CAk report

Newsletter der Cyber Akademie zur Informationssicherheit

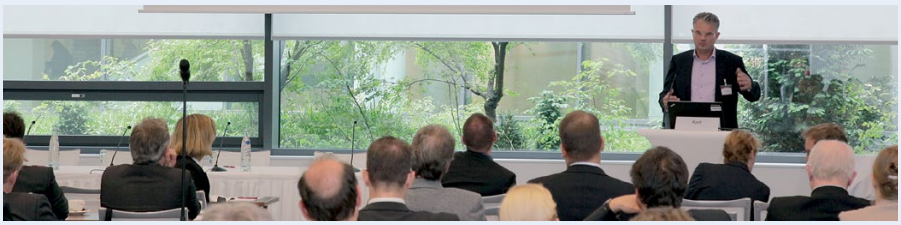
CAk Cyber Akademie

Nr. 49 Oktober 2017

Praxis-Seminar

Belastbare IT-Gutachten erstellen und bewerten

Aufgrund der zunehmenden Relevanz, der IT-Gutachten oder digitalen Beweisen in gerichtlichen Verfahren in nahezu allen Bereichen zukommt, gilt es bspw. für Gutachter oder IT-Forensiker, die rechtlichen und technischen Anforderungen zu kennen und diesen angemessen Rechnung zu tragen. Dabei gilt es insbesondere auch, die jeweiligen essenziellen Anforderungen, etwa in Bezug auf Form und Inhaltspräsentation eines Gutachtens, zu berücksichtigen. Insbesondere bei der IT-Forensik kommt es deshalb darauf an, dass die gesicherten digitalen Beweismittel den Anforderungen der Prozessordnungen genügen. Fehler bei der Beweismittelgewinnung oder Dokumentation können zu nicht unerhebliche Konsequenzen für die Verfahrensbeteiligten, aber auch den Sachverständigen selbst, nach sich ziehen.



IT-Gutachten und Forensik – Theorie trifft Praxis

In diesem Seminar der Cyber Akademie lernen die Teilnehmer sehr praxisorientiert, welche Anforderungen an sie als Gutachter / IT-Sachverständige / IT-Forensiker und diesbezüglich auch an die von ihnen erstellten Gutachten gestellt werden. Eines der Ziele der Schulung ist es deshalb, die Teilnehmenden mit den technischen und rechtlichen Fallstricken vertraut zu machen, die es im Bereich „belastbare IT-Gutachten“ zu beachten gilt. Vor diesem Hintergrund richtet sich das Seminar in erster Linie an IT-Sachverständige (wie bspw. öffentlich bestellte und vereidigte, zertifizierte oder freie Sachverständige), IT-Forensiker, Internal Investigators, Compliance Officers, sowie an alle weiteren Experten, die sich (beruflich) mit IT-Gutachten auseinandersetzen müssen.

Learning by doing – Gutachten erstellen, analysieren, verteidigen

Zu Beginn der Schulung werden die Teilnehmer mit den relevanten, zwingend zu beachtenden theoretischen rechtlichen und technischen Anforderungen und Grundlagen vertraut gemacht. Die sich daran anschließende, mehrstündige Praxiseinheit wird wichtige praktische Aspekte belastbarer IT-Gutachten in der Praxis beleuchten. Dabei werden die Teilnehmer anhand eines Falls aus der Praxis jeweils ein eigenes Gutachten erstellen. Diese Gutachten werden dann in einem Rollenspiel „vor Gericht“ von den Teilnehmenden analysiert. Dem jeweiligen Gutachtenersteller wird dabei auch die Möglichkeit gegeben, sein Gutachten zu verteidigen. Anschließend wird den Teilnehmenden anhand ihrer Gutachten ein etwaiges Optimierungspotenzial aufgezeigt.

Das Cyber Akademie-Seminar "Belastbare IT-Gutachten erstellen und bewerten" findet am 23. November 2017 in Berlin statt. Auf Anfrage führt die Cyber Akademie diese Schulung auch in Ihrer Behörde/ in Ihrem Unternehmen als Inhouse-Schulung durch. ***Weitere Informationen finden Sie hier.***

INHALT

CAk-SEMINARE 2017

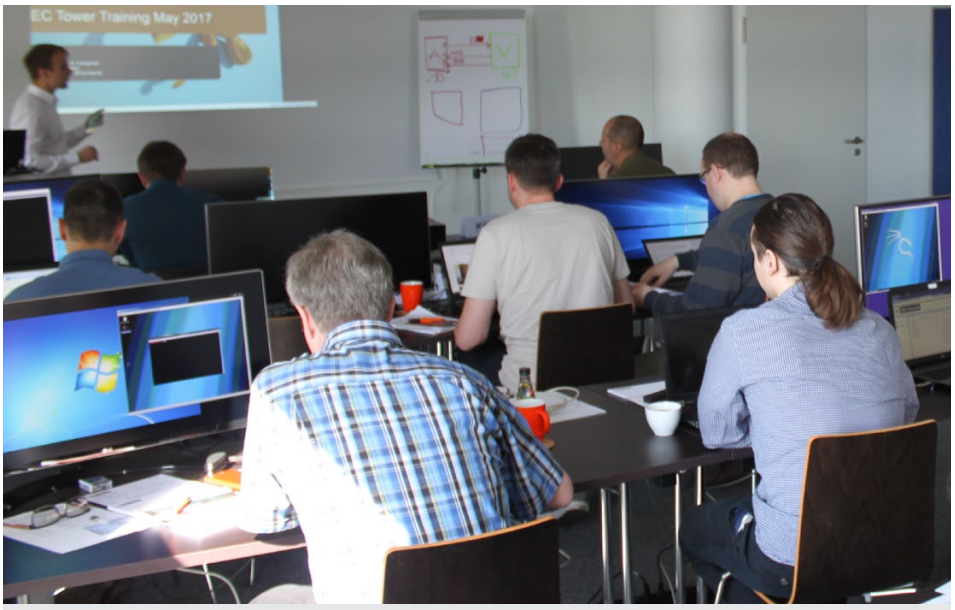
- IT-Grundschutz-Experte (13.11.2017 - 17.11.2017, Berlin)
- Sensibilisierungskampagnen planen und durchführen (14.11.2017 - 15.11.2017, München)
- Webanwendungssicherheit-Workshop (14.11.2017 - 16.11.2017, Hamburg)
- Datenschutzgerechte Datenträgerentsorgung(16.11.2017, Berlin)
- Informationssicherheitsvorfälle und Verhinderung von unerwünschtem Informationsabfluss (21.11.2017 - 22.11.2017, Berlin)

