Editorial - Grußwort des Forschungsprojektleiters »BayWiDI« Prof. Dr. Dirk Heckmann

Sehr geehrte Leserinnen und Leser,

ich wünsche Ihnen ein frohes und gesundes neues Jahr. Das Jahr 2017 beginnt mit dem dritten *BayWiDI*-Newsletter und vielen spannenden Entwicklungen im Bereich der IT-Sicherheit. So hat der Europäische Gerichtshof am 21. Dezember 2016 entschieden, dass die Mitgliedstaaten der Europäischen Union den Betreibern elektronischer Kommunikationsdienste keine allgemeine Verpflichtung zur Vorratsdatenspeicherung auferlegen dürfen. Einen Kurzkommentar zu dieser Entscheidung aus IT-sicherheitsrechtlicher Sicht finden Sie in diesem Newsletter.

Seit dem zweiten *BayWiDI*-Newsletter im vergangenen Oktober sind drei Monate vergangen, in denen das Projekt *BayWiDI* (Bayerisches Wissensnetzwerk Digitale Infrastrukturen und Recht für Unternehmen) weiter ausgebaut wurde. Im Moment befindet sich die Einführung eines internen Bereichs in der Konzeptionierung. Neben hilfreichen allgemeinen Informationen, wie einem umfassenden Lexikon zur IT-Sicherheit oder Erläuterungen zu allgemeinen Haftungsmaßstäben und -grundlagen, finden Sie als Premiumpartner von BayWiDI in diesem Bereich eine laufend aktualisierte Rechtsprechungsdatenbank zum IT-Sicherheitsrecht mit besonderem Mehrwert. Die Gerichtsentscheidungen sollen nicht nur für den unternehmerischen Gebrauch ansprechend aufbereitet werden, sondern auch eine Rechtsentwicklungsprognose beinhalten. Außerdem soll die Möglichkeit bestehen, die nach individuellem Auftrag für Sie erstellten Forschungsergebnisse (z.B. rechtswissenschaftliche Fachgutachten) zum Abruf bereitzustellen. Ein ausführlicher Bericht erwartet Sie in diesem Newsletter.

Auch der Bundesgerichtshof hat kürzlich zu den Sicherungsmaßnahmen eines WLAN-Routers entschieden und für Rechtssicherheit gesorgt. Nach Auffassung des Bundesgerichtshofs haftet ein Internetanschlussinhaber nicht als Störer einer Rechtsverletzung, wenn das WLAN mit einem vom Hersteller werksseitigen vergebenen ausreichend langen individuellen Kennwort gesichert war. Durch das Urteil werden die Rechte der privaten Anschlussinhaber gestärkt und die Störerhaftung weiter eingeschränkt. Einen ausführlichen Bericht zur Sicherheit eines WLAN-Anschlusses befindet sich in diesem Newsletter.

Am 27. und 28. April 2017 findet das 12. Internationale For..Net Symposium mit dem Titel »IT-Fitness: Kompetenz. Haftung. Versicherung« in Passau statt, zu dem ich Sie bereits jetzt herzlich einladen möchte. Die Veranstaltung steht auch dieses Jahr erneut unter der Schirmherrschaft von Frau Dorothee Bär, Parlamentarische Staatssekretärin im Bundesministerium für Verkehr und Digitale Infrastruktur. Neben der Verleihung des 4. For..Net-Awards für besonders datenschutzkonforme IT-Innovationen wird auch der 1. *BaywiDI*-Kongress stattfinden, bei dem der Projektbeirat und ein konturiertes Leistungspaket für die Zukunft vorgestellt werden.

Leider hat das neue Jahr mit dem Tod des ehemaligen Bundespräsidenten Roman Herzog, der auch lange Schirmherr des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI) (https://www.divsi.de/) war, einen großen Schatten geworfen. Er hinterlässt eine große Lücke. Mein Beileid gilt seiner Familie und seinen Angehörigen.

