# CAk report

Newsletter der Cyber Akademie zur Informationssicherheit

CAk Cyber Akademie

Nr. 44 Mai 2017


Neues Seminar

## Belastbare IT-Gutachten erstellen und bewerten

Digitalen Beweisen kommt in Gerichtsverfahren eine immer größere Bedeutung zu. In diesem neuen Seminar der Cyber Akademie wird praxisorientiert vermittelt, was Auftraggeber von IT-Forensikern und Gutachtern erwarten können und wie belastbare IT-Gutachten erstellt werden müssen.

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 neuen 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**

Revisionssichere Service Level Agreements (01.06.2017, Bonn)

CYBER AKADEMIE-KLAUSUR (19.06.2017 - 21.06.2017, Würzburg)

ISIS12 für Kommunen (20.06.2017, Berlin)

Netzwerk- und WLAN-Sicherheit (20.06.2017 - 22.06.2017, München)

IT-Sicherheit und Datenschutz – Neue Gesetzesvorgaben und ihre Auswirkungen auf die IT-Vergabe (21.06.2017, Bonn)

Webanwendungssicherheit und Penetrationstests (27.06.2017, München)

**www.cyber-akademie.de**

## Gestalteter Wandel oder administriertes Chaos?

# Münchner Cyber Dialog 2017 am 29. Juni 2017

(CAk/stb) Unter dem Motto "Gestalteter Wandel oder administriertes Chaos? Sichere Digitale Transformation in Staat, Wirtschaft und Gesellschaft", findet am 29. Juni der diesjährige Münchner Cyber Dialog in der bayerischen Landeshauptstadt statt.

Bereits zum vierten Mal organisieren die Cyber Akademie und der Behörden Spiegel die Dialogveranstaltung, bei der sich im Münchner Marriott Vertreter aus Politik, Wirtschaft und Wissenschaft über Chancen, Risiken und Gestaltungmöglichkeiten der Digitalisierung austauschen. Neben hochrangigen Vertretern aus den Verwaltungen von Bund und Ländern treffen sich in diesem Jahr Geschäftsführer und leitende Manager aus Industrie und Digitalwirtschaft, IT-Sicherheitsverantwortliche im öffentlichen und privaten Sektor sowie Experten aus Sicherheitsbehörden und Forschungseinrichtungen.

**Digitalisierung als Gemeinschaftsaufgabe**

Im April 2017 ist im Rahmen der G20-Präsidentschaft der Bundesrepublik erstmals ein Treffen der für die Digitalisierung zuständigen Ressortchefs der wichtigsten Industrie- und Schwellenländer zustande gekommen. Ergebnis des G20-Digitalministertreffens ist eine gemeinsame Erklärung und ein Arbeitsprogramm für die nächsten Jahre, in dem man sich auf wichtige Schwerpunkte für die aktive Gestaltung der Digitalisierung geeinigt hat.

Zentral für eine positive Entwicklung sind demnach Teilhabe aller Bürger am digitalen Fortschritt, fairer Wettbewerb sowie eine internationale Harmonisierung von Normen und Standards, um Zusammenarbeit und Vertrauen zu stärken. Die dafür nötigen Rahmenbedingungen müssen im Dialog aller Stakeholder geschaffen werden.

**Chancen und Risiken**

Nur so kann der digitale Wandel in allen Bereichen der Gesellschaft zum Vorteil der Menschen gelingen und nur so können negative Auswirkungen von wirtschaftlichen und sozialen Umbrüchen kontrolliert werden. Die zunehmende Automatisierung und Vernetzung der Prozesse in den Industrien birgt enorme Chancen für Wachstum und Wohlstand. Allerdings gehen Fortschritte bei Industrie 4.0, Künstlicher Intelligenz und Robotik auch mit der Furcht vor negativen Auswirkungen auf die Beschäftigung in vielen Branchen einher.

