittelpunkt das Fundament der Smartphone-Sicherheit steht – die Hardware. Dank eines sicheren Chips, der direkt in das Smartphone eingebaut ist, können Informationen lokal auf dem Gerät gespeichert werden und die Nutzer über die Verwendung ihrer Daten selbst entscheiden.

Eine offene Sicherheitsplattform

Die mobile eID-Lösung wurde im Rahmen des Förderprojekts OPTIMOS 2.0 entwickelt. Ziel ist es, ein offenes Ökosystem zu schaffen, das die Technologie und Infrastruktur für eine sichere mobile Authentifizierung bereitstellt. Daher war es allen Partnern wichtig, dass die zugrundeliegende Sicherheitsarchitektur verschiedenen Anbietern von Identitätsdiensten offensteht.

„Je mehr wir unsere Lebens- und Arbeitswelt digitalisieren, desto wichtiger ist es, die eigene digitale Identität zu schützen. Folgerichtig entwickelt, fördert und zertifiziert das BSI eID-Lösungen und -Technologien, die dazu beitragen, die digitale Identität der Menschen zu schützen. Im Rahmen von OPTIMOS 2.0 war es unsere Aufgabe, die notwendigen Komponenten, Interfaces und Abläufe zu standardisieren, damit die entwickelte Technologie hohe Sicherheitsstandards erfüllt und für möglichst viele Endnutzer zur Verfügung steht", sagt Arne Schönbohm, Präsident des Bundesamts für Sicherheit in der Informationstechnik.

Um dieses Ziel eines offenen Ökosystems zu erreichen, stellt Samsung das Software Development Kit (SDK) zu seinem eingebetteten Secure Element (eSE) Dritten zur Verfügung.1 Dies ermöglicht Service Providern und Anwendungsentwicklern, Applets für Trusted Service Manager (TSM) zu erstellen, die in die sichere, auf Chipsätzen basierende und für hoheitliche Anwendungen zertifizierte Plattform2 geladen werden können. Als Ergebnis können Anwendungen und Dienste nahtlos mit dem eID-Programm zusammenarbeiten – die Voraussetzung für den Schutz der Informationen.

Samsung Galaxy S20: Das erste Gerät, das die neuen Sicherheitsanforderungen erfüllt

Die Smartphones der Samsung Galaxy S20-Serie, einschließlich das Galaxy S20, Galaxy S20+ und Galaxy S20 Ultra, werden die ersten sein, die sich zum eID Security Framework3 des BSI für hoheitlichen Einsatz konform erklären können. Dank der im Samsung Galaxy S20 eingebetteten Sicherheitsarchitektur bietet die eID Lösung eine Sicherheitsstufe bis zum Niveau "substantial"4 gemäß eIDAS-Verordnung der EU. Diese Verordnung soll sicherstellen, dass EU-Bürger ihre nationalen eIDs grenzüberschreitend verwenden können und Missbrauch oder Änderungen der von den Regierungen ausgestellten Ausweise verhindert werden.

Die Galaxy S20-Serie bietet die höchste verfügbare Verschlüsselungsstufe, wie das kürzlich erhaltene Common Criteria Evaluation Assurance Level (CC EAL) 6+5 zeigt. Sie ist die neueste Serie von Samsung, die durch das branchenführende eSE gesichert wird. Weitere Modelle werden folgen. Das eSE speichert sensible Daten wie Kreditkarteninformationen, Dokumente und Schlüssel sicher auf dem Gerät und isoliert sie für maximalen Schutz. Wie ein Safe bietet ein separater Sicherheitsprozessor eine zusätzliche Sicherheitsebene, die zur Abwehr von Hardware-Angriffen entwickelt wurde. Damit wird der Zugriff auf die auf dem Gerät gespeicherten Informationen und das Kopieren der Daten verhindert.

So kann es mit der mobilen eID weitergehen

Die Online-Ausweisfunktion für den Personalausweis ist erst der Anfang. Mit der Möglichkeit, nicht nur den Ausweis, sondern auch andere wichtige Dokumente wie Führerschein, Krankenversiche-

rungskarte oder sogar die Auto- und Wohnungsschlüssel auf dem Mobiltelefon zu hinterlegen, sind weitreichende Szenarien und Anwendungsfälle denkbar: mit dem Smartphone auf medizinische Unterlagen zugreifen oder ein Bankkonto eröffnen.

G+D Mobile Security: nuSIM-Management-Service für IoT-Lösungen

G+D Mobile Security teilte am 15. Juli 2020 mit, dass das Unternehmen seine langjährige Erfahrung im eSIM-Management nutzt, um den ersten kommerziellen Service für eine sichere Provisionierung von SIM-Daten bereits in der Produktion von IoT-Modul- und Geräteherstellern anzubieten. Diesen Service hat die Deutsche Telekom für die Personalisierung der nuSIM, ihrer integrierten SIM-Lösung für IoT, nun ausgewählt und qualifiziert.

