Editorial - Begrüßung durch den Leiter des Forschungsprojekts »BayWiDI« Prof. Dr. Dirk Heckmann

Sehr geehrte Leserinnen und Leser,

seit dem ersten *BayWiDI*-Newsletter im vergangenen Juli sind drei Monate vergangen, in denen das Projekt *BayWiDI* (Bayerisches Wissensnetzwerk Digitale Infrastrukturen und Recht für Unternehmen) entscheidend an Fahrt aufgenommen hat. Nicht nur das *BayWiKI* (https://www.baywidi.de/wiki) ist weiter ausgebaut und u. a. um die Bereiche der netzpolitischen Positionen sowie der allgemeinen Handlungsempfehlungen erweitert worden. Am 11. Oktober fand auch der erste offizielle *BayWiDI*-Workshop statt, zu dem wir Sie recht herzlich nach Passau eingeladen haben und der sich schwerpunktmäßig mit den *rechtlichen Anforderungen an ein IT-Sicherheitskonzept* auseinandersetzte.

Gleichzeitig war hiermit der erfolgreiche Startschuss eines umfassenden Workshop-Programms verbunden, auf das noch weitere Veranstaltungen in der Zukunft folgen werden. Unter den Teilnehmern befanden sich auch Vertreter von namhaften IT-Unternehmen aus der Wirtschaft wie *Deutsche Post, Synaxon AG, Verlag C.H. BECK* oder *Kanzlei Noerr LLP*. Dem Workshop ging ein Treffen der Partnerunternehmen am 10. Oktober mit einem gemeinsamen Abendessen auf der Veste Oberhaus voraus.

Inhaltlich standen brandaktuelle Themen der IT-Sicherheit wie unter anderem Fragen zu Cyber-Security-Versicherungen,

Inhalt

die Qualifizierung des IT-Sicherheitsbeauftragten, IT-Sicherheitskonzepte oder die neuen Meldepflichten im IT-Sicherheitsgesetz im Fokus der Veranstaltung. Hinsichtlich Inhalt und Eindrücken dieses Workshops möchte ich auf den ausführlichen Tagungsbericht in diesem Newsletter verweisen.

Auch bei offenem/freien WLAN werden Fragen der IT-Sicherheit zukünftig eine größere Bedeutung einnehmen. Denn am 22. Juli 2016 sind die Änderungen zum Telemediengesetz in Kraft getreten. Ziel dieser Gesetzesänderung war die Stärkung des flächendeckenden Ausbaus von WLAN-Internetzugängen in Gesamtdeutschland und die Schaffung von Rechtssicherheit. Die Gesetzesänderung wurde in der Bevölkerung und in den Medien als eine Abschaffung der Störerhaftung aufgefasst. Dabei war jedoch vielmehr der Wunsch Vater des Gedankens. Eine vollständige Haftungsfreistellung eines WLAN-Betreibers bei illegalen Downloads über ein nicht verschlüsseltes WLAN sieht der Gesetzeswortlaut des § 8 TMG nicht vor. Zu dieser Frage hat auch kürzlich der EuGH im Fall Mc Fadden am 15. September 2016 judiziert.

Sollten offene/freie kabellose Internetverbindungen in Deutschland zum neuen Verbindungsstandard werden, ist neben dem Urheberrecht auch die IT-Sicherheit betroffen. Bei ungeschützten WLAN-Access Points ergeben sich eine Vielzahl von Angriff-Szenarien. Gerade für solche Fragestellungen ist das *BayWiDI*-Projekt eine hervorragende Schnittstelle zwischen Wissenschaft und Wirtschaft.

Unser Ziel ist es, aktuelle und zukünftige Fragen der IT-Sicherheit in einem Diskurs aufzuwerfen und der Wirtschaft eine sichere Hilfestellung auf dem Weg zu einer verlässlichen Informationsinfrastruktur zu geben. Nur wenn wir schon heute die IT-sicherheitsrechtlichen Fragestellungen von morgen erkennen, können wir die Vision von Deutschland als sicherstem IT-Standort realisieren.