Mit dem Wachstum von Angriffsflächen und Abhängigkeiten von IT im Zuge der Digitalisierung wächst auch das Schadenspotenzial durch Störungen oder Angriffe von Cyber-Kriminellen. Während Resilienz und IT-Sicherheit bei den Betreibern Kritischer Infrastrukturen mittlerweile durch Regularien eingefordert werden, fehlt es gerade bei kleinen und mittelständischen Unternehmen aber auch Behörden noch häufig an ausreichender Motivation für die hinreichende Sicherung der eigenen IT-Infrastruktur.

**Workshops beim Münchner Cyber Dialog**

Dieses Spannungsverhältnis zwischen Erwartungen und Befürchtungen zieht sich als roter Faden durch die diesjährigen Themenschwerpunkte der Workshops, in denen fachkundige Referenten aus Politik, Wirtschaft und Forschung Erfahrungen austauschen und nötige Weichenstellungen für die digitale Zukunft diskutieren werden. In der Session 1 werden Herausforderungen an die Versorgungssicherheit in der Energiewirtschaft im Zuge der Digitalisierung thematisiert. Die Session 2 widmet sich unter der Leitfrage "Wie werden wir morgen arbeiten?" den Folgen von Künstlicher Intelligenz und Robotik auf die Beschäftigung. Die Resilienz von Wirtschaft, Gesellschaft und Staat gegen Bedrohungen im Cyber-Raum ist Thema der 3. Session. In Session 4 wird über die Zukunft des Mittelstandes und die Auswirkungen der Digitalisierung auf traditionelle Geschäftsmodelle und -strukturen diskutiert.

**CIO-Talk**

Ein Höhepunkt der Veranstaltung ist die anschließende Diskussions- und Fragerunde mit Leitern der Informationstechnik aus Behörden und Unternehmen. CIOs (Chief Information Officers) und CTOs (Chief Technology Officers) werden die Inhalte der Konferenz zusammenführen und gemeinsam erörtern. Ziel wird es sein, sich über Perspektiven der Zusammenarbeit der Stakeholder der Digitalisierung zu verständigen und Maßnahmen zu besprechen, mit denen die Chancen des Wandels optimal genutzt und Risiken minimiert werden können.

***Weitere Informationen zur Konferenz und das aktuelle Programm finden Sie unter*** www.muenchner-cyber-dialog.de.

Behörden müssen sich fit fürs europäische Datenschutzrecht machen

# Countdown zur Datenschutzgrundverordnung

(BS/stb) Ende April hat der Bundestag einen Entwurf für ein neues Bundesdatenschutzgesetz beschlossen. Damit soll das Gesetz an die EU-Datenschutzgrundverordnung (DSGVO) angepasst werden, die nach einer Übergangsfrist im Mai 2018 in Kraft tritt und dann unmittelbar in allen EU-Mitgliedsstaaten gilt. Die DSGVO fußt zwar weitgehend auf denselben Grundsätzen wie das bisherige deutsche Datenschutzrecht, dennoch kommen auf Behörden Neuerungen zu – insbesondere weil nicht mehr grundsätzlich zwischen öffentlichen und nicht-öffentlichen Stellen unterschieden wird.

Neues gilt es zum Teil zu beachten, wenn es um Pflichten und Vorgaben geht, mit denen altbekannte Grundsätze wie Zweckbindung, Datenminimierung und Datensicherheit umgesetzt werden sollen. So müssen nach dem Prinzip "Privacy by design" technische und organisatorische Maßnahmen ergriffen werden, und zwar unter Abwägung von Zweck und Umfang der Datenverarbeitung, Risiken für Betroffene und Aufwand für die datenverarbeitende Stelle. Im Gegensatz zum bisherigen deutschen Datenschutzrecht macht die DSGVO hier konkrete Angaben, was die Berücksichtigung des Stands der Technik angeht: Verschlüsselung und Pseudonymisierung von Daten werden explizit genannt.

