Prof. Dr. jur. Hans-Hermann Dirksen
Professor für Medizin- und Gesundheitswirtschaftsrecht, Hochschule Fresenius
LIEBENSTEIN LAW - Kanzlei für Wirtschafts- und Gesundheitsrecht
Aystettstr. 3, 60322 Frankfurt am Main

DIGITALISIERUNG IM FADENKREUZ

Digitalisierung im Fadenkreuz

LIEBENSTEIN LAW
KANZLEI FÜR WIRTSCHAFTS- UND GESUNDHEITSRECHT

Prof. Dr. Hans-Hermann Dirksen
Rechtsanwalt | Hochschullehrer

LIEBENSTEIN LAW
Kanzlei für Wirtschafts- und Gesundheitsrecht
Aystettstr. 3 - Holzhausenviertel
60322 Frankfurt/M.
mail@liebenstein-law.de
www.liebenstein-law.de
+49 69 9592 – 8027

Herr Prof. Dirksen ist im Wirtschafts- und Wettbewerbsrecht, im Gesundheitsrecht sowie im Informationstechnologierecht. Er berät Verbände und Institutionen sowie Software-Anbieter.

Herr Prof. Dirksen lehrt an der Hochschule Fresenius in Frankfurt in den Bereichen IT-Recht, Gesundheit und Management. Prof. Dirksen ist Fachausschussmitglied bei der VDI-Gesellschaft Technologies of Life Sciences, Referent beim Deutschen Krankenhausinstitut, Lehrbeauftragter bei der Carl-Remigius Medical School, Mitglied der Ethikkommission der Hochschule Fresenius, Mitglied der Deutschen Gesellschaft für Telemedizin sowie bei gesundheitswirtschaft rhein-main e.V.

Digitalisierung im Fadenkreuz

LIEBENSTEIN LAW
KANZLEI FÜR WIRTSCHAFTS- UND GESUNDHEITSRECHT

Das Bundeskriminalamt (BKA) hat am 17. August sein aktuelles „Lagebild Cybercrime“ veröffentlicht. Darin werden für das Jahr 2016 insgesamt 82.649 Straftaten (2015: 45.793) mit einem Gesamtschaden von 51,63 Millionen Euro (2015: 40,5 Mio. Euro) sowie eine durchschnittliche Aufklärungsquote von 38,7 Prozent (2015: 32,8%) ausgewiesen.

Den starken Anstieg der Fallzahl führt das BKA darauf zurück, dass inzwischen solche Delikte, die früher als „allgemeiner Betrug“ erfasst worden waren, jetzt wegen der eindeutigen Zuordnungsmöglichkeit als Computerbetrug erfasst werden können.

Das BKA geht weiterhin von einem großen Dunkelfeld aus, das von der Statistik nicht erfasst wird. Dies bedeutet, dass die tatsächlichen Fallzahlen und Schadenssummen deutlich höher sein können.

Digitalisierung im Fadenkreuz

LIEBENSTEIN LAW
KANZLEI FÜR WIRTSCHAFTS- UND GESUNDHEITSRECHT

Hello,

You've stolen 48.48 BTC from the wrong people, please be so kind to return them and we will return your files..

Don't take us for fools, we know more about you than you know about yourself.

Pay us back and we won't take further action, don't pay and be prepared.

3BGrRU4mhAkCFx1s3Z4yQLCbNg29wtBFj8

Digitalisierung im Fadenkreuz

LIEBENSTEIN LAW
KANZLEI FÜR WIRTSCHAFTS- UND GESUNDHEITSRECHT

WannaCry ist ein Schadprogramm für Windows, das im Mai 2017 für einen schwerwiegenden Cyberangriff genutzt wurde. WannaCry befällt Windows-Betriebssysteme, die nicht mit einem bestimmten, seit März 2017 von Microsoft angebotenen Patch nachgebessert wurden.

Nach Befall eines Computers verschlüsselt das Schadprogramm bestimmte Benutzerdateien des Rechners und fordert als Ransomware den Nutzer auf, einen Betrag in der Kryptowährung Bitcoin zu zahlen, nach ungenutztem Ablauf einer Frist droht das Programm mit Datenverlust. Außerdem versucht das Programm, als Computerwurm weitere Windows-Rechner zu infizieren.

Ab dem 12. Mai 2017 wurden über 230.000 Computer in 150 Ländern infiziert und jeweils Lösegeldzahlungen verlangt. Der Angriff wurde von Europol als noch nie da gewesenes Ereignis beschrieben

Digitalisierung im Fadenkreuz

LIEBENSTEIN LAW
KANZLEI FÜR WIRTSCHAFTS- UND GESUNDHEITSRECHT

WannaCry basiert auf EternalBlue, einem Exploit der Sicherheitslücke MS17-010 im SMB-Protokoll (auch NetBIOS) von Microsoft.

Der US-amerikanische **Auslandsgeheimdienst NSA** nutzte diese Lücke über mehr als fünf Jahre, ohne Microsoft über sie zu informieren, für eigene Zwecke mit einem Exploit, der den Namen EternalBlue erhielt und von Hackern der vermutlich NSA-nahen Equation Group entwickelt worden war.

