CAk report

Newsletter der Cyber Akademie zur Informationssicherheit

CAk Cyber Akademie

Nr. 42 März 2017

CYBER AKADEMIE-KLAUSUR

Technologievorschau bei der digitalen Kriminalistik

Eine effektive und effiziente Bekämpfung der Kriminalität, die mit oder mit Unterstützung der Informations- und Kommunikationstechnik begangen wird, ist im Zeitalter einer digital vernetzten und sich fortschreitend vernetzenden Gesellschaft eine der wesentlichen Herausforderungen an die Strafverfolgungsbehörden. In keinem anderen Feld stellt die Innovationskraft der Täter und die rasante Entwicklung der Hard- und Software die Polizei vor eine größere Problemstellung. Straftaten mit dem Tatmittel Internet / IT werden künftig die Regel sein.

Ermittlungen in allen Phänomenbereichen werden künftig nicht mehr ohne die Auswertung verschiedener digitaler Datenträger denkbar sein. Für eine erfolgreiche Kriminalitätsbekämpfung müssen die Strafverfolgungsbehörden über die anstehenden neuen Entwicklungen im IT- Bereich informiert sein. Einerseits, um künftiges Täterverhalten zu antizipieren, andererseits um die neuen technologischen Möglichkeiten für die eigene Ermittlungsarbeit zu analysieren bzw. zu nutzen. Der intensive Austausch mit Forschung, Wissenschaft und Wirtschaft ermöglicht viele Chancen, bestehende oder zu erwartende Fähigkeitslücken zu vermeiden oder zu schließen.

Hauptziel der Klausur ist es, die teilnehmenden Polizistinnen und Polizisten sowie Staatsanwälte im Bereich digitaler Ermittlungen gedanklich „vor die Lage“ kommen zu lassen, um besser auf die zukünftigen Entwicklungen reagieren zu können. Die Teilnehmerinnen und Teilnehmer erhalten einen Überblick über die möglichen digitalen Bedrohungen, die das polizeiliche Gegenüber künftig anwenden könnten. Sie werden über die digitale Zukunft z.B. im Bereich der zunehmenden Datenvernetzung informiert. Die Teilnehmenden lernen neue kriminalistische/ technologische Ansätze z.B. im Bereich der Datenanalyse kennen, die für die digitale Forensik und für Auswertung/ Ermittlungen künftig von Relevanz sein können. Der betrachtete Zeithorizont soll sich auf die nächsten 2-3 Jahre konzentrieren.

Kernthemen der CYBER AKADEMIE-KLAUSUR sind:

- **Die (Cyber-)Kriminalität der Zukunft**
- **Die digitale Zukunft**
- **Zukunftsanalyse, Lösungsoptionen für die Polizei aus Sicht der Wissenschaft und Industrie**
- **Zukunftsanalyse, Lösungsoptionen für die Polizei aus Sicht von Wissenschaft und Industrie (Fortsetzung)**

Die „CYBER AKADEMIE-KLAUSUR" findet vom **19.06.- 21.06.2017** in Würzburg statt.

INHALT

CAk-SEMINARE 2017

- Sensibilisierungskampagnen planen und durchführen (28.03.2017 - 29.03.2017, München)
- Informationssicherheit für (kommunale) Betreiber kritischer Infrastrukturen (29.03.2017, Düsseldorf)
- Informationssicherheit nach BSI-Grundschutz und ISO 27001 im Praxisvergleich (29.03.2017, Berlin)
- ISMS-Tools im Vergleich (30.03.2017, Düsseldorf)
- EU-Datenschutzgrundverordnung (04.04.2017, Hannover)
- BSI-Grundschutz in der Praxis (04.04.2017 - 05.04.2017, Düsseldorf)
- Grundlagen der Kryptologie (25.04.2017 - 26.04.2017, Hamburg)
- Betriebsrat und Datenschutz (25.04.2017, Hannover)

www.cyber-akademie.de

Cyber Akademie Summer School 2017

Entspanntes Lernen im Sommer

(CAk/fl) In den Sommermonaten 2017 bietet die Cyber Akademie erstmalig Sommerkurse an. In der Summer School der Cyber Akademie können Interessierte die Ferienzeit nutzen, um sich intensiv mit dem Thema Informationssicherheit auseinanderzusetzen und Zertifizierungsseminare zu besuchen. In der wunderschönen Landschaft des österreichischen Tirols, direkt an der deutsch-österreichischen Grenze, führt die Cyber Akademie in den Monaten Juli/August zwei Zertifikatslehrgänge 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.

Die Cyber Akademie Summer School findet im Juli/August in Tirol statt. (CAk/linznix, cc by 2.0, flickr.com)

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 und die Implementierung des Standards in das Unternehmen /die Organisation vermittelt. Gleichzeitig werden praktische Hinweise für eine entsprechende Auditierung gegeben. 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 in der Cyber Akademie Summer School 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.