Im IoT-Bereich werden kleine, kostengünstige Geräte mit einem niedrigen Energieverbrauch bevorzugt. Die erforderliche Freigabe des Zugangs zum Mobilfunknetz erfolgt über eine SIM-Karte. Die Art der gewählten SIM-Karte hat dabei einen entscheidenden Einfluss auf die drei genannten Faktoren. Um Kosten zu senken und die Batterielebensdauer zu verlängern, können die Funktionen der SIM-Karte direkt in den Kommunikations-Chip integriert und so das Einlegen einer separaten, physischen SIM-Karte in ein NB (NarrowBand)-IoT- oder LTE-M-Gerät umgangen werden. Die marktführende eSIM-Management-Plattform AirOn von G+D Mobile Security ermöglicht es, die individuellen SIM-Daten während des Modul- oder Geräteherstellungsprozesses in der Fabrik sicher auf den Chip zu laden.

Der AirOn-Service wurde für das sichere Lifecycle-Management von eSIMs entwickelt und zur Unterstützung der DP-Funktion (Data Preparator) für das entstehende nuSIM-Ökosystem erweitert. Das Datenmanagement von G+D Mobile Security garantiert einen hochsicheren End-to-End-Prozess zur Personalisierung der IoT-Geräte in der häufig nicht speziell abgesicherten Produktionslinie des OEM. G+D Mobile Security ist das erste Unternehmen, das von der Deutschen Telekom für den sicheren Personalisierungsservice der nuSIM ausgewählt und qualifiziert wurde.

nuSIM, eine von der Deutschen Telekom gestartete Industrie-Initiative, wurde gezielt für IoT-Geräte entwickelt. Damit diese auch in großen Stückzahlen wirtschaftlich einsetzbar sind, müssen sie unter anderem kostengünstig sein. Dafür wird die Funktionalität der ursprünglich separierten physischen SIM in einen modernen Chip integriert, der im Gerät auch andere Funktionen übernimmt. Dadurch entfallen die Logistik, Lagerhaltung und das Handling separater SIM-Komponenten. Die Kombination von nuSIM und dem AirOn-Service erzielt einen klaren Mehrwert für die Komponenten der Chiphersteller, die somit auf aktuellste Marktanforderungen reagieren können. Modulherstellern ermöglicht das Angebot zudem die Herstellung von kleineren und energieeffizienteren Produkten sowie die direkte Zusammenarbeit mit den Mobilfunkbetreibern, um die nuSIM bereits in der Produktionsphase zu personalisieren.

„Mit der Verfügbarkeit des ersten nuSIM Data Preparator ist der nuSIM-Personalisierungsprozess nun vollständig", sagt Stefan Kaliner, Leiter der UICC-Entwicklung bei der Deutschen Telekom. „Betreiber auf der ganzen Welt können jetzt den AirOn-Service von G+D nutzen, um ihren IoT-Kunden nuSIM-Profile zur Verfügung zu stellen", so Kaliner weiter.

„Die Unterstützung der nuSIM der Deutschen Telekom ist ein weiterer wichtiger Meilenstein im Ausbau unserer marktführenden Position im Bereich eSIM-Management-Plattformen", betont Bernd Müller, Global Vice President, Head of Technology, Solutions & Strategy, Trusted Connected Devices bei G+D Mobile Security. „Für das nuSIM-Ökosystem steht damit unsere Markt-erprobte AirOn-Infrastruktur mit allen notwendigen Services zur Verfügung. Alle bestehenden AirOn-Nutzer können nun ihren SM-DP+-Service durch nuSIM-Unterstützung flexibel erweitern, um dem schnell wachsenden IoT-Markt gerecht zu werden."

Sophos: Cyber-Sicherheitsvorfälle in der Public Cloud weltweit bei fast 75% der Unternehmen

Sophos gab am 09. Juli 2020 weitere Ergebnisse aus seiner weltweiten Umfrage The State of Cloud Security 2020 bekannt. Demnach erlebten fast drei Viertel (70 Prozent) der Unternehmen im letzten Jahr einen Public Cloud-Sicherheitsvorfall – dazu zählten Ransomware und andere Malware (50 Prozent), ungeschützte Daten (29 Prozent), kompromittierte Konten (25 Prozent) und Cryptojacking (17 Prozent). Bei Organisationen mit Multi-Cloud-Umgebungen zeigt sich dabei eine um mehr als 50 Prozent höhere Wahrscheinlichkeit einen Cloud-Sicherheitsvorfall zu erleiden als bei Organisationen, die eine einzelne Cloud betreiben. Deutsche Unternehmen waren zu 61 Prozent von Vorfällen betroffen.

EU-DSGVO zeigt Wirkung

Mit viel Aufwand und unter hoher Kritik eingeführt, scheint die europäische Datenschutzgrundverordnung im weltweiten Vergleich eine positive Wirkung zu zeigen. Unternehmen in Europa hatten laut der Umfrage den niedrigsten Prozentsatz an Sicherheitsvorfällen in der Cloud zu verzeichnen – ein Indikator dafür, dass die Einhaltung der Richtlinien der EU-DSGVO dazu beiträgt, Organisationen vor einer Kompromittierung zu schützen. Am schlimmsten traf es dagegen Indien, wo 93 Prozent der Organisationen im vergangenen Jahr von einem Cyberangriff auf Daten in einer öffentlichen Cloud betroffen waren.