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

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

IT Sicherheit bei unsicheren drahtlosen Netzwerken

Sollten offene WLAN in Deutschland Standard werden, betrifft IT-Sicherheit schon morgen jeden einzelnen Bürger. Denn unverschlüsselte Drahtlosnetzwerke sind einem erhöhten IT-Sicherheitsrisiko ausgesetzt. Ein flächendeckender Ausbau von WLAN-Internetzugängen im öffentlichen Raum trägt dem Bedürfnis der Allgemeinheit bei der immer weiter voranschreitenden Digitalisierung Rechnung. Dennoch sind sich sowohl Nutzer als auch Betreiber solcher Access-Points der drohenden Risiken nicht bewusst.

Beispiele für IT-Sicherheitsrisiken bei offenen WLAN sind:

- Fehlende Authentifizierung bei der Anmeldung: Der Zugriff auf andere Geräte im selben Netzwerk ist ohne besondere IT-Kenntnisse möglich.
- Verbreitung von Schadsoftware.
- »Mitlesen von Datenströmen«: Aufzeichnung von Verbindungsdaten; Zugriff auf Bestands- oder Verkehrsdaten.
- Gefahr der Verwechslung und automatischer Verbindung zu namensähnlichen WLAN.
- Erstellung und Auswertung von Bewegungsprofilen anhand der MAC-Adresse des IT-Geräts.
- Beeinträchtigung der Funkleistung sowie Beeinträchtigung oder Verhinderung des Zugangs zum WLAN.

So kann bspw. der gesamte Datenverkehr ohne große Anstrengungen über einen öffentlichen Internet-Access-Point von einem unbefugten Dritten aufgezeichnet werden. Hierzu muss lediglich ein scheinbar echter öffentlicher Access-Point über eine ähnlich lautende Bezeichnung verfügen (City-WLAN-PA_ an Stelle von City-WLAN-PA). Der Verwender hat hiervon in der Regel keine Kenntnis, da sich insbesondere Smartphones in der Standard Konfiguration automatisch mit einem offenen Access-Point verbinden. Dieses Beispiel ist nur eines von vielen Szenarien, mit denen die IT-Sicherheit bei offenen WLAN in naher Zukunft konfrontiert wird.

Zum Schutz des Fernmeldegeheimnisses und zum Schutz personenbezogener Daten haben WLAN-Anbieter technische Schutzmaßnahmen nach dem Stand der Technik zu treffen (§ 109 TKG). Auf den ersten Blick scheint dies gerade bei offenen WLAN einen scheinbaren Widerspruch zwischen Gesetzeszweck und der technischen Ausgestaltung hervorzurufen. Richtigerweise muss sich die technische Schutzmaßnahme jedoch an der Besonderheit der jeweiligen Technik orientieren.

Im Hinblick auf die konkreten technischen Schutzmaßnahmen besteht Forschungsbedarf. Sicher ist, dass die bekannten Verschlüsselungsstandards mittels Passwort (WEP, WPA, WPA2) erkennbar ausscheiden, weil sie dem Grundgedanken eines offenen Netzwerks zuwider laufen. Das Problem soll mit der neuen Technik OWE gelöst werden, die auf einem automatischen Passwortaustausch beim Aufbau mit dem Drahtlosnetzwerk basiert.

(http://www.heise.de/netze/meldung/IEEE-diskutiert-sicheres-WLAN-ohne-Schluesseleingabe-3082881.html)

Neben der bestmöglichen technischen Absicherung ist die Aufklärung der Nutzer eine weitere wichtige Aufgabe. Hierzu können bereits die folgenden Maßnahmen zu einem sicheren Surfen in einem offenen WLAN beitragen:

- Nutzung von SSL-Verbindungen beim Surfen („https“).
- Deaktivierung der automatischen WLAN-Verbindung in den Herstellerkonfigurationen.
- Löschung aller gespeicherten unsicheren WLAN-Verbindungen.
- Nutzung von VPN-Verschlüsselungen, soweit möglich.
- Deaktivierung der Datei- und Verzeichnisfreigabe.
- Nutzung von Virenprogrammen, soweit möglich.
- keine Eingabe sensibler Daten (Passwörter, Kontodaten etc.).