Weitere Informationen zur Cyber Akademie Summer School 2017 finden Sie unter www.cyber-akademie.de.
Bei Fragen stehen wir Ihnen gerne per Mail an info@cyber-akademie.de mit dem Betreff Summer School zur Verfügung.

Cyber Akademie Workshop zur Ermittlungsarbeit bei IT-Sicherheitsvorfällen

Rechtssicheres Ermitteln in Unternehmen und Behörden

(CAk/bs) Wie im Falle eines Vorfalls in der eigenen Institution am besten reagiert werden sollte und wie externe Dienstleister und Behörden bei der Krisenbewältigung und Ermittlung helfen können, war Thema des Cyber-Akademie-Workshops “Rechtssicheres Ermitteln in Unternehmen und Behörden”.

Der letzte CAk-Workshop "Big Data Analytics in der Praxis" erfreute sich Ende Ende November 2016 großen Interesses. (CAk/Marco Feldmann)

Sicherheitsvorfälle in informationstechnischen Systemen bedrohen Unternehmen, Behörden und andere Institutionen gleichermaßen. Gleichzeitig ist die Wahrscheinlichkeit, Opfer eines Cyber-Angriffs zu werden, in den vergangenen Jahren beträchtlich gestiegen.

Dr. August Hanning, Staatssekretär a.D., sprach über das oft unterschätzte Problem des Geheimnisdiebstahls. In dem Zusammenhang sei nicht nur der klassische Hackerangriff von außen zu beachten. Auch die gezielte Abwerbung von Know-how-Trägern sei ein schwieriges Problem. Vor dem Wechsel in andere Unternehmen würden illoyale Mitarbeiter in manchen Fällen Insiderwissen nutzen, um Unbefugten Zugänge in IT-Systeme zu verschaffen.

Beispiele aus Wirtschaft, Industrie und Verwaltung

Eine Darstellung der Situation aus Sicht eines großen Konzerns bot Erik Liegle von der Volkswagen AG. Er zeigte die Komplexität des Themas IT-Sicherheit im Konzern auf. Die Automobilbranche habe sich dabei als ein besonders eindrückliches Beispiel erwiesen, weil der Wandel des gesamten Geschäftsmodells im Zuge von Vernetzung und Automatisierung von Fahrzeugen und Produktionsabläufen zahlreiche neue Herausforderungen und Risiken mit sich bringe. Dass es bei der Awareness von Mitarbeitern aber auch bei Gebäudeschutz und Organisation häufig Mängel gebe, erläuterte Wolfgang Straßer von @-yet anhand einiger Fallbeispiele. So habe man sich bei PEN-Tests für Kunden oft Zugang zu IT-Arbeitsplätzen oder Serverräumen verschaffen können, indem man die Hilfsbereitschaft von Mitarbeitern ausgenutzt habe. Straßer plädierte dafür, Angriffe durch Cyber-Kriminelle grundsätzlich öfter zur Anzeige zu bringen – schon deshalb, weil mehr Ermittlungsverfahren das Bewusstsein für die tatsächliche Gefahrenlage erhöhen.

Strafverfolgung

Wie Betroffene von Cyber-Kriminalität von der Einbindung der Ermittlungsbehörden profitieren können, erklärten Daniel Keller vom LKA Baden-Württemberg und Oberstaatsanwalt Markus Hartmann von der Staatsanwaltschaft Köln. Neben der fachlichen Expertise eigener Cyber Crime-Spezialisten warte die Polizei auch mit Ermittlungs- und Fahndungsmethoden auf, die privaten IT-Forensik-Dienstleistern nicht zu Gebote stünden, erklärte Keller. Dazu gehörten die Überwachung des WLAN-Verkehrs, aber auch klassische Methoden wie Rechtshilfeersuchen bei grenzübergreifender Kriminalität oder Hausdurchsuchungen bei Tatverdächtigen. Hartmann betonte, dass vor allem die Analyse von Finanzströmen aufschlussreich sei, weil für heutige Cyber-Kriminelle Geld die wichtigste Motivation darstelle. Hilfestellung leistet auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) – vor allem für die Bundesverwaltung und Betreiber Kritischer Infrastrukturen. Steve Ritter beschrieb exemplarisch die erfolgreiche Zusammenarbeit des BSI mit internationalen Strafermittlungsbehörden bei der Zerschlagung des Bot-Netzwerkes Avalanche.

Den Abschluss des Workshops bildete der Beitrag des öffentlich bestellten und vereidigten Sachverständigen Martin Wundram. Er berichtete über rechtliche und praktische Herausforderungen bei der Erstellung IT-forensischer Gutachten. Bei der Untersuchung von Systemen und Datenträgern seien gute Planung, eine kritische Herangehensweise und lückenlose Dokumentation notwendig, um gerichtsfeste Gutachten erstellen zu können.