Ich wünsche Ihnen eine unterhaltsame Lektüre bei dem Auszug an aktuellen spannenden Fragen rund um die IT-Sicherheit in unserem dritten Newsletter.

Prof. Dr. Dirk Heckmann,
Leiter des Forschungsprojekts »BayWiDI«

Inhalt

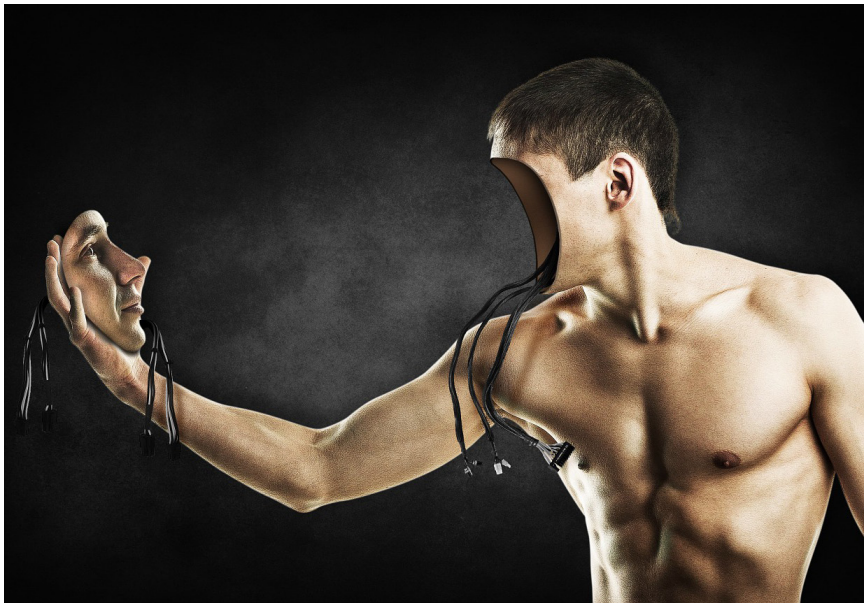
#ForNet17 - IT-Fitness: Kompetenz. Haftung. Versicherung

Was ist For..Net?

Die „Forschungsstelle für IT-Recht und Netzpolitik“ – kurz For..Net – ist eine unabhängige Forschungs- und Beratungseinrichtung der Universität Passau unter der Leitung von Herrn Prof. Dr. Dirk Heckmann. Das Forschungs- und Beratungsprofil der Forschungsstelle prägt eine Kombination von Rechtsdogmatik und Rechtspolitik. Erklärtes ganzheitliches Ziel der Forschungsstelle ist die Begleitung der mit einer rasanten technologischen Entwicklung einhergehenden notwendigen Modernisierung von Staat und Wirtschaft. Angesichts der kaum beherrschbaren Komplexität von IuK-Technologie in globalen Zusammenhängen bedarf es insoweit vor allem Rechtssicherheit. Erreicht werden soll dieses Ziel u.a. durch Expertisen, Auftragsforschung, betreute Dissertationen, Veranstaltungen sowie interaktive Plattformen im Internet. Vermittelt wird eine praxisgerechte rechtliche Beratung für Behörden und Unternehmen. Zukunftsorientierung, Interdisziplinarität, Internationalität, Kunden- und Serviceorientierung sowie Praxis- und Unternehmensbezug kennzeichnen dabei die Arbeitsweise von For..Net.

Was ist das jährliche Internationale For..Net-Symposium?

Das Internationale For..Net Symposium ist eine hochkarätige zweitägige Fachveranstaltung für IT-Rechtsexperten aus Wissenschaft, Wirtschaft und Praxis in den Passauer Redoutensälen, die von einem besonderen kulturellen Abendprogramm umrahmt wird. Die Schirmherrschaft übernimmt Frau Dorothee Bär, Parlamentarische Staatssekretärin im Bundesministerium für Verkehr und Digitale Infrastruktur. Das For..Net-Symposium sieht sich als Plattform und Impulsgeber für eine



wertorientierte Internetnutzung und möchte einen Beitrag zur diesbezüglichen rechtsdogmatischen und rechtspolitischen Auseinandersetzung leisten.