Daten in Public Clouds geraten besonders häufig in Geiselhaft

„Ransomware ist, was nicht überrascht, einer der meist gemeldeten Cybercrime-Vorfälle in der öffentlichen Cloud", sagt Chester Wisniewski, Principal Research Scientist bei Sophos. „Schon unser Report State of Ransomware 2020 hat gezeigt, dass Lösegeld-Angriffe auf Daten in der öffentlichen Cloud zu den erfolgreichsten Attacken zählen." Die Angreifer ändern zudem stetig ihre Methoden, um Cloud-Umgebungen ins Visier zu nehmen, notwendige Infrastrukturen lahm zu legen und den Druck auf Unternehmen zu erhöhen, um Lösegeldzahlungen zu kassieren.

Home-Office als zusätzliche Verlockung für Cloud-Angreifer

„Die jüngste Zunahme von Remote-Arbeitsplätzen stellt eine zusätzliche Motivation dar, Cloud-Infrastrukturen, auf die man sich mehr denn je verlässt, zu attackieren und zu deaktivieren," so Chester Wisniewski weiter. „Es ist vor diesem Hintergrund beunruhigend, dass sich viele Unternehmen ihrer Verantwortung für die Sicherheit von Cloud-Daten und -Workloads noch immer nicht bewusst sind. Cloud-Sicherheit ist eine Aufgabe, die Unternehmen

und Cloud Provider gemeinsam wahrnehmen. Organisationen müssen daher unbedingt ihren Part der Verantwortung übernehmen und ihre Cloud-Umgebungen sorgfältig verwalten und überwachen, um entschlossenen Angreifern immer einen Schritt voraus zu sein."

Die unbeabsichtigt offene Tür: Wie Angreifer einbrechen

Nach wie vor werden Organisationen durch eigene Fehler, quasi aus Versehen, zu Opfern von Daten-Angriffen. Wie im SophosLabs 2020 Threat Report bereits ausführlich beschrieben, sind Fehlkonfigurationen – nicht zuletzt angesichts der Komplexität des Cloud Managements – die Ursache für die Mehrzahl der Vorfälle: 66 Prozent der gemeldeten Angriffe entfallen auf Fehlkonfigurationen. Darüber hinaus geben 33 Prozent der befragten Unternehmen an, dass Cyberkriminelle sich Zugriff auf gestohlene Zugangsdaten von Cloud-Providern verschafft haben. Interessant dabei: Trotz dieser Zahl gibt nur ein Viertel der befragten Organisationen an, dass die Verwaltung des Zugriffs auf Cloud-Konten für sie ein Top-Thema für die IT-Sicherheit ist. Daten von Sophos Cloud Optix (Data from Sophos Cloud Optix), einem Tool zur Verwaltung der Sicherheitslage in der Cloud, zeigen außerdem, dass 91 Prozent der Accounts über privilegierte Identitäts- und Zugriffsverwaltungsfunktionen verfügen, aber 98 Prozent die Multi-Faktor-Authentifizierung in ihren Cloud-Provider-Accounts gar nicht nutzen und deaktiviert haben.

Der Silberstreifen am Datensicherheits-Horizont

Nahezu alle Befragten (96 Prozent) geben zu, dass sie sich Sorgen über ihr derzeitiges Sicherheitsniveau in der Cloud machen, ein ermutigendes Zeichen dafür, dass dies von höchster Bedeutung ist. Dementsprechend stehen „Datenlecks" für fast die Hälfte der Befragten (44 Prozent) ganz oben auf der Liste der Sicherheitsbedenken, an zweiter Stelle steht die Identifizierung und Reaktion auf Sicherheitsvorfälle (41 Prozent). Ungeachtet dieses Silberstreifens ist nur einer von vier Befragten der Ansicht, dass mangelnde Fachkenntnisse des Personals zu den größten Sorgen gehören.

Über die Umfrage

Der Report „State of Cloud Security 2020" wurde von Vanson Bourne im Auftrag von Sophos unter mehr als 3.500 IT-Managern in 26 Ländern in Europa, Nord- und Südamerika, im Asien-Pazifik-Raum, im Nahen Osten und in Afrika durchgeführt, deren Unternehmen Daten und Workloads in der öffentlichen Cloud hosten.

Der vollständige Bericht findet sich zusammen mit einer interaktiven Grafik und einer detaillierten Liste von Empfehlungen zur Sicherheit in der Cloud unter *https://www.sophos.com/en-us/content/state-of-cloud-security.aspx*.

Automobil-Sektor 2019 im Fokus von Hackerattacken

Autonomes Fahren, Elektromobilität, vernetzte Autos und Carsharing – die Automobilindustrie befindet sich im Umbruch. Neue Technologien und digitalisierte Prozesse bringen den Automotive-Unternehmen zahlreiche Vorteile, um zum einen den neuen Kundenanforderungen gerecht zu werden und zum anderen im intensiven Wettbewerb bestehen zu können. Jedoch birgt die fortschreitende Digitalisierung der Branche nicht nur Vorteile, sondern bietet Hackern eine immer größere Angriffsfläche. Und diese versuchen Cyberkriminelle intensiv auszunutzen: Die Security-Analysten des E-Mail Cloud Security Providers Hornetsecurity stellten fest, dass der Automotive-Sektor, nach der Energie- und Logistikbranche, eine der weltweit meist angegriffenen Branchen des vergangenen Jahres war. Das neue Cybersecurity Special „Cyberangriffe auf Automotive-Sektor nehmen Fahrt auf" gibt anhand tiefgehender Analysen und aktueller Vorfälle Einblicke in die Cyber-Bedrohungslage, in der sich Unternehmen der Automobil-Branche derzeit befinden.