www.cyber-akademie.de

Kenne deinen Feind

Mit Insider-Wissen zu mehr IT-Sicherheit

(CAk/bst) Die Bedrohungslage im Cyber-Raum stellt Administratoren und IT-Sicherheitsverantwortliche in Unternehmen und Behörden vor enorme Herausforderungen. Eine gute Basis für ein solides Sicherheitsmanagement ergibt sich aus einem Verständnis für die Methoden von Angreifern und die Grenzen von Sicherheitsprodukten. Das entsprechende Insider-Wissen vermittelte das Cyber Defence Simulation Training der Cyber Akademie im September.



Beim Cyber Defence Simulation Training stehen praktische Übungen in kleinen Gruppen im Mittelpunkt. Die Teilnehmer lernen das Vorgehen von Angreifern kennen und können aus dieser Erfahrung auf Prioritäten für Sicherheitsmaßnahmen in der eigenen Organisation schließen. Foto: CAk/Feldmann

Konzentriert schauen die acht "Hacker" auf ihre Bildschirme. Gleichzeitig beginnen sie einen Befehl in ihre Kommandozeile zu tippen. "use exploit/windows/smb/ms08_067_netapi" Nach einer kurzen Stille erklingt erneutes Tippen. "show options" Auf acht Bildschirmen erscheint eine Auflistung möglicher Einstellungen. Einer nach dem anderen beginnt wieder zu tippen. "set RHOST 10.0.71.170" Die Nummernfolge unterscheidet sich marginal bei jedem einzelnen. Wieder wird getippt. "exploit" Erneut erscheinen einige Zeilen Text.

"Und jetzt?", fragt einer der Acht "Jetzt habt ihr jeder den Host erfolgreich übernommen", lautet die Antwort. Der Host ist in diesem Fall ein Rechner mit einem stark veralteten Windows-Betriebssystem – ein ideales Ziel für einen Angriff. Gelungen ist dieser unter Verwendung eines sehr populären und leicht zu nutzenden Exploits, d. h. eines Programmcodes, der eine Sicherheitslücke gezielt ausnutzt. Wie der Exploit funktioniert, weiß in diesem Moment noch keiner der "Hacker" so genau. Aber das ist auch nicht nötig. Das Zielsystem ist kompromittiert.

Hacken, um nicht gehackt zu werden

Bei den acht "Hackern" handelt es sich um die Teilnehmer des Cyber Defence Simulation Trainings der Cyber Akademie, darunter Administratoren und Zuständige für die IT-Sicherheit aus verschiedenen Organisationen. Auch Vertreter aus Strafverfolgungsbehörden nehmen teil. Sie alle wollen lernen, wie ein Hacker zu denken und vorzugehen, um besser zu verstehen, wie IT-Systeme vor Angriffen geschützt werden können und wie man Eindringlingen auf die Spur kommen kann. Beibringen kann Ihnen das Seminarleiter Andreas Falkenberg. Der professionelle Ethical Hacker testet seit Jahren Applikationen und Netzwerke nach expliziter Erlaubnis auf Schwachstellen. In zahlreichen praktischen Übungen lässt er die Teilnehmer typische Hacks ausprobieren. Jeder hat einen Arbeitsplatz, von dem aus er Angriffe auf eine eigene virtuelle Trainingsumgebung durchführen kann.

Diese ist einer typischen Netzumgebung in Organisationen nachempfunden: Es gibt Arbeitsplatzrechner mit verschiedenen Windows-Betriebssystemen, einen Administrator-PC und verschiedene Server. Gesichert wird das Netz durch Virenscanner, Firewall, Network- und Agent-based Client-Monitoring sowie eine Lösung für Security Information and Event Management (SIEM). Die Ausführung des Windows-Exploits hat dieses Aufgebot nur begrenzt verhindert.

"Das Problem ist, das solche Sicherheitsprodukte für den jeweiligen konkreten Kontext in der Organisation konfiguriert werden müssen, um wirklich Mehrwert zu liefern", kommentiert Seminarleiter Falkenberg. "In vielen Fällen werden aber die Standardeinstellungen nie wirklich geändert. Hinzu kommt, dass selbst sinnvolle Konfigurationen von Sicherheitsprodukten oft durch simple Tricks umgangen werden können." Dass allerdings ein seit Jahren bekannter und gerne genutzter Exploit nicht unter Standardeinstellungen unterbunden wird, stößt bei Falkenberg auf Unverständnis. Und es kommt noch schlimmer: Hat man erst einmal die Kontrolle über den Zielrechner übernommen, lässt sich der Agent-based Monitor auf dem Windows-Client unbemerkt beenden. "Wir können aber auch mit unserer Malware unbemerkt in den Prozess des lokalen Agent-based Monitor migrieren", schlägt Falkenberg vor. "Das ist eine triviale, aber gut funktionierende Methode, um hier die Grenzen dieses Sicherheitsprodukts aufzuzeigen."