Ein effektiver Schutz kann nur gemeinsam durch Betreiber und Nutzer gewährleistet werden.

IT Sicherheit und Verantwortung

Für die IT-Sicherheit innerhalb einer Institution ist der IT-Sicherheitbeauftragte (ITSB) zuständig. Obwohl man davon ausgehen darf, dass die Stellung und Funktion des IT-Sicherheitsbeauftragten im Informationszeitalter neben der des Datenschutzbeauftragten eine zentrale Rolle einnimmt, gibt es bislang keine allgemeinen gesetzlichen Vorgaben hinsichtlich der Einrichtung und Ausgestaltung dieser Position. Dabei sind Schäden durch IT-sicherheitsrechtliche Gefahren mit erheblichen Haftungsrisiken für die Unternehmensleitung verbunden. Daher gehört es im Rahmen der »üblichen Sorgfaltsanforderungen« der Unternehmensleitung auch zu der Pflicht, einen IT-Sicherheitsbeauftragten zu ernennen.

Zu dem Hauptaufgabenbereich des IT-Sicherheitsbeauftragten gehört es, für die Einhaltung der Informationssicherheit des Unternehmens beratend und bei der Umsetzung unterstützend tätig zu werden. Die Aufgaben des IT-Sicherheitsbeauftragten lassen sich wie folgt abbilden:

- Steuerung des Informationssicherheitsprozesses.
- Unterstützung der Leitungsebene bei der Erstellung einer Leitlinie zur Informationssicherheit.
- Erstellung eines Sicherheits- und Notfallvorsorgekonzepts
- Koordination von anderen Teilkonzepten und System-Sicherheitsrichtlinien.
- Initiierung und Überprüfung der Realisierung von Sicherheitsmaßnahmen.
- Berichte über den Status quo der Informationssicherheit des Unternehmens.
- Koordination von sicherheitsrelevanten Projekten.
- Untersuchung von Sicherheitsvorfällen.
- Initiierung von Sensibilisierungs- und Schulungsmaßnahmen der Beschäftigten.

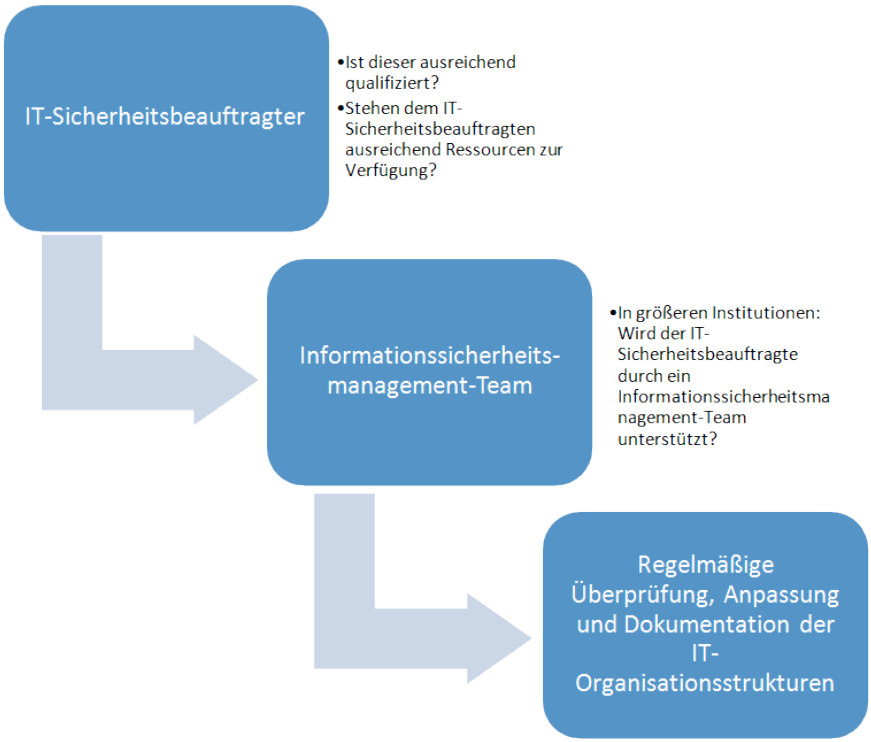
Zur umfassenden Realisierung der vorbezeichneten Maßnahmen empfiehlt sich der Aufbau eines Informationssicherheitsmanagement-Teams, das den IT-Sicherheitsbeauftragten unterstützt und Vorgaben und Richtlinien erarbeitet.