E-mail-Kommunikation – Einfallstor für Schadsoftware?

Um in die Systeme von Unternehmen zu gelangen, stellt die E-Mail-Kommunikation das Haupteinfallstor für Cyberangriffe dar. Nach der Analyse der Schad-E-Mails, denen Automobilunternehmen im Jahr 2019 ausgesetzt waren, konnten die Security-Experten diese nach genauen Angriffsarten aufschlüsseln. Dabei beobachtete das Hornetsecurity Security Lab bei Betrieben der Automobilbranche einen hohen Anteil an E-Mail-Angriffen mit schädlichen Anhängen: Unbemerkt werden Spionage-Software, Ransomware oder andere zerstörerische Malware heruntergeladen. Angriffe dieser Art können schwerwiegende Folgen mit sich bringen, wie beispielsweise die Manipulation des Betriebsablaufs, Ausfall der Produktion oder aber Diebstahl von geheimen Informationen der Forschungs- und Entwicklungsabteilung. Bei rund 29% der als schädlich eingestuften E-Mails handelt es sich um Nachrichten mit eingebetteten Links zu infizierten Webseiten.

Die Mobilität der Zukunft ist digital und angreifbar

Dass nicht nur kleinere Zulieferer Opfer von Hackerattacken werden können, beweisen die erst kürzlich durchgeführten Cyberangriffe auf die internationalen Autokonzerne Hyundai und BMW. Die vietnamesische Cyberspionagegruppe „APT32" wird verdächtigt, die Schadsoftware „CobaltStrike" auf den IT-Systemen von BMW installiert zu haben, um damit die Unternehmensnetzwerke auszuspionieren. Es wird vermutet, dass die Hacker auf der Suche nach internen Entwicklungsinformationen waren – genauere Informationen liegen jedoch nicht vor, da das IT-Team des Autobauers die betroffenen Rechner Anfang Dezember 2019 vom Netz nahm, bevor es den Cyberkriminellen gelang, wichtige Daten zu entwenden.

Allgemein sehen sich die Unternehmen immer häufiger professionell entwickelten Cyberattacken durch organisierte Hackergruppen ausgesetzt. Zwar gibt es hin und wieder Einzeltäter, doch die Motive, die sich hinter solchen Angriffen verbergen, deuten auf geplante und strukturierte sowie erfahrene Gruppen hin. Manche dieser cyberkriminellen Banden lassen sich anhand bestimmter Taktiken und ihrer eingesetzten Techniken mittlerweile wiedererkennen, einige haben sich sogar auf bestimmte Branchen oder Märkte als Angriffsziel spezialisiert.

Welche cyberkriminellen Gruppen es auf die Automobilbranche abgesehen haben, was für Ziele die Hacker mit ihren Attacken verfolgen und wie ein Angriff auf ein Automotive-Unternehmen aussieht, beschreibt das Cybersecurity Special „Cyberangriffe auf Automotive-Sektor nehmen Fahrt auf". Der Bericht steht unter *https://www.hornetsecurity.com/de/cybersecurity-special-automobilbranche-im-fokus/* zum kostenlosen Download bereit.

TÜV SÜD Sec-IT bietet neuen Datenschutzservice für KMU

Der Schutz personenbezogener Daten gewinnt im Bewusstsein der Öffentlichkeit zunehmend an Bedeutung. Ein neuer am 15. Juli 2020 veröffentlichter Service von TÜV SÜD Sec-IT soll es besonders kleinen und mittleren Unternehmen (KMU) jetzt noch einfacher machen, beim Thema Datenschutz immer gesetzeskonform zu handeln.

Kunden und Mitarbeiter legen zunehmend Wert auf Datenschutz. Gleichzeitig steigen die Anforderungen an Unternehmen durch gesetzliche Vorgaben wie die EU-DSGVO. „Mit unserem neu gestalteten Datenschutzservice wollen wir vor allem kleine und mittlere Unternehmen bei der gesetzeskonformen Umsetzung noch besser unterstützen", erklärt Tobias Tissberger, Geschäftsführer TÜV SÜD Sec-IT. Die neuen Servicepakete bieten eine bessere Kostentransparenz und Planbarkeit, gleichzeitig profitieren Unternehmen wie bisher von der umfassenden, überregionalen und langjährigen Expertise der TÜV SÜD-Datenschutzexperten.

Datenschutz für KMU: Für jeden Bedarf die passende Lösung

Der neue Datenschutzservice für KMU besteht aus individuell buchbaren Bausteinen. Alle umfassen eine Datenschutz-Management-Software, eine bestimmte Anzahl Beraterstunden, umfangreiche Vorlagen, Leitlinien und Konzepte:

Basis: Vor allem für Handwerksbetriebe, Sportvereine und den Einzelhandel geeignet sowie für alle kleinen Unternehmen, die keinen Datenschutzbeauftragten stellen müssen (unter 20 Mitarbeitern). Sechs Beraterstunden im Jahr sowie ein digitales Audit mit Berichtslegung sind enthalten.