"Privacy by default" meint hingegen die Forderung, die Abläufe von vornherein so zu organisieren, dass die Daten nur im für den jeweiligen Zweck erforderlichen Maße erhoben, verarbeitet und gespeichert werden. Die DSGVO ermöglicht die Einrichtung von Zertifizierungsverfahren, um bestehende Unsicherheiten in Bezug auf diese Verpflichtungen abzufangen. Die Vergabe und Genehmigung der entsprechenden Verfahren unterliegt den Datenschutzaufsichtsbehörden. Ansonsten unterliegt es den datenverarbeitenden Stellen und ihren Datenschutzbeauftragten, Erfordernisse einzuschätzen.

Eine gänzlich neue Pflicht betrifft die Datenschutz-Folgenabschätzung. Sobald eine Datenverarbeitung besondere Risiken für die Rechte von Betroffenen birgt, weil zum Beispiel rechtswirksame Entscheidungen von ihr abhängen oder sensible Daten betroffen sind, muss eine Folgenabschätzung vorgenommen werden. Diese muss die geplante Datenverarbeitung sowie ihren Zweck, Risiken und Maßnahmen zur Abhilfe erläutern. Bestätigt sich dabei das hohe Risiko für Betroffene, ist die zuständige Datenschutzaufsichtsbehörde in die Planung des Vorhabens einzubeziehen.

**Meldepflichten und Sanktionen auch für Behörden**

Die folgenreichsten Neuerungen der DSGVO für Behörden betreffen den Umgang mit Pflichtverletzungen und Datenschutzvorfällen. Im Falle eines Verlusts der Kontrolle über erhobene personenbezogene Daten muss die datenverarbeitende Stelle mindestens die zuständige Aufsichtsbehörde und gegebenenfalls auch Betroffene unterrichten – egal, ob eine Datenpanne selbstverschuldet oder zum Beispiel durch einen Cyber-Angriff verursacht wurde. Bisher galten solche grundsätzlichen Meldepflichten nur für nicht-öffentliche Stellen.
Die Meldung an die Aufsichtsbehörde hat dabei unverzüglich, in der Regel binnen drei Tagen zu erfolgen. Besteht ein deutliches Risiko für die Rechte von Betroffenen, so gilt die Pflicht zur Information auch ihnen gegenüber. Ob Betroffene benachrichtigt werden müssen, kann im Zweifelsfall auch in Konsultation mit der Aufsichtsbehörde entschieden werden.

Behörden sollten nun Konzepte zur Umsetzung erforderlicher Maßnahmen und zur Einführung der notwendigen Abläufe entwickeln, um spätestens zum Inkrafttreten der DSGVO die Vorgaben zu erfüllen. Im Gegensatz zum bisherigen Datenschutzrecht können ab Mai nächsten Jahres nämlich bei Pflichtverletzungen erhebliche Bußgelder von bis zu 20 Millionen Euro verhängt werden. Auch hier gilt die Verordnung grundsätzlich für alle Stellen, die personenbezogene Daten erheben.


(Foto:BS/Rob Pongsajapan cc by 2.0/www.flickr.com)

## Entspannt Lernen

# Cyber Akademie SUMMER SCHOOL in Tirol

(CAk/fl) 2017 bietet die Cyber Akademie erstmalig Sommerkurse an. In der Summer School der Cyber Akademie können Interessierte diese Zeit nutzen, um sich intensiv mit dem Thema Informationssicherheit auseinanderzusetzen und Zertifizierungsseminare zu besuchen. In der wunderschönen Landschaft des österreichischen Tirols, führt die Cyber Akademie in den Monaten Juli/August zwei Zertifizierungslehrgänge und einen Workshop durch. Neben den Schulungen bietet die Summer School ein entspannendes Rahmenprogramm für die Teilnehmer, um Informationssicherheit in Ruhe und im Dialog mit erfahrenen Dozenten zu erfahren.