IT-Organisationsstrukturen sind keinesfalls statisch. Sie haben sich vielmehr an den ständigen Änderungen und dem Fortschritt der Informationstechnologie auszurichten. Folgende Punkte sind hierbei als wichtig hervorzuheben:

- **Verantwortungsüberwachung:** Ständige Überprüfung von Verantwortlichkeiten und Zuständigkeiten.
- **Vorgabenüberprüfung:** Anwendung und Durchführung der Prozesse und Abläufe innerhalb der Sicherheitsorganisation; Einhaltung der Organisationsstrukturen für die IT-Sicherheit.
- **Effizienzbeurteilung von Prozessen und organisatorischen Regelungen:** Einhaltung des Sicherheitsmanagements im Hinblick auf Praxistauglichkeit und Effizienz. Zu komplizierte Prozesse oder Regelungen sind zu vermeiden!
- **Regelmäßige Information des Managements:** Neben der Lösung von zeitkritischen Problemen dient die Information der Steuerung des Sicherheitsprozesses durch die Leitungsebene.

Zusammenfassend zum Thema der Verantwortlichkeit im Bereich der IT-Sicherheit dienen das folgende Schaubild bzw. die vertiefenden Hinweise:

https://www.baywidi.de/wiki/organisatorische-grundlagen/organisatorische-grundlagen-zur-it-sicherheit/verantwortlicher-fuer-den-bereich-it-sicherheit/ .



Handlungsempfehlungen zur IT-Sicherheit für Unternehmen

Zur Einhaltung der IT-Sicherheit müssen Unternehmen konkrete Handlungsempfehlungen aufgezeigt werden. Die erforderlichen Maßnahmen richten sich dabei nach der Größe des Unternehmens und der Qualität der dort verarbeiteten Daten. In Deutschland richten sich die IT-Sicherheitsstandards zum einen nach den Vorgaben des Bundesministeriums für Sicherheit (BSI) im IT-Grundschutzkatalog sowie nach der ISO/IEC 27001. Letztere definiert auf knapp 30 Seiten die Anforderungen an ein Informationssicherheitsmanagementsystem (ISMS).

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

Da gerade die Standards des IT-Grundschutzkatalogs sehr ausführlich sind, gibt es zusätzlich kostenpflichtige Sicherheitskonzepte wie der bayerische IT-Sicherheitscluster ISIS 12 oder die VdS Cyber-Richtlinien 3473, die zwar weniger komplex sind, aber auch oftmals ein niedrigeres Schutzniveau gewährleisten. Die folgenden Empfehlungen dienen lediglich der Orientierung und erheben keinen Anspruch auf Vollständigkeit. Hierbei empfiehlt sich eine Aufteilung in **Organisation** und **Technik**.

https://www.it-sicherheit-bayern.de/produkte-dienstleistungen/isis12.html; https://vds.de/