Aller Anfang ist leicht

Trivial ist ein Wort, dass öfter fällt während die Teilnehmer des Trainings klassische Vorgehensweisen von Hackern nachvollziehen. Das Eindringen in IT-Netzwerke ist längst nicht nur erfahrenen und besonders kreativen Köpfen vorbehalten. Im Internet

können leicht verständliche Anleitungen und kostenlose Werkzeuge dafür gefunden werden. So gelingt es auch mit begrenzten Informatikkenntnissen, schlecht gesicherte Systeme zu infiltrieren.

Das lässt sich z. B. durch Ausnutzung von Sicherheitslücken von Web-Applikationen erreichen. Diese Ebene stellt häufig das schwächste Glied in IT-Systemen dar – zumindest in technischer Hinsicht, denn das wohl häufigste Einfallstor für Cyber-Angriffe ist Phishing. Dabei werden betrügerische E-Mails als Köder verwendet, um Schadsoftware in IT-Systemen zu platzieren oder Zugangsdaten zu erlangen. Hat ein professionellerer Angreifer einmal den Fuß in der Tür, sucht er nach Möglichkeiten, sich weiter im Netzwerk auszubreiten, um schließlich zu seinem Ziel zu gelangen, zum Beispiel Zugriff auf bestimmte sensible Daten zu erhalten. Ein Überspringen auf weitere interne Systeme ist über diverse Wege möglich. Mithilfe von Windows-Standardbefehlen können detaillierte Informationen über Nutzerrechte in der Domäne abrgerufen werden. Hacker planen so den schnellsten Weg, um Administratorrechte zu erhalten. “Es gibt auch Tools, die einem diese Rechte-Beziehungen grafisch darstellen”, erklärt Falkenberg. “So erhält man ein besseres Bild über die Domäne, als oftmals selbst der Administrator hat. Und das ohne als Angreifer großen Lärm zu machen.”

Eine weitere Ausbreitung im Netz erfordert in der Regel Nutzerpasswörter. Auch hier helfen wieder beliebte Tools. Mit einem kann ein Angreifer alle auf einem System hinterlegten gehashten Passphrasen einsammeln. Diese kann er dann z. B. automatisiert gegen riesige Listen von typischen Passwörtern abgleichen lassen.

Vom Angriff zur Verteidigung

Konzentriert gehen die acht “Hacker” die nächsten Übungen durch, die Andreas Falkenberg vorbereitet hat, und bekommen dabei ein Gefühl dafür, wo IT-Systeme besonders anfällig sind und welche Möglichkeiten Angreifern offenstehen. Zwischendurch wird immer wieder diskutiert: über den sinnvollen Einsatz von IT-Sicherheitslösungen, über grundlegende Entscheidungen zur Netzwerkarchitektur und organisatorische und personelle Schwierigkeiten bei der Umsetzung von Sicherheitskonzepten. “Was kann man dagegen tun?”, lautet eine häufige Frage, wenn den acht “Hackern” wieder ein Exploit gelungen ist oder sie sich wieder weitreichendere Zugriffsrechte in ihrer Trainingsumgebung verschaffen konnten. Konkrete Maßgaben sind nur mit genauem Blick auf die jeweiligen Bedingungen vor Ort zu formulieren, es bleiben allerdings diverse grundlegende Aussagen hängen. IT-Sicherheitstechnologien sollten gezielt eingesetzt und immer kontextsensitiv angepasst werden. Typische Methoden von Angreifern sollten gezielt in der eigenen Organisation getestet werden.

Eines aber wird allen Teilnehmern des Cyber Defence Simulation Trainings klar. Jedes Netzwerk ist angreifbar und die Erfolgsaussichten von Hackern hängen vor allem davon ab, wie viel Motivation und Zeit sie mitbringen. Mit einem gut durchdachten, mehrstufigen Sicherheitskonzept sollten Angreifern daher so viele Steine wie möglich in den Weg gelegt werden, damit sie an irgendeinem Punkt hängen bleiben, Fehler machen und entdeckt werden können. “Es kann nicht nur darum gehen, die Zugbrücke möglichst hochzuziehen”, betont Falkenberg. “Früher oder später wird immer ein Angreifer die äußere Verteidigungslinie durchbrechen.” Die realistische Grundannahme laute sogar, dass das bereits geschehen ist.

Das nächste Cyber Defence Simulation Training wird vom 6. bis 8. März 2018 in Berlin stattfinden. *Weitere Informationen hier.*

Zentrale Anlaufstelle angekündigt

Cyberwehr für Baden-Württemberg

(CAk/stb) Die Landesregierung-Baden Württemberg baut eine Kontakt- und Beratungsstelle zur Cyber-Sicherheit für kleine und mittlere Unternehmen auf. Die Cyberwehr Baden-Württemberg soll außerdem als landesweite Koordinierungsstelle bei Hackerangriffen fungieren.

"Die Cyberwehr ist die Feuerwehr des 21. Jahrhunderts, erreichbar an sieben Tagen in der Woche, 24 Stunden am Tag. Wir schaffen damit eine Stelle mit einheitlicher Notfallnummer", erklärt der baden-württembergische Minister für Inneres, Digitalisierung und Migration, Thomas Strobl.

Die Cyberwehr soll als ganzheitliche Lösung für Unternehmen etabliert werden und dazu eng mit bestehenden Institutionen im Land zusammenarbeiten – so mit der Zentralen Ansprechstelle Cybercrime (ZAC) beim Landeskriminalamt (LKA), dem Landesamt für Verfassungsschutz, dem CERT BW und dem Forschungszentrum Informatik am Karlsruher Institut für Technologie. "Man möchte hier das gesamte Landes-Know-how aus Behörden, Polizei, Wirtschaft und Forschung bündeln und teilen", sagt Reinhard Tencz, Abteilungsleiter Cybercrime und Digitale Spuren im LKA Baden-Württemberg.

