CAk report
Newsletter der Cyber Akademie zur Informationssicherheit

CAk Cyber Akademie

Nr. 30 / März 2016

Einschneidende Änderungen

Seminar zur EU-Datenschutzgrund-verordnung erfolgreich gestartet

Ende 2015 beschlossen, wird die Europäische Datenschutzgrundverordnung (EUDSGVO) zum 1. Januar 2018 in Kraft treten. Mit dem neuen Seminar stellt die Cyber Akademie die gesetzlichen Neuerungen und Compliance-Anforderungen für Behörden und Unternehmen vor. Im Zentrum stehen dabei die praktischen Auswirkungen für die tägliche Datenschutzarbeit.
Das Auftaktseminar der Cyber Akademie Anfang März lieferte interessante Ergebnisse für alle Stellen, die sich mit der Erhebung, Verwaltung und Verarbeitung von Daten sowie dem Schutz dieser Daten vor Missbrauch befassen.
Bußgelder: Neben Unternehmen laufen auch Behörden Gefahr bei Datenschutzverstößen Bußgelder bis zu 10.000.000,00€ zahlen zu müssen.
Neue organisatorische Herausforderungen: Bei der Verletzung des Schutzes personenbezogener Daten muss innerhalb von 72 Stunden eine Meldung an die Aufsichtsbehörde gemacht werden (Art. 31). Auch Betroffene müssen dann informiert werden. Eine entsprechende Meldeorganisation und Meldewege müssen intern festgelegt und organisiert werden.
Mehr Dokumentation: Es müssen Verfahren zur regelmäßigen Überprüfung der Datenschutzmaßnahmen eingerichtet werden. Die Maßnahmen sind zu dokumentieren (Art. 30). Bei Verstößen droht ein Bußgeld.
Auswirkungen auf Ausschreibungen: Die neuen Regelungen zum Datenschutz müssen bereits jetzt bei Ausschreibungsverfahren, beispielsweise bei mehrjährigen Rahmenverträgen, beachtet werden.

Das nächste Seminar zur EU-Datenschutzgrundverordnung findet am 31. Mai 2016 in München statt.

INHALT

Predictive Analytics Workshop ..... **Seite 2**

Bundesdruckerei sichert Cloud-Daten ..... **Seite 3**

Cyber Angriffe auf öffentliche Infrastrukturen in NRW ... **Seite 3**

Informationssicherheit in der EKD ..... **Seite 4**

CAk-Seminare 2016

Outsourcing von Geschäftsprozessen
12.–13. Apil 2016, Berlin

Betriebsrat und Datenschutz
19. April 2016, München

Social Media rechtssicher und datenschutzkonform nutzen
19. April 2016, Bonn

Das neue IT-Sicherheitsgesetz
21. April 2016, Hannover

Sichere Webanwendungen in der öffentlichen Verwaltung – Vergabe, Entwicklung, Abnahme
27.–28. Apil 2016, Bonn

www.cyber-akademie.de

Einsatzfelder, Praxisbeispiele und Anwendungsbereiche

Workshop der Cyber Akademie zu Predictive Analytics in Berlin

(CAk/mfe) Ende Februar 2016 kamen 60 Vertreter aus Wissenschaft, Behörden und Unternehmen auf Einladung der Cyber Akademie und Fraunhofer FOKUS zum Predictive Analytics-Workshop im Fraunhofer Forum Berlin zusammen.

Anhand der Anwendungsfelder Sicherheit, Energiewirtschaft, Medizin und Stadtplanung diskutierten Experten und Teilnehmer über Rahmenbedingungen, Voraussetzungen, Herausforderungen und Zielen des Einsatzes von Predictive Analytics.

Zum Auftakt berichtete Dieter Schürmann, Landeskriminaldirektor im Innenministerium Nordrhein-Westfalens, vom Projekt SKALA („System zur KriminalitätsAnalyse und LageAntizipation“). Durch das Pilotprojekt, das in Duisburg und Köln zur Bekämpfung des Wohnungseinbruchsdiebstahls eingesetzt wird, wolle man die Möglichkeiten und Grenzen der Vorhersage von Kriminalitätsschwerpunkten prüfen. Er unterstrich, dass bei SKALA keine personenbezogenen Daten erhoben würden. Schürmann sagte: „Wir wollen keine konkreten Täter, sondern bestimmte Räume vorhersagen.“ Mögliche Straftaten wolle man durch eine verstärkte Präsenz in diesen „Hotspots“ verhindern. SKALA werde polizeilichen Sachverstand keinesfalls ersetzen, sondern angesichts von 62.000 Einbrüchen in Nordrhein-Westfalen im Jahr 2014 vielmehr als „Entscheidungshilfe“ für die Beamten fungieren.