Organisation

- **Schulung und Sensibilisierung der Beschäftigten mit typischen IT-Gefährdungslagen**
- **Turnusmäßige Fortbildungsmaßnahmen sowie unternehmensbezogene Workshops (IT-JOUR FIXE)**
- **Erstellung und Einweisung der Beschäftigten in IT-Sicherheitsrichtlinien**
- **Schutz der IT-Systeme vor unberechtigter Nutzung Dritter (Sichere Passwörter; Automatische Sperren; Physische Zugangssperren)**
- **Verbot der Nutzung privater Endgeräte und Speichermedien sowie Verbot privater Internetnutzung auf dienstlichen Endgeräten**
- **Melde- und Dokumentationspflichten bei IT-Sicherheitsvorfällen**
- **Erstellung eines IT-Notfallkonzepts**
- **Erstellung eines Zutrittsrechtemanagements für die Serverinfrastruktur**

Zur Vertiefung wird auf die Ausführungen im BayWiKI verwiesen:

https://www.baywidi.de/wiki/allgemeine-handlungsempfehlungen-zur-it-sicherheit/

Technik

- **Verschlüsselungsstandards für stationäre und mobile Endgeräte**
- **Betriebssystem der IT-Systeme hat dem aktuellen Stand der Technik zu entsprechen**
- **Sicherung des Unternehmensnetzwerks vor unautorisierten Zugriffen durch Firewalls**
- **Einsatz elektronischer Signaturen und Verschlüsselungsverfahren zur Gewährleistung einer sicheren elektronischen Kommunikation**
- **Verhinderung von Datenverlust durch regelmäßige Backups**
- **Verhinderung von Infizierung mit schadhaftem Programmcode durch Softwarelösungen, Spamfilter, PlugIns und Add-Ons**

So zahlreich die Arten von potentiellen Sicherheitsrisiken für die IT-Infrastruktur eines Unternehmens sind, so zahlreich sind gleichermaßen die zu beachtenden IT-Sicherheitsstandards. Hieraus wird bereits ersichtlich, dass eine nahezu vollständige Abbildung, die auf jedes IT-Sicherheitsrisiko reagieren kann, kaum möglich ist. Die Verzahnung von organisatorischen und technischen Maßnahmen ist dabei ein entscheidendes Kriterium für eine sichere IT-Infrastruktur.

Insoweit kommt der Schulung und Sensibilisierung der Beschäftigten mit IT-Sicherheitsszenarien eine besondere Bedeutung zu. Sowohl der Standard ISO/IEC 27001 als auch der BSI Grundschutz bieten eine gute Grundlage für die IT-Sicherheit im Unternehmen. Nachteile des ISO/IEC 27001 Standards sind die hohen Kosten beim Aufbau der Organisation und der aufwändige Zertifizierungsprozess. Der IT-Grundschutzkatalog des BSI ist hingegen gerade für KMU oftmals zu umfangreich und überfordert viele IT-Verantwortliche, die das IT-Management nur als Nebenaufgabe wahrnehmen.

Tagungsbericht des 1. BayWiDI Workshops

Am 11. Oktober fand in Passau der 1. offizielle BayWiDI Workshop zu aktuellen Fragen der IT-Sicherheit und zum IT-Sicherheitsrecht statt. Dieser stellte auch gleichzeitig den Auftakt für ein zukünftiges umfassendes Tagungsprogramm im Rahmen des BayWiDI-Projekts dar.

Dem Workshop ging am 10. Oktober ein Strategietreffen mit den Premiumpartnern voraus. Diese wurden vertreten durch Herrn Dr. Thomas Thalhofer (Kanzlei Noerr LLP), Herrn Uwe Molzahn (Synaxon AG), Frau Anke Zimmer-Helfrich (Verlag C.H. BECK) und Herrn Dr. Goettrik Wewer (Deutsche Post AG).

Prof. Dr. Dirk Heckmann mit den Premiumpartnern.

