Neues aus der Cyber Akademie

Mai 2017

Themenseite in Kooperation mit:

CAk Cyber Akademie

IT-Gutachten erstellen und bewerten

(CAk) 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.

Fehler bei der Beweismittelgewinnung oder Dokumentation können im schlimmsten Fall zur Nichtverwertbarkeit von Beweisen in Gerichtsverfahren führen. Dieses gilt in besonderer Weise bei der IT-Fornsik. Foto: CAk/©deepagopi2011, Fotolia.com

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 im schlimmsten Fall zur Nichtverwertbarkeit dieser Beweise führen. Im Ergebnis kann dies nicht unerhebliche Konsequenzen für die Verfahrensbeteiligten, aber auch den Sachverständigen selbst, nach sich ziehen.

IT-Gutachten und Forensik – Theorie trifft Praxis

Um die Teilnehmenden für die Risiken zu sensibilisieren, gehen in diesem eintägigen Seminar Theorie und Praxis Hand in Hand.

Die Teilnehmer lernen 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.

Münchner Cyber Dialog 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.

Staatsminister Dr. Marcel Huber eröffnet den Münchner Cyber Dialog 2017. Foto CAk/Bayrische Staatskanzlei

IT-Direktor Peter Batt wird eine Key-note-Rede zum Thema Cyber-Sicherheit aus Sicht des Bundeministeriums des Innern halten. Foto CAk/BMI

Bereits zum vierten Mal organisieret die Cyber Akademie die Dialogveranstaltung, bei der sich 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 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.

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, haben gerade kleine und mittelständische Unternehmen Defizite im Bereich der IT-Sicherheit.

Dieses Spannungsverhältnis zwischen Erwartungen und Risiken zieht sich als roter Faden durch die diesjährigen Themenworkshops, in denen fachkundige Referenten aus Politik, Wirtschaft und Forschung Erfahrungen austauschen und nötige Weichenstellungen für die digitale Zukunft diskutieren werden. In einer Session werden Herausforderungen an die Versorgungssicherheit in der Energiewirtschaft im Zuge der Digitalisierung thematisiert. Die Resilienz von Wirtschaft, Gesellschaft und Staat gegen Bedrohungen im Cyber-Raum ist Thema einer weiteren Session. In Workshop 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 Diskussionsrunde mit Leitern der Informationstechnik aus Behörden und Unternehmen. Ziel ist es, die Perspektiven der Zusammenarbeit der Stakeholder der Digitalisierung zu diskutieren und Maßnahmen zu erörtern, mit denen die Chancen des Wandels optimal genutzt und Risiken minimiert werden können.

Das aktuelle Programm finden Sie unter www.muenchner-cyber-dialog.de .

NEUES aus IT- und Datenschutzrecht — **von Thomas Feil**

Aufgaben Datenschutzbeauftragter nach DSGVO

Für viele Datenschutzbeauftragte stellt sich die Frage, ob mit der Datenschutz-Grundverordnung (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 Schadensersatzansprüche 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 drei 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 drei 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.

Thomas Feil ist Fachanwalt für IT-Recht und Dozent der Cyber Akademie.

Foto CAk/privat