Medium: Richtet sich an etwas größere Firmen, die ebenfalls keinen Datenschutzbeauftragten benötigen, jedoch mehr Aufwand betreiben müssen. Darunter fallen Tourismus, Gastronomie und die Immobilienbranche. Inklusive sind zwölf Beraterstunden jährlich sowie ein digitales Audit mit Berichtslegung.

Premium: Sobald ein Unternehmen einen Datenschutzbeauftragen stellen muss (über 20 Mitarbeiter), eignet sich das Premium-Paket. Es richtet sich daher vor allem an Ärzte, Kanzleien und Online-Shops. 36 Beraterstunden gehören dazu. TÜV SÜD Sec-IT stellt den Datenschutzbeauftragten und führt ein Audit durch – wahlweise am Standort oder digital mit Berichtslegung

Excellence: Das Paket hat die großen unter den mittelständischen Unternehmen und Einrichtungen im Blick, darunter auch Krankenhäuser und Pflegeeinrichtungen. 60 Beraterstunden jährlich sind enthalten. TÜV SÜD Sec-IT stellt den Datenschutzbeauftragten und führt ein Audit durch – wahlweise am Standort oder digital inklusive Berichtslegung.

Besondere Bedürfnisse von KMU

Nicht jedes Unternehmen muss einen Datenschutzbeauftragten (DSB) benennen. Seit Ende 2019 ist dies erst ab 20 Beschäftigten vorgeschrieben. Dennoch sind alle Organisationen, egal welcher Größe, dazu verpflichtet, die Vorgaben der Europäischen Datenschutzgrundverordnung (EU-DSGVO), einzuhalten. Verstöße zerstören nicht nur das Vertrauen von Geschäftspartnern und Belegschaft, hinzu können empfindliche Bußgelder der Behörden kommen, die zudem am Image kratzen.

Durch die neu zugeschnittenen Servicepakete sind die Datenschutzleistungen von TÜV SÜD Sec-IT noch transparenter und besser auf die Kundenbedürfnisse anpassbar. KMU profitieren dabei von der jahrelangen Erfahrung des interdisziplinären TÜV SÜD-Datenschutz-Teams mit Psychologen, Informatikern, Rechts- und Wirtschaftswissenschaftlern, das überregional in ganz Deutschland verfügbar ist. Um Kunden optimal begleiten zu können, erhält jeder Kunde einen verantwortlichen Ansprechpartner – durch das Team wird aber sichergestellt, dass auch im Datenschutznotfall Kunden schnell unterstützt werden können. Für Unternehmen bedeutet dies: effiziente, schnelle Umsetzungsunterstützung durch ein kompetentes Team bei kompletter Kostentransparenz.

Bundesverbandes IT-Sicherheit e.V. (TeleTrusT) zum Privacy-Shield-Urteil des EuGH

Zum Urteil des Europäischen Gerichtshofes betreffend die Unwirksamkeit des „Privacy Shield"-Abkommens zwischen der EU und den USA nimmt der Bundesverband IT-Sicherheit e.V. (TeleTrusT) am 20. Juli 2020 Stellung und gibt zugleich Handlungsempfehlungen für Unternehmen, wie jetzt verfahren werden sollte.

Mit seinem Urteil vom 16.07.2020 hat der EuGH das Privacy-Shield-Abkommen zwischen der EU und den USA für Datenübermittlungen in die USA für unwirksam erklärt, da es kein Schutzniveau auf dem Level der DSGVO sicherstellt. Insbesondere stehe Betroffenen in den USA kein Rechtsweg zur Durchsetzung der im Unionsrecht verankerten Rechtsgarantien offen. Die Standardvertragsklauseln (SCC) für die Übermittlung an Auftragsverarbeiter hat der EuGH dagegen nicht als unwirksam angesehen. Einem Transfer von Daten in Nicht-DSGVO-Staaten kann die Entscheidung dennoch entgegenstehen. Datentransfers in die USA sind ab sofort datenschutzwidrig, wenn sie (ausschließlich) auf Grundlage einer Privacy-Shield-Zertifizierung erfolgen. Erfasst sind nicht nur Übermittlungen an Auftragsverarbeiter, sondern auch solche innerhalb eines Konzerns oder an Geschäftspartner.

Sowohl der Einsatz von Software-Tools, bei denen zumindest ein Teil der Datenverarbeitung in den USA erbracht wird, als auch die konzerninternen Datenflüsse an US-Konzernunternehmen müssen überprüft werden. Auf den Sitz der beteiligten Unternehmen kommt es nicht an. Entscheidend ist allein, ob die Daten in die USA verbracht werden sollen. Auf Basis des Privacy Shields ist das nicht mehr zulässig.

Ob Transfers in die USA oder andere Rechtsordnungen unter den SCC zulässig sind, dürfte davon abhängen, ob dem Betroffenen auch tatsächliche wirksame Mittel der Ausübung zentraler Rechte nach der DSGVO im Zielland bereitstehen.