Nach einer Begrüßung durch den Projektleiter Prof. Heckmann und einer anschließenden Vorstellungsrunde der Teilnehmer wurden die Säulen des Projekts durch den Projektleiter erläutert und Möglichkeiten zur Gestaltung der Kooperation und Ziele von BayWiDI aufgezeigt. In Zukunft soll ein Projektbeirat gegründet werden, der sich u.a. aus den Premiumpartnern zusammensetzt. Im Rahmen des 12. For..Net-Symposiums am 27. April 2017 wird der 1. BayWiDI-Kongress stattfinden, bei dem der Projektbeirat und ein konturiertes Leistungspaket vorgestellt werden. Den Abschluss dieses Tages bildete ein gemeinsames Abendessen mit den Premiumpartern auf der Veste-Oberhaus mit einem einzigartigen Panoramablick über die Universitätsstadt Passau.

Der eigentliche Workshop wurde am nächsten Tag mit einer Vorstellung des Projekts von Prof. Heckmann und einem anschließenden Vortrag seines wissenschaftlichen Mitarbeiters Alexander Schmid eröffnet, der den Mangel an frei zugänglichen Informationen zum IT-Sicherheitsrecht aufzeigte und die bisherigen Projektarbeiten an der BayWiDI-Webseite sowie den Fortschritt des BayWiKIs erläuterte. Im Anschluss daran folgte ein Vortrag des Projektleiters zu den rechtlichen Anforderungen an IT-Sicherheitskonzepte. Neben möglichen Haftungsrisiken und Folgen bei IT-Unsicherheit durch fahrlässiges Verhalten wurden die gesetzlichen Quellen der IT-Sicherheit anhand konkreter Anwendungsszenarien wie bspw. autonomer Systeme vorgestellt. Bei den einzuhaltenden rechtlichen Vorgaben nahm die nationale Vorschrift des § 13 Abs. 7 TMG neben der DS-GVO, NIS-RL bzw. dem IT-Grundschutz-Katalog des BSI eine zentrale Schlüsselrolle ein. Hierbei hatten die Teilnehmer in einem offenen Diskurs die Gelegenheit, eigene Fragen in Bezug zu IT-Sicherheitskonzepten zu stellen. Abschließend gab der Leiter des Projekts auch eine rechtspolitische Perspektive zur IT-Sicherheit anhand der steigenden Bedeutung von Qualitätskontrollen bei IT-Sicherheitsszenarien. Die Präsentationen der Vorträge sind öffentlich abrufbar unter:

https://www.baywidi.de/workshop-oktober-2016/

Nach einem gemeinsamen Mittagessen mit anschließender Kaffeepause, bei dem die Teilnehmer die Möglichkeit zum gemeinsamen Austausch hatten, beantwortete der Projektleiter im zweiten Teil des Workshops spezielle Fragen zu aktuellen IT-Sicherheitsthemen. Hierzu zählten u.a. die Abschaffung der Störerhaftung, die private Nutzung des geschäftlichen E-Mail Accounts oder die Datensparsamkeit anhand von Data Loss Prevention. Der erste BayWiDI Workshop endete mit einer gemeinsamen Abschlussdiskussion und einem Feedback der Teilnehmer, wobei die Synergien zwischen Wissenschaft und Praxis besonders herausgestellt wurden. Um den Fokus für zukünftige Projektarbeit auf dem weiten Feld der IT-Sicherheit zu bündeln, wurde abschließend eine Priorisierung nach drei Phasen vorgenommen. Auf dem 12. For..Net Symposium, das am 27. April 2017 in Passau unter dem Leitthema »IT-Fitness« stattfinden wird, sollen die weiteren Arbeitsergebnisse wie u.a. die Profilbildung von BayWiDI präsentiert werden.

Programm - 11. Oktober 2016

- 09.30 Uhr - Registrierung der Teilnehmerinnen und Teilnehmer
- 10.00 Uhr - Begrüßung und organisatorische Hinweise
- 10.25 Uhr - Vorstellung von BayWiDI
- 11.00 Uhr - Rechtliche Anforderungen an ein IT-Sicherheitskonzept unter besonderer Berücksichtigung des IT-Sicherheitsgesetzes
- 12.30 Uhr - Mittagspause
- 13.30 Uhr - Aktuelle Fragen zu IT-Sicherheit und IT-Sicherheitsrecht
- 15.30 Uhr - Organisatorisches und Ausblick
- 16.00 Uhr - Ende des Workshops