Die diesjährige 12. Veranstaltung findet am 27. und 28. April 2017 statt und wird sich dem Thema „IT-Fitness“ widmen. Unter diesem Generalthema geht es um verschiedene Einzelaspekte, die sich jeweils der Frage zuwenden, ob Staat, Wirtschaft und Gesellschaft insbesondere der Bürger „fit“ sind für die IT-Nutzung. „Fit“ bedeutet in diesem Kontext in der Lage zu sein, rechtskonform und interessengerecht zu agieren. Freuen Sie sich auch auf einen besonderen Auftritt von Max Schrems. Wie bereits bei den zurückliegenden Veranstaltungen der vergangenen Jahre gibt es auch dieses Jahr wieder einen interessanten Veranstaltungsbestandteil. Wir werden das Thema „IT-Fitness“ nicht nur aus der Perspektive fit für IT, sondern auch fit trotz IT betrachten. Hierfür dürfen wir SHENTISPORTS®, einen der größten deutschen Anbieter für Personal Training und Firmenfitness, in unserer Universitätsstadt Passau begrüßen. Lassen Sie sich überraschen. Während des traditionellen Galaabends auf der Veste Oberhaus wird bereits zum 4. Mal der For..Net-Award, ein Preis für datenschutzkonforme IT-Innovationen, verliehen.

Die Veranstaltung ist kostenfrei, aber anmeldepflichtig. Online Anmeldungen über:

https://www.for-net.info/symposien/symposium-2017/anmeldung/

Last but not least wird auch der 1. *BayWiDI*-Kongress stattfinden, bei dem der Projektbeirat und ein konturiertes Leistungspaket für die Zukunft vorgestellt werden.

Weiterführende Informationen zum Tagungsprogramm sowie zur Anmeldung entnehmen Sie folgender Webseite:

https://www.for-net.info/symposien/symposium-2017/

Neues aus Luxemburg zur Vorratsdatenspeicherung

Das Bundesverfassungsgericht hat im Jahr 2010 die Vorratsdatenspeicherung in ihrer damaligen Form, für verfassungswidrig erklärt (BVerfG, Urt. v. 02.03.2010 - 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08). Der deutsche Gesetzgeber hat daraufhin Ende des Jahres 2015 mit dem Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (BGBl. I 2015, S. 2218) einen Neustart zur Umsetzung der umstrittenen Datenspeicherung gewagt.

Die neu eingefügten §§ 113a ff. TKG sehen jetzt eine verpflichtende zehnwöchige Speicherung von Verbindungsdaten zu Telefongesprächen sowie IP-Adressen (§ 113b Abs. 1 Nr. 1, Abs. 2, 3 TKG) und die vierwöchige Speicherung von Standortdaten bei der Nutzung mobiler Telefondienste (§ 113b Abs. 1 Nr. 2, Abs. 4 TKG) durch die Telekommunikationsunternehmen vor. Der Inhalt der Kommunikation darf hingegen nicht gespeichert werden (vgl. § 113b Abs. 5 TKG).

Durch die neueste Rechtsprechung des Europäischen Gerichtshofs werden die vorgenannten Regelungen erneut auf den Prüfstand gestellt. So wurde kurz vor Ende des letzten Jahres die anlasslose flächendeckende Überwachung aller Bürgerinnen und Bürger für unzulässig erklärt (EuGH, Urt. v. 21.12.2016 - C-203/15, C-698/15). Auf das Vorabentscheidungsersuchen eines schwedischen und eines britischen Gerichts hat der Europäische Gerichtshof klargestellt, dass das Unionsrecht eine „allgemeine und unterschiedslose“ Speicherung von Verkehrs- und Standortdaten auf Vorrat nicht zulasse. Aus der Gesamtheit der gespeicherten Daten ließen sich sehr genaue Schlüsse auf das Privatleben der erfassten Personen ziehen. Der mit der Speicherung dieser Daten einhergehende Grundrechtseingriff sei deshalb als besonders schwerwiegend einzustufen. Ausnahmen hiervon seien nur zur Bekämpfung schwerer Straftaten möglich. Eine solche gezielte Vorratsspeicherung müsse jedoch »hinsichtlich der Kategorien von zu speichernden Daten, der erfassten Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Speicherungsdauer auf das absolut Notwendige beschränkt« werden. Die nationalen Regelungen müssten hierzu klar und präzise formuliert sein und hinreichende Garantien enthalten, um Missbrauchsrisiken vorzubeugen.