Die zur Veröffentlichung freigegebenen Präsentationen der Veranstaltungen finden Sie unter www.cyber-akademie.de.

Die Cyber Akademie auf der CeBIT 2017

CAk Programm auf der CeBIT 2017

Wir laden Sie herzlich ein, uns am **22. März 2017** in der **Halle 6** zu besuchen. Die Cyber Akademie bietet im **TrainingssraumE58** einen praktischen Einblick in ihr Cyber Defence Simulation Training und ihr Seminarprogramm.

Folgendes Programm halten wir für Sie bereit:

Cyber Defence Simulation Training
Ziel ist es, das die Teilnehmer verschiedenste moderne Angriffe auf Unternehmensnetzwerke unter Anleitung verstehen, erkennen und ggf. abwehren.
Andreas Falkenberg, arbeitet seit vielen Jahren als professioneller White-Hat Hacker. In vielen internationalen Projekten in Europa, Asien und den USA kann er auf ein breites Erfahrungsspektrum, beginnend mit der Überprüfung von einfachen Webseiten bis hin zu Audits für Core-Banking Applikationen, zurückgreifen.

EU-Datenschutzgrundverordnung
In diesem Einsteigerseminar werden die gesetzlichen Neuerungen und die neuen Compliance-Anforderungen für Behörden und Unternehmen vorgestellt. Im Mittelpunkt der Veranstaltung stehen die praktischen Auswirkungen für die tägliche Datenschutzarbeit im Vergleich zum bisher geltenden Datenschutzrecht, beispielsweise im Bundesdatenschutzgesetz oder Telemediengesetz.

IT-Sicherheitsgesetz, NIS-Richtlinie und mehr
Das Seminar gibt einen Überblick über das aktuelle IT-Sicherheitsrecht, Anwendungsbereiche, externe Anforderungen sowie mögliche Interdependenzen. In einem zweiten Schritt werden Hinweise und praktische Handlungsoptionen vermittelt.

Aktuelles zum BSI-Grundschutz
Ziel des Seminares ist es, den Teilnehmern einen Überblick über das aktuelle IT-Sicherheitsrecht, Anwendungsbereiche, externe Anforderungen sowie mögliche Interdependenzen zu geben. In einem zweiten Schritt werden Hinweise und praktische Handlungsoptionen vermittelt.

Wir freuen uns auf Ihren Besuch in **Halle 6, Trainingsraum E58**. Anmeldungen zu den Trainings sind nicht notwendig. Eintrittskarten zur CeBIT stellen wir Ihnen gerne zur Verfügung.

Anfragen bitte an info@cyber-akademie.de.

Digitale Verwaltung 2025

Zukunftsperspektiven für den öffentlichen Sektor

Staatssekretär Klaus Vitt hielt die Eröffnungsrede auf der Konferenz. (Foto: Fujitsu)

Die Cyber Akademie war Partner der Fujitsu Jahreskonferenz Digitale Verwaltung, die am 14./15. Februar in Berlin stattgefunden hat. Vertreter aus Politik, Wissenschaft und Wirtschaft gaben unterschiedlichste Einblicke in die digitale Zukunft des Verwaltungssektors. In Keynotes, Podiumsdiskussionen, Breakout Sessions und einer begleitenden Ausstellung wurden Themen wie IT-Konsolidierung, IT-Security, Open Government und Elektronische Akte diskutiert. Klaus Vitt, Staatssekretär im Bundesministerium des Innern und Beauftragter der Bundesregierung für Informationstechnik, eröffnete die Veranstaltung mit der Keynote „Die digitalisierte Verwaltung – was jetzt zu tun ist! Darin wurden bereits umgesetzte und geplante Projekte, unter anderem den Ausbau des Online-Angebots der öffentlichen Verwaltung, mit konkreten Maßnahmen wie Verwaltungsportalen sowie Bürger- und Unternehmenskonten, präsentiert. Beispiele aus der Praxis gaben Dorothea Störr-Ritter, Landrätin Landkreis Breisgau-Hochschwarzwald, mit der Einführung der elektronischen Akte auf kommunaler Ebene, sowie Hagen Graeff, Generalbevollmächtigter des DVW – Gesellschaft für Geodäsie, Geoinformation und Landmanagement e. V., zur aktiven Beteiligung von Bürgern und Wirtschaft durch Open Government. Ein Highlight der Veranstaltung war die Vorstellung der Arbeit zur Zukunftsstudie „Mobilität 2025+“ des MÜNCHNER KREISES. Mitglieder des Forschungsteams und weitere Experten stellten exklusiv erste Eindrücke aus der branchenübergreifenden Zukunftsstudie vor und diskutierten u.a. zentrale Themen wie zukünftige Anforderungen an die Mobilität, den Wandel von Mobilitätsbedürfnissen sowie Schritte auf dem Weg zur vernetzten, intelligenten Mobilität.