Anhand der Anwendungsfelder Sicherheit, Energiewirtschaft, Medizin und Stadtplanung diskutierten die Teilnehmer über Rahmenbedingungen, Voraussetzungen und Ziele des Predictive Analytics-Einsatzes. Foto CAk/Feldmann

Effizienter Einsatz knapper Ressourcen

„Vor die Lage kommen“ und seine Ressourcen effizienter einsetzen ist auch das Ziel von David von der Lieth, stellvertretender Abteilungsleiter für Gefahrenabwehr und Rettungsdienst bei der Berufsfeuerwehr Düsseldorf. Von der Lieth erläuterte, dass man Analyse-Tools zur Ermittlung von Abdeckungsgraden sowie zur Festlegung von Schutzzielen verwende. Damit träfe man die Entscheidung über die optimale lokale Verteilung von Rettungswagen sowie die Sicherstellung der Abdeckungswahrscheinlichkeiten mithilfe von Predictive Analytics. Gleichzeitig schränkte er jedoch auch ein: „Die Berufsfeuerwehr Düsseldorf macht noch kein Echtzeit-Predictive. Momentan fühlen wir uns mit einer quartalsweisen Analyse gut aufgehoben.“ Zu schaffen machten der Behörde zum Teil noch die großen Datenmengen.

Von der Influenza zum „Influencer“

Der Einsatz von Predictive Analytics steht nach wie vor am Anfang. Fast alle Beteiligten schilderten, dass der Schwerpunkt darauf liege, Zusammenhänge und Muster aufgrund vorhandener, bzw. verfügbarer Datenbestände zu erkennen und sein Handeln zielgerichtet darauf auszurichten. Dabei spiele die Qualität der vorhandenen Daten natürlich eine besondere Rolle. Pascal Lauria von Cogia Intelligence schilderte, dass die Marketing-Branche den „influencer“, die entscheidende Person mit einer großen Reputation und Reichweite suche, um Produkte und Meinungen zielgerichtet bewerben und verbreiten zu können. Dr. Göran Kirchner vom Robert-Koch-Institut hingegen erläuterte, dass Mediziner und Rettungsdienste nach Korrelationen und Wissen suchen, um ihre Ressourcen zielgerichtet einzusetzen und so beispielsweise die Ausbreitung von Krankheiten zu verhindern.

Bedarf an Erfahrungsaustausch – Best Practice Workshop 2017

Alle Beteiligten waren sich einig darin, dass der Einsatz von Predictive Analytics nur dann nachhaltig Akzeptanz bei den Anwendern finden werde, wenn er einen Mehrwert für Anwender und „Datenbereitsteller“ biete, sowie die Nutzung transparent und unter wissenschaftlicher Begleitung erfolge. Gleichzeitig sei es weiterhin notwendig, dass der „Faktor Mensch“ bei der Einschätzung und Bewertung der Analyseergebnisse und Vorhersagen eine zentrale Rolle spiele. Darüber hinaus müssten sich in den meisten Fällen die technisch-organisatorischen Rahmenbedingungen noch verbessern, um die Potenziale von Predictive Analytics – auch in Echtzeit - weiter erschließen zu können. Hierzu werden die Cyber Akademie und Fraunhofer FOKUS im Jahr 2017 wieder zu einem Praxis-Workshop einladen, um Fortschritte und neue Projekte im Analytics-Bereich vorzustellen.

Microsoft Cloud

Bundesdruckerei sichert Daten

Microsoft wird seine Cloud-Dienste Azure, Office 365 und Dynamics CRM Online ab der zweiten Jahreshälfte 2016 auch aus deutschen Rechenzentren anbieten. Für die Verschlüsselung und Absicherung des Datenverkehrs zwischen Kundenanwendungen und Cloud-Servern setzt Microsoft künftig auf die Zertifizierungsstelle D-Trust der Bundesdruckerei GmbH.

„Die Zusammenarbeit mit einer so vertrauenswürdigen Institution wie der Bundesdruckerei garantiert unseren Kunden, dass ihre Daten in der Microsoft Cloud Deutschland durch die neuesten im Markt verfügbaren Verschlüsselungstechnologien geschützt werden", so Michael Kranawetter, National Security Officer bei Microsoft Deutschland. Die Bundesdruckerei hat sich laut Microsoft in den vergangenen Jahren zu einem international führenden Anbieter für ID-System- und IT-Sicherheitslösungen entwickelt.