Es bleibt abzuwarten, welchen Einfluss die Entscheidung auf die nationalen Vorschriften der §§ 113a ff. TKG hat. Bereits jetzt sind Widersprüche erkennbar. Der Europäische Gerichtshof knüpft bereits strengere Voraussetzungen an die Speicherung der Daten durch den Telekommunikationsanbieter als an die Verwendung bislang anlasslos und flächendeckend erhobener Daten durch die Sicherheits- und Strafverfolgungsbehörden. Interessant wird in diesem Zusammenhang auch sein, wie sich die Ausführungen des EuGH auf die Entscheidung des BVerfG über die noch anhängigen Verfassungsbeschwerden gegen die deutsche Regelung zur Vorratsdatenspeicherung auswirken werden.

Die Umsetzung der Vorratsdatenspeicherung stellt auch in IT-sicherheitsrechtlicher Hinsicht eine Herausforderung dar. Die Bundesnetzagentur hat Ende des vorherigen Jahres den Anforderungskatalog nach § 113f TKG veröffentlicht. In ihm werden die technischen Vorkehrungen und sonstigen Maßnahmen zur Gewährleistung der Datensicherheit und Datenqualität bei der Vorratsspeicherung normiert. Der Verband der Internetwirtschaft e.V. hat den Katalog scharf kritisiert (https://www.eco.de/wp-content/blogs.dir/20160621_stn_vds-anforderungskatalog.pdf). Es würden zu hohe Anforderungen an die IT-Sicherheit gestellt. „Eine entsprechende Umsetzung sei denkbar und erfüllbar, aber heute in den Systemen der Betreiber keinesfalls technischer Stand der Dinge. Derartige Systeme müssten vollkommen neu designt und aufgesetzt werden, denn aktuell gibt es kein System, das diese Anforderungen erfüllt“ sagt Klaus Landefeld, Eco-Vorstand Infrastruktur & Netze.

Die vorstehenden Ausführungen zeigen, wie verzahnt die Vorratsdatenspeicherung und die IT-Sicherheit sind. Den Auswirkungen auf nationaler Ebene darf mit Spannung entgegengeblickt werden.

Vertiefung:

- Bundesnetzagentur, Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten,

https://www.bundesnetzagentur.de/cln_1432/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/VDS_113aTKG/VDS-node.html

- Verband der Internetwirtschaft e.V., Stellungnahme zum Anforderungskatalog nach § 113 f TKG der Bundesagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen,

https://www.eco.de/wp-content/blogs.dir/20160621_stn_vds-anforderungskatalog.pdf

- Mittelstandskiller Vorratsdatenspeicherung, Eco kritisiert Anforderungskatalog der Bundesnetzagentur,

https://www.itsicherheit-online.com/news/mittelstandskiller-vorratsdatenspeicherung

IT-Sicherheit bei WLAN Routern ab Werk

Nach einem Grundsatzurteil des Bundesgerichtshofs zur Störerhaftung aus dem Jahr 2010, haftet der Internetanschlussinhaber für Rechtsverletzungen Dritter als Störer auf Unterlassung, wenn er es unterlässt die im Kaufzeitpunkt des WLAN-Routers marktüblichen Sicherungen anzuwenden. Diese bestehen regelmäßig aus der Wahl eines angemessenen Verschlüsselungsstandards sowie der Festlegung eines sicheren Passworts. In der angesprochenen Entscheidung hatte es der Beklagte nach Anschluss des WLAN-Routers bei den werksseitigen Standardeinstellungen des Herstellers belassen und kein ausreichend langes persönliches Passwort vergeben. Der BGH postulierte wie folgt:

„Der Schutz von Computern, Kundenkonten im Internet und Netzwerken durch individuelle Passwörter gehörte auch Mitte 2006 bereits zum Mindeststandard privater Computernutzung und lag schon im vitalen Eigeninteresse aller berechtigten Nutzer. Sie war auch mit keinen Mehrkosten verbunden."