**Zertifizierungskurse**

In der Summer School bietet die Cyber Akademie die Zertifizierungslehrgänge "IT-Grundschutzexperte" und "LEAD-Auditor" an. Der "IT-Grundschutz-Experte" erläutert den Teilnehmern die Grundsätze der Informationssicherheit auf Basis des IT-Grundschutzes, vermittelt die Implementierung des Standards in das Unternehmen oder die Behörde und bietet praktische Hinweise für die interne Auditierung und den Zertifizierungsprozess. Im Seminar "LEAD-Auditor" werden den Teilnehmern die Grundsätze der Informationssicherheit auf Basis des internationalen Standards ISO/IEC 27001 erläutert. In beiden Seminaren stehen die praktische Herangehensweise an den IT-Grundschutz bzw. ISO/IEC 27001-Standard sowie die Implementierung und Auditierung des Standards im Zentrum der Schulungen. Durch Kurzvorträge, praktische Übungen, Gruppenarbeiten sowie Rollenspielen auf Basis einer Fallstudie mit zahlreichen Praxis-Beispielen werden die Teilnehmer in die Lage versetzt, den Standard zu durchdringen sowie Implementierung und Auditierung in der Praxis umzusetzen bzw. zu begleiten.

**Incidence-Response-Workshop**

Ende August findet zudem der Workshop "Incidence Response" statt. Der Kurs, der in Form eines Rollenspiels unter Begleitung eines Trainerteams und unter realitätsnahen Bedingungen stattfindet, richtet sich in erster Linie an Führungskräfte aus Wirtschaft, Industrie und Verwaltung. Die Teilnehmer müssen im Rahmen des Rollenspieles als Team auf Informationssicherheitsvorfälle reagieren und ihr Unternehmen erfolgreich durch die Krise steuern. Neben Notfallbewältigung (Response) und Krisenmanagement (Organisation) sind Kommunikation (Reputation Management) und Kooperation mit Dienstleistern, Behörden etc. Kernthemen dieses Trainings.

(CAk/linznix, cc by 2.0, flickr.com)

***Weitere Informationen zur Cyber Akademie Summer School 2017 finden Sie unter*** www.cyber-akademie.de.

## VIDEO: Vernetzte Welt - Vernetzte Sicherheit

# Die Public-IT- Security am 12. + 13. September 2017


Am 12. + 13. September 2017 geht es auf der PITS 2017 um Effektivität und Effizienz des Zusammenwirkens von Strategien, Konzepten und Instrumenten für erfolgreiche Prävention, Bekämpfung und Abwehr von Cyber-Risiken und Cyber-Bedrohungen.

**Weitere Informationen sowie das aktuelle Programm finden Sie unter** www.public-it-security.de

Praxistipps der Cyber Akademie

# Neues aus IT- und Datenschutzrecht

(CAk) In regelmäßigen Abständen präsentiert die Cyber Akademie neue Entwicklungen im IT- und Datenschutzrecht. Im Zentrum dieser Ausgabe stehen Entscheidungen zur EU-Datenschutzgrundverordnung (DSGVO).

## Die Aufgaben des Datenschutzbeauftragten nach der DSGVO

Für viele Datenschutzbeauftragte stellt sich die Frage, ob mit der Datenschutzgrundverordnung (DSGVO) neue Aufgaben auf sie zukommen. In § 38 Abs. 1 a DSGVO beginnt es zunächst harmlos. Aufgabe des Datenschutzbeauftragten ist die Unterrichtung und Beratung des Verantwortlichen bzw. des Auftragsverarbeiters. Auch die Beschäftigten sind zu unterrichten und zu beraten. Neu und durchaus „speziell" ist die Anforderung aus Artikel 38 Abs. 1 b DSGVO. Nach dieser Regelung ist eine gesetzliche Überwachungspflicht festgelegt. Der Datenschutzbeauftragte soll die Einhaltung der DSGVO und der nationalen Datenschutzvorschriften überwachen. Hier stellt sich für viele Datenschutzbeauftragte die Frage, ob neue Haftungsrisiken mit dieser gesetzlichen Überwachungspflicht entstehen.