"Natürlich arbeiten wir dabei auch eng mit dem Bundesamt für Sicherheit in der Informationstechnik, dem BSI, zusammen", erklärt Minister Strobl. "Ich habe mich deshalb mit dem BSI-Präsidenten Arne Schönbohm auf einen noch engeren Austausch verständigt und angeregt, eines der geplanten Verbindungsbüros des BSI bei uns in Baden-Württemberg anzusiedeln."

Mit dem Aufbau eines Netzwerks soll direkt begonnen werden – zunächst wird eine 15-monatige Pilotphase eingeleitet. Wie das Innenministerium mitteilt, seien für die Cyberwehr im kommenden Haushalt etwa drei Millionen Euro angemeldet worden. Weitere acht Millionen sind für weitere Maßnahmen im Bereich Cyber-Sicherheit vorgesehen. So sollen gezielt Startups im Bereich IT-Sicherheit gefördert werden, wie Strobl erläutert.

Achter Anwendertag IT-Forensik

Cybercrime stellt Behörden vor Herausforderungen

(CAk/bst) Cybercrime sowie Straftaten mit dem Tatmittel Internet sind längst zu alltäglichen Deliktsformen geworden, mit denen Strafverfolgungsbehörden regelmäßig konfrontiert werden. "Der technische Aufwand für die digitale Forensik wächst ständig. Gleichzeitig steigen Anforderungen an IT-Kenntnisse für die Polizisten." Das sagte Prof. Dr. Roman Povalej von der Polizeiakademie Niedersachsen in seinem Vortrag auf dem 8. Anwendertag IT-Forensik des Fraunhofer-Institut für Sichere Informationstechnologie SIT.

Forderte mehr institutionen- und länderübergreifenden Austausch von Know-how: Reinhard Tencz beim 8. Anwendertag IT-Forensik des Fraunhofer-Institut SIT. Foto: CAk/Stiebel

Povalej plädierte für eine Aufnahme von IT-orientierten Studieninhalten in die Ausbildung aller Polizisten. "Eine klare Trennung von Ermittler und IT-Forensiker ist nicht möglich", betonte er. Zum Beispiel müsse jeder Ersteinschreiter wissen, wie er sich in Bezug auf die Sicherstellung von PCs oder mobilen Endgeräten zu verhalten habe, um eine umfängliche und gerichtsfeste Auswertung von Daten nicht zu erschweren.
Reinhard Tencz vom Landeskriminalamt Baden Württemberg warnte davor, im Zuge der digitalen Revolution im Bereich der Cyber-Kriminalität immer mehr in Rückstand zu geraten, wenn in den Sicherheitsbehörden nicht ein Umdenken in Bezug auf Organisation, Ausstattung sowie Aus- und Weiterbildung erfolge. Insbesondere betonte Tencz die Notwendigkeit von Kooperationen zwischen den Behörden aber auch mit Forschungseinrichtungen und Anbietern von technischen Lösungen aus der freien Wirtschaft. "Die Polizei kann heute nicht mehr alles alleine leisten", resümierte Tencz.

Ermittlungserfolge im Darknet

Eine besondere Herausforderung für die Strafverfolgung ergibt sich aus Technologien, die Kriminellen ein hohes Maß an Anonymität versprechen. Auf Grundlage des TOR-Netzwerkes, das Internetzugriffe mehrfach verschlüsselt umleitet, und der Kryptowährung Bitcoin, mit der Zahlungen an sonst üblichen, streng regulierten Kreditinstituten vorbei getätigt werden können, hat sich im Darknet in wenigen Jahren eine Nische für den Handel mit illegalen Gütern entwickelt.
Dass es sich hier aber nicht um einen rechtsfreien Raum handelt, zeigten Cai Rüffer von der Generalstaatsanwaltschaft Frankfurt am Main und Jürgen Gause vom Bundeskriminalamt (BKA) anhand von Beispielen aus der Ermittlungspraxis. So konnte der Hansa Market – einer größten illegalen Marktplätze im Darknet – vom BKA in Zusammenarbeit mit der niederländischen Polizei übernommen und abgeschaltet werden. Die beiden Administratoren der vor allem für den Drogenhandel genutzten Plattform befinden sich seit Juni 2017 in Untersuchungshaft. "Bislang konnten wir 787 Bitcoins der beiden Plattformbetreiber sicherstellen. Das entspricht rund 2,5 Millionen Euro", erklärte Gause.
Ein weiteres Beispiel für erfolgreiche Ermittlungen erläuterte Staatsanwalt Rüffer. Der Waffenhändler, von dem David S. die Tatwaffe für den Amoklauf in München bezogen hatte, konnte auf Grundlage von bereits zuvor begonnenen Ermittlungen im Darknet verhaftet werden. Mittels übernommener Accounts von Interessenten für Waffenkäufe konnten die Ermittler einen vertrauensvollen Kontakt mit dem Waffenhändler aufnehmen. Dieser belastete sich bei der Kommunikation mit den vermeintlichen Kunden selbst und konnte schließlich bei einem Scheinkauf verhaftet werden.

Zu diesem Themenkomplex veranstaltet die Cyber Akademie vom 15.01.2018 bis 17.01.2018 die Cyber-Akademie-Klausur "Digitale Ermittlungen und Kriminalistik heute und morgen" in Würzburg. *Weitere Informationen finden Sie hier.*

Europäischer Cyber-Sicherheitsmonat

Viele Aktionen und Angebote im Oktober

(CAk/stb) Bereits zum fünften Mal wird der European Cyber Security Month (ECSM) unter Federführung der ENISA (European Agency for Network and Information Security) durchgeführt. Im Oktober werden dazu EU-weit Sensibilisierungsaktionen angeboten. In Deutschland erfolgt die Koordinierung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI).
Ziel des Aktionsmonats ist es, Cyber-Sicherheit als grenzübergreifende Herausforderung bewusst zu machen und auf Risiken und Schutzmaßnahmen im digitalen Raum aufmerksam zu machen. In Deutschland beteiligen sich über 60 Partner, darunter Organisationen der öffentlichen Verwaltung, Unternehmen, Verbände sowie wissenschaftliche Einrichtungen.
Die Partizipationsmöglichkeiten sind dabei vielfältig. Neben Awareness-Kampagnen oder Veranstaltungen werden auch Schulungen und Experten-Workshops durchgeführt und Informationsangebote im Web aufbereitet. Die ENISA wird während des ECSM wochenweise verschiedene Schwerpunktthemen in den Fokus rücken, darunter "Cyber-Sicherheit am Arbeitsplatz" und "Sicherheit und Schutz persönlicher Daten".