Ob diese Grundsätze nun auch für den Fall gelten, wenn der Hersteller des Routers von Werk aus bereits ein individuelles, ausreichend langes und sicheres Passwort vergibt, hat die Gerichte in den letzten Jahren beschäftigt. Hierbei muss beachtet werden, dass ein Kennwort, das nur dem Internetanschlussinhaber bekannt ist, mindestens genauso sicher ist wie ein selbst gewähltes. In vielen Fällen ist dieses individuelle werksseitige Passwort des Herstellers sogar sicherer als die eigenen Passwörter von Privatnutzern (so auch bereits Koch, jurisPR-ITR 1/2014 Anm. 4; Mantz, MMR 2013, 607).

Diese Auffassung hat letztlich der Bundesgerichtshof im November 2016 bestätigt (BGH, Urt. v. 24.11.2016 - I ZR 220/15). Der WLAN-Router war im zu entscheidenden Fall mit einem vom Hersteller vergebenen auf der Rückseite aufgedruckten WPA2-Schlüssel gesichert, der aus 16 Ziffern bestand. Dies hatte der Bundesgerichtshof als ausreichende Sicherung erachtet, wenn es sich um ein für jedes Gerät individuell vergebenes Passwort handelt, das nicht für eine Mehrzahl von Geräten vom Hersteller vergeben wird. Auch der Standard WPA2 ist aus Fachkreisen als hinreichend sicher anerkannt. Dafür, dass ein 16-stelliger Zifferncode nicht den marktüblichen Sicherungen entspricht und Dritte die Möglichkeit hätten, ihn zu entschlüsseln, sind keine Anhaltspunkte ersichtlich.

Ob diese Grundsätze auch dann gelten, wenn der Routertyp eine Sicherheitslücke aufweist, die der Öffentlichkeit bekannt ist und ob die Kenntnis des Anschlussinhabers von dieser Sicherheitslücke entscheidend ist, bleibt der Veröffentlichung der Entscheidungsgründe vorbehalten.

Checkliste zur IT-Sicherheit bei werksseitig verschlüsselten Routern:

- **Handelt es sich um ein individuelles und nicht um ein standarisiertes Kennwort ab Werk?**
- **Ist der Sicherheitsstandard des WLAN angemessen? (WEP = unsicher) (WPA2 = sicher)**
- **Ist das Passwort des Herstellers ausreichend lang und sicher?**

Ransomware – unterschätzte IT-Sicherheitsgefahr?

Mit Ransomware sind Erpressungstrojaner oder Verschlüsselungstrojaner gemeint, mit deren Hilfe die Angreifer den Zugriff oder die Nutzung auf Daten unmöglich machen. Obwohl der Begriff vielen bekannt ist, ist die Praxis für diese Art von IT-Sicherheitsrisiken noch nicht genug sensibilisiert. So gingen zwischen dem 1. Dezember 2015 und dem 29. Februar 2016 bei den Landeskriminalämtern 156 Anzeigen ein. Dabei stammten alleine 113 Anzeigen von Firmen und Einrichtungen wie beispielsweise mehrere Kliniken und das Ministerium für Inneres und Kommunales des Landes Nordrhein-Westfalen.