Umgekehrt ist nicht jede Datenübermittlung in die USA von dem EuGH-Urteil betroffen. Zulässig bleibt eine Übermittlung, die zur Erfüllung eines Vertrages (oder Durchführung vorvertraglicher Maßnahmen) mit dem Betroffenen erforderlich ist. Ebenso nicht unmittelbar betroffen ist die Nutzung von US-Dienstleister, wenn die Leistungserbringung vollständig in europäischen Rechenzentren erfolgt.

Handlungsempfehlungen:

1. Identifizieren der betroffenen Datenflüsse
2. Umstellen auf alternative Garantien

Standardvertragsklauseln (SCC)

Die Übermittlung der personenbezogenen Daten kann nach wie vor auf die sog. Standardvertragsklauseln der EU-Kommission gestützt werden. Diese stellen grundsätzlich ein angemessenes

Datenschutzniveau beim Empfänger her, sofern sie unverändert vereinbart werden. Der EuGH hat die SCC in seinem Urteil ausdrücklich als solche nicht beanstandet. Allerdings hat er zugleich auch darauf hingewiesen, dass der Verantwortliche auch bei Verwendung der SCC prüfen muss, ob das Recht des Ziellandes einen angemessenen Schutz personenbezogener Daten bietet.

Ausdrückliche Einwilligung des Betroffenen

Besteht keine Garantie für ein angemessenes Datenschutzniveau kann die Übermittlung ins Drittland auch auf eine Einwilligung des Betroffenen gestützt werden. Die Einwilligung muss aber ausdrücklich erfolgen und erfordert, dass der Betroffene auf die Risiken eines fehlenden Angemessenheitsbeschlusses oder der Garantie eines Datenschutzniveaus hingewiesen wurde.

3. Hinweise der Aufsichtsbehörden beachten

Das Urteil schafft für die betroffenen Unternehmen große Rechtsunsicherheit: Eine langfristige und verlässliche Absicherung des Datentransfers in die USA fehlt. In dieser Lage ist zu erwarten, dass sich die Aufsichtsbehörden auf nationaler und europäischer Ebene zeitnah äußern und eigenen Hinweisen und Handlungsempfehlungen veröffentlichen werden. Die Berliner Behörde ist bereits vorgeprescht, obwohl hier eine Abstimmung der Datenschutzbehörden aller EU-Länder angezeigt wäre.

Das Urteil des EuGH entfaltet unmittelbar Gültigkeit. Damit sind die betroffenen Datenübermittlungen ab sofort rechtswirig. Entsprechend sollten die Maßnahmen unverzüglich ergriffen werden. Gleichzeitig ist nicht zu erwarten, dass Aufsichtsbehörden unmittelbar Bußgelder verhängen werden.

RA Karsten U. Bartels LL.M., Stellvertretender TeleTrusT-Vorsitzender und Leiter der TeleTrusT-AG „Recht" fasst zusammen: „Das Urteil betrifft in erster Linie den Datentransfer in die USA. Bereits hier sind die Auswirkungen für Unternehmen gravierend, da derzeit keine langfristige Möglichkeit der Übermittlung von Daten in die USA ersichtlich ist. Die Auswirkungen sind aber noch weitreichender. Für viele typische Verarbeitungsländer bestehen die gleichen erheblichen Zweifel an entsprechendem Rechtsschutz, insbesondere nachdem der EuGH diesen ausdrücklich auch für den Arbeitsbereich der Sicherheitsbehörden fordert. Wer alle Risiken vermeiden möchte, wird daher auf einer Verarbeitung in Europa unter ausschließlicher Kontrolle europäischer Unternehmen bestehen müssen. Nachdem das häufig technisch oder wirtschaftlich nicht als Option erscheint, kann auch abgewartet werden, wie die Aufsichtsbehörden die Risiken einschätzen werden."

https://www.teletrust.de/publikationen/stellungnahmen/

McAfee COVID-19 Threat Report: So veränderte die Pandemie die Cyber-Kriminalität

PresseBox) (München, 22.07.20) McAfee hat am 22. Juli 2020 seinen neuen COVID-19 Threat Report veröffentlicht, in dem die Entwicklung von Cyber-Kriminalität während der Pandemie untersucht wurde. Die Forscher von McAfee konzentrierten sich dabei auf die Veränderungen während des ersten Quartals 2020. Dabei wurden unter anderem im Durchschnitt 375 neue Bedrohungen pro Minute identifiziert. Zudem nutzten viele Cyber-Kriminelle die Pandemie aus, indem sie verstärkt auf Phishing-Kampagnen und Malware setzten, die thematisch auf COVID-19 abzielten. Die Anzahl der neuen PowerShell-Malware stieg im Laufe des Quartals um 689 Prozent, während die Gesamtverbreitung der Malware in den letzten vier Quartalen um 1.902 Prozent zunahm.

„Die Bedrohungslandschaft des Jahres 2020 wurde bisher davon geprägt, wie schnell sich die Cyber-Kriminellen die Pandemie zu Nutze gemacht haben sowie den erheblichen Auswirkungen der damit einhergegangenen Cyber-Angriffen", sagte Raj Samani, Chief Scientist bei McAfee. „Was als ein Rinnsal von Phishing-Kampagnen und gelegentlichen bösartigen Apps begann, verwandelte sich schnell in eine Flut von schädlichen URLs und geschickten Cyber-Kriminellen, die den weltweiten Durst nach mehr Informationen über COVID-19 als Einfallstor in Systeme auf der ganzen Welt ausnutzen."