Zur Eröffnungsveranstaltung, die an der Technischen Universität in Tallinn stattfand, sagte Andrus Ansip, Vizepräsident der Europäischen Kommission und Kommissar für den digitalen Binnenmarkt: "Cyber-Sicherheit ist ein Grundstein der digitalen Welt; sie liegt in unserer gemeinsamen Verantwortung, für jeden von uns, jeden Tag. Ich begrüße die gemeinschaftlichen Bestrebungen, Awareness zu steigern sowie die konkreten Aktivitäten im Sinne der Cyber-Sicherheit in ganz Europa."

Anmeldung weiter möglich
Bislang sind europaweit über 300 Aktionen angekündigt. Eine Übersicht über Angebote in Deutschland nach Zielgruppen stellt das BSI auf seiner Webseite bereit. Die Anmeldung weiterer Aktionen im Zeitraum bis Mitte November 2017 ist weiterhin über die Webseite des ECSM möglich. "Der Aktionsmonat ECSM macht deutlich, dass Cyber-Sicherheit in allen Lebensbereichen relevant ist und dass sie wesentlicher Bestandteil einer nachhaltigen Digitalisierung ist. Das spiegelt sich auch in der Bandbreite der diesjährigen Aktionen wider, die sich an unterschiedliche Zielgruppen richten – Bürger, Unternehmen, Verwaltung und Wissenschaft", sagt Arne Schönbohm, Präsident des BSI.

Internationale Datenschutzkonferenz

Entschließung zu autonomen Fahren verabschiedet

(CAk/mfe) Die Internationale Datenschutzkonferenz, in der Behörden aus 78 Nationen vertreten sind, hat eine Entschließung zum Datenschutz beim automatisierten und vernetzten Fahren beschlossen. Das Dokument umfasst insgesamt 16 Punkte. Darin wenden sich die Tagungsteilnehmer an Autohersteller, -zulieferer, Gesetzgeber und Behörden sowie an Unternehmen, die fahrzeugbezogene Internetdienste anbieten.
Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Andrea Voßhoff und ihre Kollegen appellieren in dem Dokument an die Adressaten, das Recht auf Privatsphäre der Fahrzeugnutzer in jeder Entwicklungs- und Herstellungsphase neuer Produkte und Dienste zu beachten. Gleiches gilt für den Schutz personenbezogener Daten.
Voßhoff erklärte zu der Entschließung: "Das Auto ist Symbol von Freiheit und Unabhängigkeit. Die Digitalisierung des Straßenverkehrs könnte dies grundlegend verändern." In modernen Fahrzeugen sammelten bereits heute zahlreiche Sensoren Daten zum Fahrverhalten und zu den zurückgelegten Strecken. Daraus ließen sich detaillierte Persönlichkeitsprofile erstellen, warnte sie. Aus diesem Grunde müssten Fahrer immer die komplette Entscheidungshoheit über die Verwendung personalisierbarer Fahrzeugdaten haben. Grundsätzlich sollten sie über jede Datenverwendung vollständig und transparent unterrichtet werden, verlangte Voßhoff.

Unschlagbares Nachschlagwerk zur Datenschutz-Grundverordnung

Praktisch und umweltfreundlich

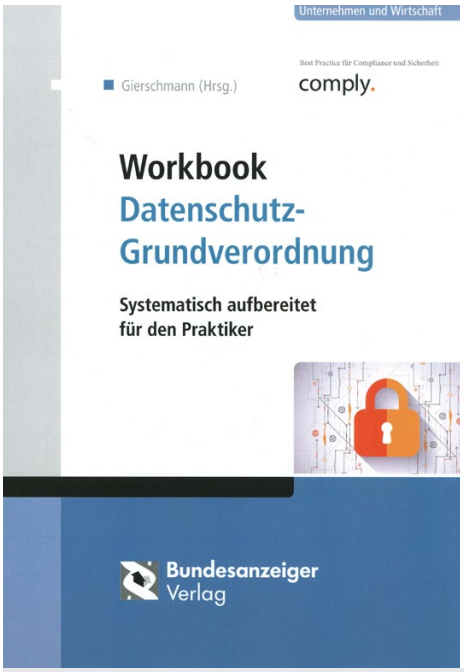
(CAk/vs) Ob in Behörden oder Unternehmen: Datenschutzverantwortliche Personen erhalten mit dem Workbook Datenschutz-Grundverordnung aus dem Bundesanzeiger Verlag eine praxisorientierte Handlungshilfe.

Das 176-seitige Werk besticht durch seine klare und verständliche Gliederung. Denn je nach Typus findet der Leser die einzelnen Artikel der EU-Datenschutz-Grundverordnung (EU-DSGVO) inklusive der jeweiligen Erwägungsgründe sowie der daraus resultierenden Sanktionen im Fließtext aufgelistet als auch in einer tabellarischen Übersicht. Auf der einen Seite enthält der Fließtext sämtliche wichtigen Informationen und ermöglicht es dem Nichtjuristen, sich durch den Aufbau schnell in den Gesetzestext einzulesen.