Dabei existiert Ransomware bereits seit fast 30 Jahren. Ursprünglich wurde es noch auf Disketten verbreitet, heute wird es mittels E-Mail-Anhängen, der Ausnutzung von Sicherheitslücken in Webbrowsern oder über Datendienste wie Microsofts One Drive oder Apples iCloud in den Computer eingeschleust. Das Programm verschlüsselt die sich auf dem betroffenen Computer befindlichen Daten, um anschließend für die Entschlüsselung der Daten ein Lösegeld zu verlangen. Die Zahlung des Lösegelds bringt jedoch im seltensten Fall die Daten zurück. Allenfalls werden auf diese Weise die Straftäter unterstützt, wenn der Betroffene der Forderung nachkommt. Es sollte daher in jedem Fall von einer Zahlung abgesehen werden.

Am besten lässt sich die Komplexität solcher Schadprogramme an einem aktuellen Fall darstellen.

Der Verschlüsselungstrojaner GoldenEye hat sich im Dezember 2016 innerhalb weniger Stunden in ganz Deutschland verbreitet. Die Angreifer versendeten E-Mails an personalverantwortliche Mitarbeiter in Unternehmen und Organisationen mit Sitz in Deutschland. In deren Anhang befanden sich eine Bewerbung im PDF-Format und eine Excel-Datei. Die Bewerbungen bezogen sich alle auf tatsächliche Stellenausschreibungen, waren korrekt adressiert und in fehlerfreiem Deutsch verfasst. Die Excel-Datei war mit dem Logo der Bundesagentur für Arbeit (BA) versehen und forderte den Verwender zur Aktivierung von Makros auf, um so Daten über den Bewerber vom Server der BA herunterladen zu können. Die E-Mail kam dem ungeschulten Auge so authentisch vor, dass eine Vielzahl von Mitarbeitern die Makrofunktion aktivierten. Dann verschlüsselte Golden-Eye zunächst die Dateien und machte sich anschließend an die Boot-Prozesse. Darauf folgte ein Bluescreen, gefolgt von einem erzwungenen Neustart durch die Schadsoftware. Diese verschlüsselte die auf dem betroffenen Computer befindlichen Daten, was ein Öffnen der Dateien unmöglich machte. Währenddessen erschien eine gefälschte Mitteilung über eine Systemreparatur, in der darauf hingewiesen wurde, den Vorgang nicht abzubrechen, da andernfalls irreparable Schäden entstehen könnten. In der Datei your_files_are_encrypted.txt wurden die Opfer angewiesen auf das Tor-Netzwerk zuzugreifen und die Bezahlung des Lösegelds vorzunehmen (etwa 950€).

Goldeneye ist nur eine Variante von vielen Schadprogrammen, die ein System befallen können. Es gibt verschiedene Wege für Angreifer Zugang zu Ihren Daten zu erlangen, wobei die Verschlüsselungen stets komplexer werden und die Entschlüsselung durch ein Antivirusprogramm erschweren. Schadprogramme ohne Verschlüsselung können durch handelsübliche Antivirusprogramme entfernt werden, ohne finanzielle Schäden zu hinterlassen. Teilweise gelingt es Sicherheitsforschern die Ransomware zu knacken und die Daten zu entschlüsseln. Dies ist jedoch nur selten der Fall und nimmt einige Zeit in Anspruch.

IT-Sicherheits-Basics zur Vermeidung von Ransomware:

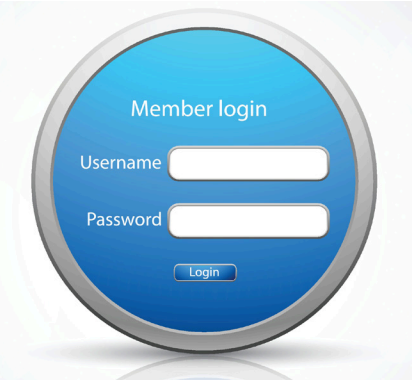
- **Regelmäßige Durchführung von Backups**
- **Bei fragwürdigen E-Mail-Anhängen o.ä. einen fachkundigen Dritten hinzuziehen**
- **Kein Einlassen auf Erpressungsforderungen**
- **Antivirusprogramme verwenden und aktuell halten**
- **Betriebssystem aktuell halten**
- **Vermeidung der Anmeldung und Arbeit mit Administrator-Rechten**
- **Individuelle Webbrowsereinstellungen vornehmen: JavaScript stoppen; Werbeblocker verwenden etc.**
- **Entwicklung von verhaltensanalysierten Scannern beobachten und bei Fortschritten in der Entwicklung selbst testen**