Mit den Hochsicherheitskonzepten der Bundesdruckerei werden Nutzer und Server zuverlässig authentifiziert, um einen verschlüsselten Datenverkehr zu gewährleisten. Für die Microsoft Cloud Deutschland wird D-TRUST für die Server sogenannte TLS-Zertifikate ausstellen, die die Kommunikation zwischen den Anwendern

Microsoft setzt bei der Verschlüsselung und Absicherung von Cloud-Daten zukünftig auf Lösungen der Bundesdruckerei.

Foto: CAk/ Chariclo, www.Fotolia.com

von Microsoft Azure und Office 365 sowie den Servern in den neuen deutschen Rechenzentren absichern. Zusätzlich können Kunden auch ihre eigenen Anwendungen in der Microsoft Azure Cloud mit den Zertifikaten der D-TRUST absichern. „Wir freuen uns sehr, dass sich Microsoft für die Absicherung seiner zukünftigen Public-Cloud-Angebote aus deutschen Rechenzentren die Bundesdruckerei und ihre Tochter D-TRUST als Partner ausgesucht hat", sagt Dr. Kim Nguyen, Geschäftsführer D-TRUST GmbH. „Wir bieten Microsoft und seinen Kunden eine etablierte Zertifikatslösung „Made in Germany" und zeigen, welche hohen Sicherheitsstandards Cloud-Angebote erfüllen."

Das lokale Angebot von Microsoft für Azure, Office 365 und Dynamics CRM Online richtet sich besonders an Organisationen und Unternehmen in datensensiblen Bereichen wie dem öffentlichen, dem Finanz- oder dem Gesundheitssektor. Der Datenaustausch zwischen den beiden Rechenzentren in Magdeburg und Frankfurt/Main findet über ein privates, vom Internet getrenntes Netzwerk statt, womit der Verbleib der Daten in Deutschland gesichert ist. T-Systems, eine Tochter der Deutschen Telekom, kontrolliert als Datentreuhänder den Zugang zu den Kundendaten. Durch die Garantie, dass sich die Daten auf Servern in Deutschland befinden, ist das Cloud-Modell auch für staatliche Stellen in Deutschland nutzbar.

Kooperation und Prävention als Gebot der Stunde

Cyber Angriffe auf öffentliche Infrastrukturen in NRW

In einer gemeinsamen Pressekonferenz bezogen die Spitzen des Landeskriminalamtes (LKA) Nordrhein-Westfalen, der Zentralstelle Cybercrime (ZAC), des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und dem Bundesverband der IT-Anwender (VOICE e.V.) Stellung zu der aktuellen Cyber-Bedrohungslage. Laut Uwe Jacob, Direktor des LKA NRW, sei der Verschlüsselungstrojaner „Locky", der u.a. das Lukaskrankenhaus Neuss lahmgelegt hatte, ein Weckruf gewesen. „Wenn ein Krankenhaus die Notfallversorgung einstellen und Operationen verschieben muss, wenn eine Stadtverwaltung keinen Zugriff mehr auf ihre Daten hat oder auch Unternehmen in ihrer Existenz bedroht sind, dann macht mir das große Sorgen" so Jacob mit Blick auf die jüngsten Attacken auf Krankenhäuser in NRW. Auch das LKA NRW war offenbar nur einen Klick davon entfernt, selbst Opfer von „Locky" zu werden.

Aktuell beobachten die Strafverfolger beobachten eine erhebliche Steigerung der Attacken sowie eine wachsenden Professionalisierung der Angreifer. BSI-Präsident Arne Schönbohm sprach sich für eine stärkere Zusammenarbeit zwischen Wirtschaft und Behörden aus, um der Cyber-Bedrohung begegnen zu können. Gleichzeitig legte er Arbeitgebern nahe, regelmäßige Awareness-Schulungen für die Mitarbeiter durchzuführen, denn „Prävention ist günstiger als Reaktion", so Schönbohm.

Zum Thema IT-Security-Awareness bietet die Cyber Akademie Live-Hacking Demonstrationen und Sensibilisierungs-Workshops für Unternehmen und Behörden an. ***Für weitere Informationen kontaktieren Sie uns bitte info@cyber-akademie.de***

Informationssicherheit in der Kirche

Evangelische Kirche bündelt Datenschutzaufsicht

(CAk/Michael Jakob) Mit der Berufung eines neuen Beauftragten für den Datenschutz der Evangelischen Kirche in Deutschland (EKD) wurde vor gut zwei Jahren angefangen, eine neue unabhängige Datenschutzaufsichtsbehörde in der EKD aufzubauen. Bis heute haben 16 von 20 Landeskirchen sowie fünf Diakonische Werke die Datenschutzaufsicht auf die EKD übertragen.