Auf der anderen Seite bietet die Übersicht gerade erfahrenen Datenschutzbeauftragten eine Gegenüberstellung der finalen Fassung der EU-DSGVO mit der Ursprungsversion. So können Interessierte die jeweiligen Entwicklungen zwischen den beiden Gesetzestexten nachvollziehen.

Erleichternd wirkt ein Glossar mit allen englischen datenschutzrechtlichen Begriffen. Aufgrund der englischsprachigen Urfassung umfasst dieser nicht nur die Erläuterungen der englischen, sondern auch der deutschen Datenschutzbegriffe. Somit wird dem Leser das Nachschlagen in einem "Dictionary" erspart. Für Notizen, Randbemerkungen und Kommentare steht auf jeder Seite ein separater Abschnitt zur Verfügung, was die leidige Auseinandersetzung mit abfallenden Klebezetteln unnötig macht. Sehr praktisch und umweltfreundlich noch dazu. Abgerundet wird das Buch durch ein Stichwortverzeichnis, das ebenfalls die Suche nach dem ein-schlägigen Artikel, dem jeweiligen Erwägungsgrund sowie dem dazugehörigen Sanktionsartikel erleichtert. Das Stichwortverzeichnis ist so ausgelegt, dass auch Begriffe aus dem allgemeinen Praxissprachgebrauch zu finden sind und den jeweiligen Artikel ausweisen.

Fazit: Das Workbook gibt nicht nur Praktikern und alteingesessenen Datenschutzbeauftragten durch einen kurzen Blick den sofortigen Durchblick, sondern ist insbesondere für Neueinsteiger im Gebiet des Datenschutzes und Nichtjuristen empfehlenswert.



Dr. Sibylle Gierschmann: Workbook Datenschutz-Grundverordnung, Systematisch aufbereitet für den Praktiker; Bundesanzeiger Verlag 2016, Preis: 39,80 Euro.

Cybercrime im Wandel

Vom Skript Kiddie bis zur Organisierten Kriminalität

(CAk/bst) Diebstahl, Sabotage, Spionage, Betrug: Viele seit Jahrhunderten bekannte Deliktsformen haben heute ihre digitalen Entsprechungen. Kriminelle dringen in fremde Netze ein, beschädigen IT-Systeme, schöpfen persönliche Daten ab oder spähen Betriebsgeheimnisse aus.

Gleichermaßen beobachtet man eine zunehmende Verlagerung von Formen der Organisierten Kriminalität ins Internet. Das Darknet bietet eine ideale Plattform für den Handel mit allen möglichen illegalen Gütern von gestohlenen Daten, über Waffen und Drogen bis hin zu kriminellen Dienstleistungen im Cyber-Raum oder der tatsächlichen Welt.

Cybercrime im engeren Sinne bezeichnet Straftaten, bei denen IT-Systeme wesentlich für die Tatausführung sind oder sogar die Tatwaffe darstellen. Das Bundeskriminalamt (BKA) unterscheidet hier zwischen Computerbetrug, Spionage beziehungsweise Datendiebstahl, Fälschung und Täuschung im Zusammenhang mit Daten, Sabotage und Manipulation von Daten sowie Missbrauch von Kommunikationsdiensten. Diese Deliktsformen gehen in vielen Fällen mit einer Kompromittierung von IT-Systemen der Betroffenen einher.

Für Hacker ist aller Anfang leicht

Das Eindringen in IT-Netzwerke ist dabei längst nicht nur erfahrenen und besonders kreativen Hackern vorbehalten. Dank leicht zu verstehender Anleitungen und kostenloser Hacker-Werkzeuge, die ohne Probleme im Internet gefunden werden können, gelingt es

Professionelles Kollektiv, genialer Hacker oder unbedarftes Skript Kiddie? Täterprofile sind bei Cybercrime nicht immer leicht zu ermitteln.
Foto: CAk/medithIT, CC BY 2.0, flickr.com

auch mit begrenzten IT-Kenntnissen schlecht gesicherte Systeme zu infiltrieren. Sogenannte Skript Kiddies profilieren sich in einschlägigen Internetforen mit solchen Erfolgen.
Regelmäßig sind aber auch große Unternehmen mit nicht unerheblichen IT-Sicherheitsbudgets von Cyber-Angriffen betroffen – große Datenlecks der letzten Jahre wie bei Sony, Yahoo oder Equifax sind nur eine mögliche Folge. Auch bei solchen Aufsehen erregenden Fällen sind nicht immer geniale Profis am Werk gewesen. Oft genug sind es lang bekannte Angriffsmethoden und Sicherheitslücken, die die Hacker zum Erfolg führen. Das von Unternehmen am häufigsten genannte Einfallstor für Hacker ist Phishing. Das ist Ergebnis des Threat Landscape Survey 2017 des SANS Institute, für den weltweit 250 Sicherheitsexperten aus der Privatwirtschaft befragt wurden. Allein im letzten Jahr sind demnach 40 Prozent der Unternehmen betroffen gewesen. Außerdem seien durch Phishing-Angriffe die größten Schäden entstanden.

Hohe Schäden durch Cyber-Kriminelle

Beim Phishing werden mal mehr, mal weniger professionell gestaltete betrügerische E-Mails als Köder verwendet, um Schadsoftware wie Verschlüsselungstrojaner zu verbreiten, sensible Informationen zu erlangen oder durch sogenanntes Social Engineering durchdachte Betrugsmaschen durchzuführen. So beim CEO-Fraud, bei dem im Namen eines Vorgesetzten eine Geldüberweisung angeordnet wird. Schließlich können sich kriminelle Hacker und Cyber-Spione auch Zugang zu Unternehmensnetzen verschaffen, indem sie Mitarbeiter unter einem Vorwand zur Herausgabe ihrer Login-Daten bringen.
Wie konkret die Gefahr der Spionage für die Privatwirtschaft ist, zeigen Ergebnisse einer vom Bitkom beauftragten repräsentativen Umfrage, der zufolge über ein Drittel der deutschen Unternehmen davon ausgeht, dass ihnen innerhalb der letzten zwei Jahre sensible Daten gestohlen worden sind. 28 Prozent glauben, dass ihre digitale Kommunikation ausgespäht wurde und wiederum mehr als ein Drittel meint, von digitalem Social Engineering betroffen gewesen zu sein. Insgesamt ist der deutschen Wirtschaft der Studie zufolge ein Schaden von 53 Milliarden Euro durch Delikte im Bereich der Cyber-Kriminalität entstanden.