Praxistipps der Cyber Akademie

Aktuell: Datenschutz-Recht & Recht der IT-Sicherheit 03/2017

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

Die Einwilligung nach der Datenschutzgrundverordnung (DS-GVO)

Die Einwilligung ist ein zentrales Element des Datenschutzes. Es ist auch abzusehen, dass die Einwilligung auch mit Geltung der DS-GVO ein zentraler Bestandteil bleiben wird.
Die Einwilligung wird in Art. 4 Nr. 11 der DS-GVO definiert. Eine Einwilligungder betroffenen Person ist jede, freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Die Einwilligung ist grundsätzlich höchstpersönlich zu erteilen. Eine Ausnahme kommt nur dann in Betracht, wenn mangels Einwilligungsfähigkeit nicht ohne gesetzlichen Vertreter eingewilligt werden kann. Dies betrifft insbesondere Minderjährige oder Geschäftsunfähige. Der Betroffene muss freiwillig handeln, also eine echte Wahl haben. Insbesondere in Arbeitsverhältnissen muss dies sorgsam eingehalten werden. Die Einwilligung darf nicht pauschal sein, sondern muss sich auf einen konkreten Vorgang beziehen. Zuletzt muss der Einwilligende auch über die konkrete Bedeutung und Reichweite seiner Erklärung informiert werden. Er muss letztlich wissen, worin er einwilligt.

Heimlicher Einsatz eines „Keyloggers“ am Arbeitsplatz

Das Landesarbeitsgericht Hamm hat sich in einer aktuellen Entscheidung (vom 17. 06. 2016 – 16 Sa 1711/15) mit der Frage auseinandergesetzt, ob der heimliche Einsatz eines Keyloggers zur Aufdeckung einer verbotenen privaten Nutzung des PC zu einem Beweisverwertungsverbot der dadurch erlangten Daten führt.
Der gekündigte Arbeitnehmer wurde als Webentwickler beschäftigt. Er war verpflichtet, den PC nur zu dienstlichen Zwecken zu nutzen. Im Zuge des Arbeitsverhältnisses informierte der Arbeitgeber darüber, dass er den Traffic und die Benutzung der Systeme mitloggen wird. Würde das ein Arbeitnehmer nicht wollen, könne er sich melden.

Das Gericht entschied, dass die mittels Keylogger gewonnenen Beweise nicht verwertet werden durften und die Kündigung daher unzulässig gewesen sei. Selbst wenn man § 32 I S. 2 BDSG als dem Grunde nach einschlägig betrachte, wäre der Eingriff unverhältnismäßig gewesen, weil man zuvor Kontrollen im Beisein des Arbeitnehmers hätte durchführen können und müssen. Eine wirksame Einwilligung läge mangels Schriftform und ausdrücklicher Erklärung des Arbeitnehmers nicht vor. Zuletzt sei auch der Eingriff in das informationelle Selbstbestimmungsrecht so groß, dass dieser nicht durch das Beweisinteresse des Arbeitgebers gerechtfertigt gewesen und daher von einem Beweisverwertungsverbot auszugehen sei.

Kernpunkte des NIS-Umsetzungsgesetzes

Das NIS-Umsetzungsgesetz dient der Änderung des IT-Sicherheitsgesetzes und basiert auf der Grundlage der NIS-Richtlinie der EU aus 2016. Ein entsprechender Regierungsentwurf wurde am 25.01.2017 von der Bundesregierung beschlossen. Im Wesentlichen sollen kritische IT-Infrastrukturen wirksamer vor Cyberangriffen geschützt werden. Die Planungen beinhalten konkret:
Das BSI (Bundesamt für Sicherheit in der Informationstechnik) erhält neue Befugnisse. So dürfen zukünftig auch vor Ort Termine stattfinden und die Übermittlungspflichten von KRITIS (kritische Infrastrukturen) wurden ausgeweitet. Das BSI wird nun auch in besonderen Fällen mit eigenen Kräften an Sicherheit und Funktionsfähigkeit derartiger Systeme mitwirken können (operative Mitwirkung). Dabei dürfen auch die notwendigen personenbezogenen Daten erhoben und verarbeitet werden.
Es erfolgt eine Vollharmonisierung der IT-Sicherheitsanforderungen für bestimmte Gruppen von digitalen Diensten mit Ausnahme der öffentlichen Verwaltung. Die Haftung für IT-Sicherheitsmängel wird vermutlich nicht angetastet.

CAk News in 100 Sekunden . . .

Umsetzungsgesetz NIS-Richtlinie

Thomas Feil,
Fachanwalt für IT-Recht,
Datenschutzbeauftragter
TÜV

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, Rebecca Hesse (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); Olivier Burgersdijk, 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