Gezielte Ausnutzung der Pandemie

Die Forscher von McAfee konnten herausfinden, dass cyber-kriminelle Kampagnen während der COVID-19 Pandemie typischerweise auf Themen zurückgreifen, die mit der Pandemie zusammenhängen, wie beispielsweise COVID-19-Tests, medizinische Behandlung oder sogar potentielle Heilmittel. Um an entsprechende Informationen zu kommen, besteht bei vielen Menschen in dieser besonderen Situation eine erhöhte Bereitschaft vielversprechende Links anzuklicken, bestimmte Dateien herunterzuladen oder auf PDFs zuzugreifen, die vermeintlich neue Informationen zur Pandemie enthalten. Vor diesem Hintergrund hat McAfee das COVID-19 Threat Dashboard veröffentlicht, das täglich aktualisiert wird und die aktuell größten Bedrohungen, die mit der Pandemie in Zusammenhang stehen, sammelt und aufzeigt.

Datendiebstahl: Der neue Ransomware-Angriff

Im ersten Quartal von 2020 konnten die Forscher von McAfee außerdem feststellen, dass Cyber-Kriminelle insbesondere Sektoren anvisierten, die stark von Datenintegrität abhängig sind, wie beispielsweise die verarbeitende Industrie, aber auch Rechts- und Bauunternehmen.

„Bei diesen Angriffen handelt es sich um mehr als nur Ransomware. Wenn sich Cyber-Kriminelle Zugang in das Netzwerk verschaffen, dort sensible Daten abgreifen und anschließend drohen, diese zu veröffentlichen falls nicht gezahlt wird, dann handelt es sich um Datendiebstahl", so Christiaan Beek, Senior Principal Engineer und Lead Scientist bei McAfee. „Wir konnten beobachten wie Cyber-Kriminelle mithilfe von ungeschützten Remote Desktop Protocols (RDP) oder gestohlenen Zugangsdaten in kürzester Zeit sensible Daten aus Netzwerken abgreifen und verschlüsseln konnten".

In den vergangenen vier Quartalen stiegen Ransomware-Angriffe um 32 Prozent an.

Cyber-kriminelle Aktivitäten in Q1 2020

- **Fileless Malware:** Die neue PowerShell-Malware wuchs um 689 Prozent, während die Gesamtzahl in den letzten vier Quartalen um 1.902 Prozent zunahm. Neue JavaScript-Malware ging zwar um fast 38 Prozent zurück, wohingegen die gesamte Malware in den letzten vier Quartalen um fast 24 Prozent anstieg.
- **Malware insgesamt:** Neue Malware-Samples verlangsamten sich um 35 Prozent. Die Gesamtzahl der Malware stieg in den letzten vier Quartalen um 27 Prozent. Neue Mac OS-Malware-Samples nahmen um 51 Prozent zu.
- **Mobile Malware:** Neue Malware für mobile Geräte stieg im ersten Quartal 2020 um 71 Prozent, wobei mobile Malware insgesamt in den letzten vier Quartalen um fast 12 Prozent zunahm.

- **Sicherheitsvorfälle:** In Q1 wurden 458 Sicherheitsvorfälle öffentlich gemeldet, was einem Anstieg von 41 Prozent gegenüber dem vierten Quartal 2019 entspricht. 9 Prozent der gemeldeten Fälle fanden in Europa statt.
- **Branchenspezifische Aktivitäten:** Angriffe auf den öffentlichen Sektor stiegen mit 73 Prozent am meisten. Die Vorfälle in der verarbeitenden Industrie stiegen um 44 Prozent, die im Bildungssektor um 33 Prozent.
- **IoT-Geräte:** Neue Malware-Samples nahmen um fast 58 Prozent zu. Die Gesamtzahl der IoT-Malware stieg in den letzten vier Quartalen um 82 Prozent.
- **Cryptomining:** Neue Coinmining-Malware stieg im ersten Quartal 2020 um 26 Prozent. Insgesamt stieg die Anzahl von Coinmining-Malware in den letzten vier Quartalen um fast 97 Prozent.

Weiterführender Link: https://www.mcafee.com/enterprise/de-de/threat-center/mcafee-labs/reports.html

Rezensionen

Veranstaltungen

Ebru Öztürk, datenschutz nord GmbH, Justiziarin und Rechtsanwältin (LL.M.Eur.)
Stefan R. Seiter, datenschutz nord GmbH, Justiziar und Rechtsanwalt

DuD 2020, Datenschutzkongress DSGVO, 15. und 16. Juni 2020 in Berlin

Zu besten sommerlichen Bedingungen startete am 15. Juni die auf „lediglich" zwei Tage verkürzte DuD-Jahreskonferenz. Von aufsichtsbehördlicher Seite waren dabei die Länder Baden-Württemberg, Niedersachsen, Schleswig-Holstein sowie der Bundesbeauftragte vertreten, teilweise auch über Videokonferenz. Höchst aktuelles Thema war selbstverständlich auch die kürzlich veröffentlichte Corona-Warn-App, von deren Konzept sich Ulrich Kelber (BfDI) überzeugt sah. Sowohl mit Blick auf die vorherrschende Pandemie als auch auf den gesamten bisherigen Zeitraum seit Geltung der DS-GVO stellte er die Wichtigkeit eines funktionierenden Datenschutzes heraus. Gleichwohl gebe es weiterhin Nachholbedarf bei der konzeptionellen Umsetzung; als Beispiele führte er die Beschilderung zur Videoüberwachung und die Information beim Profiling an.