Ransomware weiter beliebt

Ein vermehrt auftretendes Phänomen ist die Erpressung durch Ransomware. Krypto-Trojaner verschlüsseln ganze Festplatten und Geräte in der unmittelbaren Netzumgebung. Eine Freischaltung wird gegen Überweisung eines Lösegeldes in Bitcoin oder anderen digitalen Währungen in Aussicht gestellt. Der Vorteil für die Täter liegt darin, dass Transaktionen hier pseudonym ablaufen und die Eingriffsmöglichkeiten durch Strafverfolgungsbehörden beschränkt sind.
Auch die Erpressung mit Ransomware kann weitgehend ohne besonderes Expertenwissen durchgeführt werden. Einerseits lassen sich eigene Krypto-Trojaner mittels Malware-Toolkits – das sind Werkzeugkästen für Schadsoftware – aus Versatzstücken anderer zusammenbauen.
Basis für Nutznießer ist jedoch eine regelrechte Industrie, die sich um das Geschäftsmodell Ransomware entwickelt hat. Tätergruppierungen, die auf Grundlage originärer und gut entwickelter Schadsoftware Erpressungen durchführen, sind häufig hoch professionell organisiert und verfügen über mehr als reine Hacker-Expertise. Es gibt Zuständigkeiten für die Abwicklung der Finanztransaktionen und das Management von Hunderten oder Tausenden Entschlüsselungscodes, die nach Zahlungseingang ausgegeben werden. In einigen Fällen soll es sogar eine Art Service- und-Support-Center gegeben haben. Dort konnten Betroffene sich melden, um Informationen zum Ablauf der Lösegeldzahlungen einzuholen. Weitere Mittäter kümmern sich gegebenenfalls um den Vertrieb von Dienstleistungen oder den Weiterverkauf entwickelter Schadcodes.

Digitale Schwarzmärkte boomen

Plattform dafür sind Foren und Marktplätze im Internet, auf denen neben Drogen, Waffen und anderen klassischen illegalen Waren auch immer mehr Handwerkszeug für Cyber-Kriminelle angeboten wird. Während viele Standardtools für Hacker ohne Weiteres kostenfrei im Netz zu finden sind, werden für hochpotente Malware oder bisher nicht veröffentlichte Sicherheitslücken hohe Summen verlangt.
Fündig wird man auch im Bereich Infrastrukturen für Distributed Denial of Service-Attacken (DDoS-Angriffe). Ziel solcher Attacken ist es, Webseiten und Dienste durch eine Flut von unerwünschten Anfragen zu überlasten und schließlich auszuschalten. Dafür können Botnetze als Grundlage dienen: Armeen von infizierten Computern und netzwerkfähigen Geräten, die nun ohne Wissen ihrer Besitzer ferngesteuert werden.
Bots können aber nicht nur für DDoS-Angriffe, sondern auch zur massenhaften Verteilung von Spam oder schadhaften E-Mails gemietet werden. Es sind auch Fälle bekannt, in denen kriminelle Betreiber feststellten, dass sie bei der wahllosen Verteilung ihrer Botnetz-Schadsoftware zufällig einzelne Rechner in großen Organisationen erwischt hatten. Solche kompromittierten Geräte werden dann auch zu hohen Preisen einzeln angeboten – als Eintrittstor für andere Kriminelle, die es auf eben diese Organisation abgesehen haben.

Ermittlungserfolge im Darknet

Eine besondere Herausforderung für die Strafverfolgung ergibt sich aus Technologien, die Kriminellen ein hohes Maß an Anonymität versprechen. Grundlage für den Boom des Darknets für illegale Geschäfte sind das TOR-Netzwerk, das Internetzugriffe mehrfach verschlüsselt umleitet, und die Kryptowährung Bitcoin, mit der Zahlungen an sonst üblichen, streng regulierten Kreditinstituten vorbei getätigt werden können.
Dass es sich hier aber nicht um einen rechtsfreien Raum handelt, zeigen Ermittlungserfolge. Schon 2013 gelang es US-amerikanischen Behörden den ersten großen Darknet-Markt Silk Road zu schließen. Der Betreiber Ross Ulbricht wurde zu einer lebenslangen Haftstrafe verurteilt. Auch in Europa kommt es immer wieder zu Sperrungen und Verhaftungen. So konnte der Hansa Market – einer der größten illegalen Darknet-Märkte der letzten Jahre – vom BKA in Zusammenarbeit mit der niederländischen Polizei übernommen und abgeschaltet werden. Die beiden Administratoren der vor allem für den Drogenhandel genutzten Plattform befinden sich seit Juni 2017 in Untersuchungshaft. Aus deren illegalen Geschäften konnten Bitcoins im Wert von über 2,5 Millionen Euro beschlagnahmt werden.

Praxistipps der Cyber Akademie

Neues aus IT- und Datenschutzrecht

(CAk) In regelmäßigen Abständen präsentiert die Cyber Akademie neue Entwicklungen im IT- und Datenschutzrecht.

Über das Recht auf „Vergessenwerden“

In Art. 17 der ab dem 25.05.2018 geltenden DSGVO ist nicht nur die Pflicht des Verantwortlichen zur Löschung nicht mehr benötigter Daten festgelegt, sondern auch „Recht auf Vergessenwerden“ im Original „Right to be forgotten“ .