Datensparsamkeit und Data Loss Prevention

Zwischen Datenschutz/informationeller Selbstbestimmung und IT-Sicherheit/ Kontrolle besteht ein Spannungsverhältnis. Für die IT-Sicherheit ist das Sammeln von möglichst vielen Informationen wegen einer besseren Kontrolle vorteilhaft. Denn je mehr Informationen einem IT-Sicherheitsbeauftragten zur Verfügung stehen, desto besser kann er IT-Risiken bekämpfen. Dem steht das Recht auf informationelle Selbstbestimmung des Beschäftigten an der Geheimhaltung seiner Informationen sowie der im Datenschutz verankerte Grundsatz der Datensparsamkeit (vgl. § 3a BDSG) gegenüber. Die Unternehmenspraxis trennt die beiden Funktionen daher weitgehend. Auch in der Datenschutz-Grundverordnung ist der Interessenkonflikt in Art. 38 Abs. 6 S. 2 DSGVO ausdrücklich benannt. Danach stellt der Verantwortliche oder der Auftragsverarbeiter sicher, dass derartige [(Anm.: des Datenschutzbeauftragten) Aufgaben und Pflichten] nicht zu einem Interessenkonflikt (Anm. mit anderen Aufgaben und Pflichten, § 38 Abs. 6 S. 1 DSGVO) führen. Dieser Interessenkonflikt lässt sich an sog. *Data Loss Prevention Maßnahmen* (DLP) veranschaulichen.

Das Ziel von *Data Loss Prevention* oder auch *Data Leakage Protection* ist es, sensible Daten im Unternehmen zu identifizieren und einen ungewollten Abfluss und Missbrauch von Unternehmensdaten zu verhindern. Dabei sollen Datenlecks erfolgreich abgedichtet werden, bevor ein IT-Sicherheitsfall eintritt. Um dieses Ziel zu erreichen, wird eine Echtzeitüberwachung von Netzwerken und Endgeräten genutzt. Solche Systeme bemerken, wenn Daten auf einem nicht autorisierten Speicherort abgelegt werden wie z.B. auf einem privaten USB-Stick. Zudem können sie Übertragungen in Netzwerken bei E-Mails oder Uploads beobachten und inhaltlich nach bestimmten Mustern oder Stichworten durchsuchen, um Abweichungen vom üblichen Verhalten festzustellen.

Um den Grundsatz der Datensparsamkeit zu beachten, dürfen also bei weitem nicht alle Funktionen des DLP-Systems genutzt werden, die technisch möglich sind. Eine den Grundsatz der Erforderlichkeit wahrende Lösung könnte beispielsweise sein, das System so zu programmieren, dass es nur bei hinreichenden, tatsächlichen Anzeichen eines Verstoßes aktiv wird. Andernfalls sind die Daten auf der Stelle zu löschen. Ein weiteres Problem tritt auf, wenn das Unternehmen die private Nutzung von IT-Systemen gestattet wie z.B. die private E-Mail-Nutzung. In diesem Fall muss das DLP-System so konfiguriert sein, dass die Privatnutzung technisch nicht von der Überwachung betroffen ist. Dies ist nur mit großen Schwierigkeiten zu realisieren.

Fazit

- **Die Gewährleistung von IT-Sicherheit im Sinne der Verhinderung eines unautorisierten Datenabflusses hat keinen allgemeinen Vorrang vor dem Datenschutz.**
- **Moderne DLP-Systeme sind in der Lage, die IT-Sicherheit zu maximieren.**
- **Sie müssen jedoch den Grundsatz der Datensparsamkeit wahren; insbesondere ist eine Totalüberwachung von Mitarbeitern unzulässig.**
- **Eine datenschutz- und arbeitsrechtskonforme Ausgestaltung von DLP-Maßnahmen ist oft technisch und rechtlich anspruchsvoll.**

Das nächste Magazin erscheint am 15. Januar 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.