In Vorbereitung: BayWiDI Intern

Wie bereits im Vorwort erwähnt, befindet sich das *BayWiDI*-Projekt derzeit in Konzeptionierungsphase zur Umsetzung eines interne Bereichs (*BayWiDI* Intern). Dieser wird exklusiv für Premiumpartner zugänglich sein. Im *BayWiDI* Intern werden hilfreiche allgemeine Informationen wie etwa ein umfassendes Lexikon zur IT-Sicherheit oder Erläuterungen zu allgemeinen Haftungsmaßstäben und -grundlagen zu finden sein. Daneben werden den Premiumpartnern über die internen Seiten die nach individuellem Auftrag für sie erstellten Forschungsergebnisse wie beispielsweise rechtswissenschaftliche Fachgutachten zum Abruf bereitgestellt.

Zusätzlich erwartet die Premiumpartner ein ganz besonderer Mehrwert: eine laufend aktualisierte Datenbank zu Entscheidungen rund um Fragen des IT-Sicherheitsrechts, welche – unter besonderer Berücksichtigung der Handhabbarkeit im unternehmerischen Kontext – in strukturierten Datensätzen aufbereitet und mit einem spezifischen Abrufsystem verknüpft sein werden. Hinzu kommt das Kernstück der Idee, der SecurityLawScout. Dieser soll als dogmatische Pionierleistung die gesammelten Entscheidungen rund um IT-Sicherheitsrechtsfragen mit einer speziellen Rechtsentwicklungsprognose versehen. Dies ermöglicht den beteiligten Unternehmen, über die Erfüllung der von der Rechtsprechung aufgestellten Grundsätze und konkretisierten Anforderungen hinaus aus ebendiesen Entscheidungen die relevanten Trends zu erfahren, welche sich in naher Zukunft auf etwaige neue Haftungsfälle auswirken werden. Diese Projektidee trägt den Namen eLIAS (electronic law information agency for security).

Nach Abschluss der technischen Umsetzung wird der Zugang zum internen Bereich von BayWiDI voraussichtlich Ende April 2017 auf dem 1. *BayWiDI*-Kongress vorgestellt. Über den Start des SecurityLawScout werden Sie noch gesondert informiert.



Der nächste Newsletter erscheint am 15. April 2017.

Sie finden den Newsletter und die Möglichkeit, sich an-, bzw. abzumelden auch unter https://www.baywidi.de/

Hinweise, Anregungen, Lob und Kritik sind herzlich Willkommen. Schreiben Sie einfach an baywidi@uni-passau.de

Impressum

Universität Passau
Innstraße 41
94032 Passau
Telefon: 0851/509-0
Telefax: 0851/509-1005
E-Mail: praesidentin@uni-passau.de
Internet: www.uni-passau.de
USt-Id-Nr.: DE 811193057

Organisation
Gemäß Art. 4 Abs. 1 BayHSchG ist die Universität Passau als Hochschule des Freistaates Bayern eine Körperschaft des öffentlichen Rechts und zugleich staatliche Einrichtung. Aufsichtsbehörde ist das Bayerische Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst in München (Anschrift: Salvatorstraße 2, 80333 München).

Vertretung:
Die Universität Passau wird von der Vorsitzenden des Leitungsgremiums, Präsidentin Prof. Dr. Carola Jungwirth, gesetzlich vertreten. Verantwortliche im Sinne des § 5 TMG (Telemediengesetz) ist die Präsidentin. Für namentlich oder mit einem gesonderten Impressum gekennzeichnete Beiträge liegt die Verantwortung bei den jeweiligen Autorinnen und Autoren.