Die Evangelische Kirche ist ihrem Ziel, die Datenschutzaufsicht zukünftig gemeinsam für die Landeskirchen, die Diakonie und die EKD wahrzunehmen, in den letzten beiden Jahren einen wichtigen Schritt näher gekommen.

Oberkirchenrat Michael Jacob ist seit Januar 2014 Beauftragter für den Datenschutz in der EKD. *Foto: CAk/EKD*

Neue Datenschutzaufsichtsbehörde aufgebaut

Zur Erledigung der Aufgaben der Datenschutzaufsicht hat die EKD eine neue unabhängige Behörde (BfD EKD) aufgebaut, die der Beauftragte für den Datenschutz der EKD leitet. Die Behörde hat ihren Hauptsitz in Hannover und ist regional in vier Datenschutzregionen mit je einer Außenstelle gegliedert. Um sowohl dem rechtlichen als auch dem technischen Datenschutz bei der Aufgabenerledigung gerecht zu werden, arbeiten in der Behörde Juristen und Informatiker Hand in Hand. Die Datenschutzaufsicht in der evangelischen Kirche und ihrer Diakonie wird damit deutlich einheitlicher und umfänglicher wahrgenommen als in der Vergangenheit. Zugleich hat der BfD EKD die Vorgaben der (voraussichtlich) Anfang 2018 in Kraft tretenden Europäischen Datenschutzgrundverordnung im Blick auf eine unabhängige Datenschutzaufsicht bereits jetzt umgesetzt.

Die rechtlichen Vorgaben zum evangelischen Datenschutz und die Aufgaben einer Datenschutzaufsichtsbehörde sind im EKD-Datenschutzgesetz festgelegt. Zu den Hauptaufgaben des Beauftragten für den Datenschutz gehört, über die Einhaltung des Datenschutzes zu „wachen“. Dieses Wächteramt entspricht dem Selbstverständnis der evangelischen Kirche bei der Wahrnehmung dieser Aufgabe. Daneben geht es in der evangelischen Kirche heute natürlich vor allem auch um den Schutz der Daten von Gemeindegliedern und von Menschen, die kirchliche oder diakonische Einrichtungen in Anspruch nehmen sowie um den Schutz der Daten von Mitarbeitenden. Neben dem „Wächteramt“ sind Beratung und Weiterbildung die hauptsächlichen Aufgaben des BfD EKD. Vor allem die Weiterbildung der örtlich Beauftragten für den Datenschutz und der Betriebsbeauftragten für den Datenschutz hat dabei oberste Priorität. Gemeinsam mit dieser Gruppe bietet der BfD EKD kirchlichen Stellen Beratung an, um frühzeitig bei allen Vorhaben rechtliche und technische Aspekte des Datenschutzes zu berücksichtigen.

Ausblick

Nicht zuletzt durch die vielfältigen gesellschaftlichen Diskussionen und staatlichen Entwicklungen im Bereich Datenschutz der letzten Jahre liegt das Thema Datenschutz auch im evangelischen Bereich oben auf. Auch zukünftig sollen der eigene Datenschutz weiter ausgebaut und die speziell kirchliche Sicht in die allgemeine Diskussion eingebracht werden. Dabei ist dem BfD EKD besonders wichtig, dass die kirchliche Datenschutzaufsichtsbehörde nicht die Daten als solche, sondern die hinter den Daten stehenden Menschen schützt. Datenschutz ist und bleibt eben Menschenschutz.

Zum Thema IT-Sicherheit und Datenschutz in Einrichtungen der EKD und zur Umsetzung IT-Sicherheitsverordnung bietet die Cyber Akademie ein Seminar für IT-Beauftragte und Entscheidungsträger der EKD an.
Weitere Informationen finden Sie hier

IMPRESSUM

Herausgeber: Cyber Akademie GmbH, Geschäftsführer: R. Uwe Proll (presserechtlich verantwortlich); Leiter der Cyber Akademie: 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 , Angela Götze, Sebastian Lahr (Berlin)
Programmbeirat: Dr. Bernd Benser, Chief Business Officer GridLab GmbH; Dr. Gerd Landsberg, Geschäftsführendes Präsidialmitglied des Deutschen Städte- und Gemeindebundes (DStGB); Olivier Burgersdijk, Europol, European Cybercrime Centre (EC3); Dr. August Hanning, Staatssekretär a.D. Bundesministerium 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