Für externe Datenschutzbeauftragte ist dies sicherlich zu bejahen. Deshalb werden viele Behörden und Unternehmen in der Praxis sicherlich überlegen, die sich aus dem Datenschutz ergebenden finanziellen Risiken durch hohe Bußgelder oder Schadensersatzansprüchen über eine externe Beauftragung „auszulagern".

Für interne Datenschutzbeauftragte wird auf den Erwägungsgrund 97 der DSGVO verwiesen. Dort wird im Schwerpunkt auf eine Unterstützung des Verantwortlichen und des Auftragsverarbeiters abgestellt. Dies insbesondere mit Verweis darauf, dass der Datenschutzbeauftragte nicht persönlich verantwortlich gemacht werden kann, wenn die Regelungen nicht eingehalten werden.

Selbst wenn man dieser Rechtsauffassung folgt, sind datenschutzrechtliche Missstände deutlich anzusprechen. Wir empfehlen Datenschutzbeauftragten, Mängel in der Datenschutzorganisation dokumentiert gegenüber der Leitungsebene zu thematisieren, um zu dokumentieren, dass die gesetzlichen Überwachungspflichten auch wahrgenommen wurden.

## Wechsel des Datenschutzbeauftragten?

Wechselt ein Datenschutzbeauftragter, ergeben sich verschiedene Anforderungen im Zusammenhang mit dem Wechsel im Amt. Das bayerische Landesamt für Datenaufsicht hat einige Grundsätze im 7. Tätigkeitsbericht 2015/2016, Ziff. 4.2, veröffentlicht. Dem neuen Datenschutzbeauftragten sind die entsprechenden Dokumente der Datenschutzorganisation zu übergeben, beispielsweise Verfahrensverzeichnisse, Unterlagen über durchgeführte Vorabkontrollen oder laufende Beschwerdefälle. Weiterhin sind die internen Tätigkeitsberichte, die Materialien bezüglich der Mitarbeiterschulungen sowie weitere Unterlagen zu den Regelungen der Datenschutzorganisation zu übermitteln. Unterlagen, die älter als 3 Jahre sind, müssen nicht übergeben werden. Nach Auffassung des bayerischen Landesamts für Datenschutzaufsicht ist bei der Verjährung auf die Regelung des § 195 BGB abzustellen, der von einer allgemeinen Verjährungsfrist von 3 vollen Kalenderjahren ausgeht. Die Verjährungsfrist beginnt immer am Ende des Kalenderjahres, in dem die Unterlagen abgeschlossen wurden.

Soweit Anfragen und Beschwerden gezielt vertraulich an die bisherige Datenschutzbeauftragte und den bisherigen Datenschutzbeauftragten gerichtet wurden, sind diese zu löschen oder zu vernichten. Eine Übergabe an den neuen Datenschutzbeauftragten erfolgt nicht.

## Außerordentliche Kündigung bei unberechtigtem Meldedatenabruf aus Neugier

Das Landesarbeitsgericht Berlin-Brandenburg hat in einem Urteil vom 01.09.2016 (Aktenzeichen 10 Sa 192/16) über eine außerordentliche Kündigung wegen unberechtigter Meldedatenabrufe zu entscheiden. Eine 55-jährige Mitarbeiterin des Landes hatte massenhaft Meldedaten im Bürgeramt abgerufen. Insgesamt ging es um 164 nicht autorisierte Abrufe aus dem Melderegister. Das Argument der Mitarbeiterin, die Abrufe seien aus reiner Neugierde erfolgt, ließ das Gericht nicht gelten. Die außerordentliche Kündigung ist nach Auffassung der Berliner Richter zu Recht erfolgt.

**IMPRESSUM**

**Herausgeber:** Cyber Akademie GmbH, Geschäftsführer: R. Uwe Proll (presserechtlich verantwortlich); Florian Lindemann;
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; **Redaktion:** Benjamin Bauer, Florian Lindemann; **Redaktionsassistenz:** Angelina Meyer (Bonn), Kerstin Marmulla, Kirsten Klenner, Sebastian Lahr (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