Nach Art. 17 Abs. 1 lit. (a) bis (f) muss ein Verantwortlicher (das Unternehmen, oder die Behörde) personenbezogene Daten löschen, wenn die betroffene Person die Löschung verlangt, hat der Verantwortliche die Daten öffentlich gemacht, die dann gelöscht werden müssen, muss er dafür Sorge tragen, dass auch Verknüpfungen zu diesen Daten gelöscht werden (Art. 17 Abs. 2 DSGVO).

In der Praxis bei der Anwendung des Art. 17 DSGVO zunächst zu prüfen, ob Daten öffentlich gemacht wurden und an welcher Stelle, bzw. an wen diese weitergegeben worden sind. Anschließend ist weiter zu prüfen, ob eine der in Art. 17 Abs. 3 DSGVO genannten Ausnahmen greift und insoweit keine Löschung nötig sein könnte. Sofern die betroffene Person eine Löschung verlangt hat und keine Ausnahmen vorliegt, müssen andere Verantwortliche, die die öffentlich gemachten Daten weiterverwendet haben, von der Pflicht zur Löschung informiert werden.

Für die praktische Umsetzung dieser Vorschrift ist es für den Verantwortlichen unerlässlich, im Vorfeld ein detailliertes Lösch- und Sperrkonzept entwickelt zu haben, um dem Anspruch auf Löschung und „Vergessenwerden“ im Sinne der Vorschrift gerecht werden zu können.

Insbesondere sollte in diesem Konzept festgelegt werden, wer die rechtliche Kontrolle durchführt und wer im Falle einer positiven Prüfung die Informationen weiterleitet. Hierfür sind im Konzept auch die Voraussetzungen einer reibungslosen internen Kommunikation und das Vorhalten der erforderlichen Technik zur Umsetzung der Vorschrift zu definieren und zu fordern.

Aussetzung der Vorratsdatenspeicherung vs. Videoaufzeichnung in öffentlichen Verkehrsmitteln

Videoüberwachung in den Stadtbahnen und Bussen der hannoverschen ÜSTRA ist mit dem Datenschutzrecht vereinbar

Der 11. Senat des Niedersächsischen Oberverwaltungsgerichts hat mit Urteil vom 7. September 2017 (Az. 11 LC 59/16) die Berufung der Landesbeauftragten für den Datenschutz Niedersachsen gegen ein Urteil des Verwaltungsgerichts Hannover zurückgewiesen und damit die Aufhebung einer datenschutzrechtlichen Anordnung im Ergebnis bestätigt.

Die klagende ÜSTRA hat in zahlreichen ihrer Fahrzeuge feststehende Videokameras installiert, mit denen im sog. Blackbox-Verfahren durchgehend Bewegtbilder vom Fahrzeuginnenraum aufgezeichnet werden, diese werden nach 24 Stunden wieder gelöscht. Die Aufzeichnung dienen unter anderem zur Beweissicherung bei Vandalismusschäden und zur Verfolgung von Straftaten

Das Oberverwaltungsgericht hat die Entscheidung des Verwaltungsgerichts im Ergebnis bestätigt. Nach Ansicht des 11. Senates ist das Bundesdatenschutzgesetz allerdings anwendbar und erlaubt der ÜSTRA die Videoüberwachung in ihren Fahrzeugen. Die Videoüberwachung dient der Wahrnehmung berechtigter Interessen der ÜSTRA, insbesondere der Verfolgung von Straftaten gegen ihre Einrichtungen und der Verhütung solcher Straftaten. Die erforderliche Abwägung mit den schutzwürdigen Interessen des von den Überwachungsmaßnahmen betroffenen Personenkreises fällt zugunsten der von der ÜSTRA geltend gemachten Belange aus. Die Revision zum Bundesverwaltungsgericht hat der 11. Senat nicht zugelassen.

IMPRESSUM

Herausgeber: Cyber Akademie GmbH, Geschäftsführer: Florian Lindemann; R. Uwe Proll
Seminarleiter: Benjamin Bauer
Geschäftsstelle: Friedrich-Ebert-Allee 57, 53113 Bonn, Telefon: 0049-228-97097-0, Telefax: 0049-228-97097-75, ↗ *www.cyber-akademie.de*
Registergericht: HRB 148255 AG Berlin (Charlottenburg)
Redaktionelle Leitung: R. Uwe Proll (presserechtlich verantwortlich); **Redaktion:** Benjamin Bauer, Florian Lindemann; **Redaktionsassistenz:** Kerstin Marmulla, Kirsten Klenner, Sebastian Lahr, Virginia Schmidt (Berlin)
Programmbeirat: Dr. Bernd Benser, Chief Business Officer GridLab GmbH; Prof. Dr. Wilfried Bernhardt, Staatssekretär a.D., Rechtsanwalt und Honorarprofessor für Internetrecht, Dr. Gerd Landsberg, Geschäftsführendes Präsidialmitglied des Deutschen Städte- und Gemeindebundes (DStGB); Dr. Philipp Amann, Europol, European Cybercrime Centre (EC3); Dr. August Hanning, Staatssekretär a.D. Bundeministerium des Innern, Präsident des Bundesnachrichtendienstes a.D.; Reinhold Harnisch, Geschäftsführer Kommunales Rechenzentrum Minden-Ravensberg/Lippe; Hans-Jürgen Hohnen, Staatssekretär a.D. Innenministerium Brandenburg; Prof. Dr. Radu Popescu-Zeletin, ehem. Leiter des Fraunhofer Instituts für Offene Kommunikationssysteme; Dieter Schneider, LKA-Präsident Baden Württemberg a.D.; Jörg Bruchmüller, Landesbezirksvorsitzender der Gewerkschaft der Polizei (GdP) in Hessen; Dieter Schürmann, Landeskriminaldirektor im Ministerium für Inneres und Kommunales NRW