In ähnlicher Weise äußerten sich auch Dr. Stefan Brink (LfDI Baden-Württemberg) und Barbara Thiel (LfD Niedersachsen), die beide – wenngleich von unterschiedlichen Ansätzen geprägt – ein Vollzugsdefizit in der Praxis konstatierten. Noch immer seien die mangelnde personelle bzw. finanzielle Ausstattung sowie das Dickicht von verwaltungsrechtlichen Besonderheiten in einigen EU-Ländern die hauptsächlichen Hinderungsgründe für ein besseres Ineinandergreifen der verschiedenen Instanzen.

Insbesondere im Gesundheitsbereich mangele es an hinreichend bestimmten Erlaubnisvorschriften, sodass den Behörden hier oft rechtsstaatlich die Hände gebunden seien. Besonders deutlich sei dies wahrzunehmen u. a. bei Diensten der Telemedizin und der Nutzung von sog. Wearables (z. B. Fitness-Armbändern). Dabei biete gerade die fortschreitende technologische Entwicklung auch große Chancen für eine bessere Versorgung von Patienten. Hierzu ergänzte Marit Hansen (ULD Schleswig-Holstein) in ihrem Vortrag, dass der Trend zur Digitalisierung zweifelsohne durch die Corona-Krise befeuert worden sei. Weitere spannende Entwicklungen, die sich abzeichneten, wie etwa ein elektronischer Immunitätsnachweis oder Datenspende-Apps, bedürften dabei aber stets einer kritischen Würdigung und vor allem akkurater Umsetzung der Informationspflichten.

In den weiteren Fachvorträgen wurden weitere Themen aus Beratersicht erörtert. Die (stellenweise) weitschweifigen Nachfragen aus dem Publikum ließen den Eindruck erwecken, dass auch einige „Evergreens" offenbar noch lange nicht ausdiskutiert sind. So wurden Beispiele zur möglichen Abmahnung von Datenschutzverstößen (Werner Hülsmann, datenschutzwissen.de) ebenso angeregt aufgenommen wie der kurzweilige Blick von Marco di Filippo (whitelisthackers UG) auf die entlarvend effiziente Methodik, die Produktions-IT eines Unternehmens angreifen zu können. In diesem Zusammenhang wiederum ist ein Appell von Isabel Münch (BSI) zu sehen, die – neben dem Skizzieren von Besonderheiten des BSI in der noch relativ jungen Rolle als Aufsichtsbehörde – eindringlich und bildhaft darauf hinwies, dass gerade für die Betreiber von kritischen Infrastrukturen (KRITIS) umfassende Meldepflichten bestehen, die es präzise einzuhalten gelte. Schließlich sei wenig damit geholfen, wenn sie als Bundesbehörde von dem Ausfall eines großflächigen Teils des Mobilfunknetzes über Twitter erfahre statt durch eine vom Betreiber offiziell eingereichte Meldung.

Dass ein solches Verhalten mitunter auch geeignet wäre, die Verhängung einer Geldbuße nach sich zu ziehen, zielte direkt auf den Vortrag von Dr. Jens Eckhardt (Derra, Meyer & Partner Rechtsanwälte PartGmbB). Er setzte sich kritisch mit dem neuen Bußgeldmodell, welches die Aufsichtsbehörden mittlerweile zur Anwendung bringen, auseinander und bot zugleich einen Einblick in strategische wie prozessuale Besonderheiten, die vor allem für die Tätigkeit von erfahrenen Beratern eine absolute Bereicherung darstellten.

Klarheit in eine viel diskutierte Frage brachte auch Ebru Öztürk mit ihrem breitbandigen Überblick zur gemeinsamen Verantwortlichkeit. Mit dem Modell der Arbeitnehmerüberlassung stellte sie in diesem Zusammenhang einen Anwendungsfall zur Diskussion, der rege Anlass zu Nachfragen und engagiertem Austausch bot. Mehrere Ansätze zur rechtskonformen Ausgestaltung des Usertracking im Internet erläuterte Stefan R. Seiter. Anhand der von der Datenschutzkonferenz veröffentlichten Orientierungshilfe Telemedien präsentierte er verschiedene rechtliche Ansichten und bezog dabei neben den jüngsten höchstrichterlichen Entscheidungen auch die Perspektive der Anwender, also der Nutzer ein. Dabei zeigte er Konstellationen auf, in denen das pauschale Erfordernis einer Einwilligung stattdessen auch durch eine Abwägung von gegenseitigen Interessen ersetzt werden könne.

Einen der nicht nur fachlich herausragenden, sondern auch in der Präsentation unterhalterischen Höhepunkte setzte Volker Kozok (Bundesministerium der Verteidigung) mit seinem Vortrag zur gefühlten und tatsächlichen Bedrohungslage. Er gab eindrucksvolle Einblicke in die tiefschürfende Arbeit von speziellen Ermittlungs-