Erst nachdem die NSA erfahren hatte, dass das Wissen über EternalBlue gestohlen worden war, informierte sie Microsoft über die Sicherheitslücke.

Das Unternehmen stellte daraufhin am 12. März 2017 einen Sicherheits-Patch für den SMBv1-Server zur Verfügung.

Digitalisierung im Fadenkreuz

LIEBENSTEIN LAW
KANZLEI FÜR WIRTSCHAFTS- UND GESUNDHEITSRECHT

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (BSI-Kritisverordnung)

Digitalisierung im Fadenkreuz

LIEBENSTEIN LAW
KANZLEI FÜR WIRTSCHAFTS- UND GESUNDHEITSRECHT

Gesetz
zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)*

Vom 17. Juli 2015

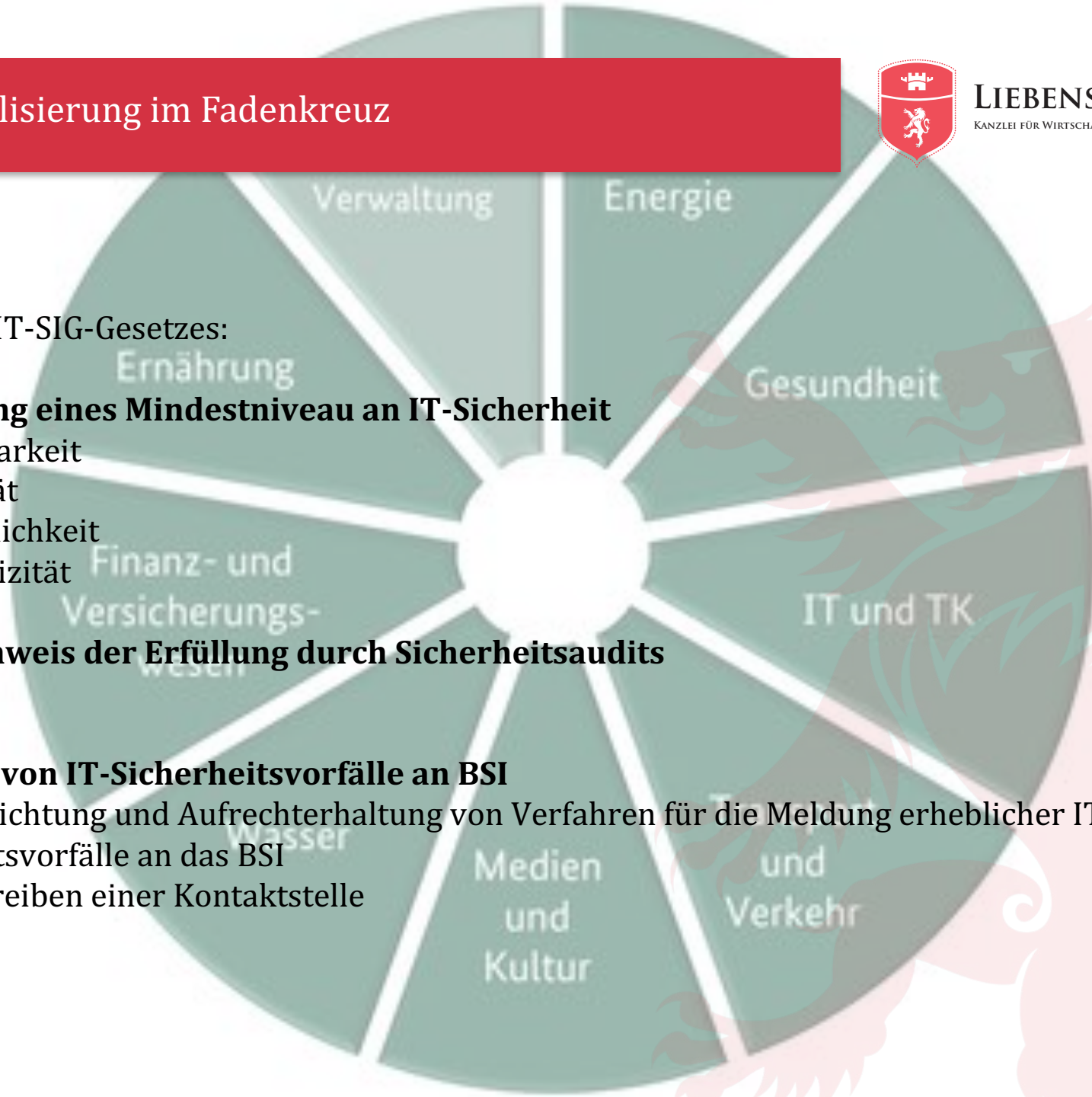
Am 25. Juli 2015 ist **das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme** (IT-Sicherheitsgesetz, IT-SiG) in Kraft getreten.

Betreiber kritischer Anlagen müssen künftig:

- einen Mindeststandard an IT-Sicherheit einhalten und
- erhebliche IT-Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik (BSI) melden.

Kritische Infrastrukturen (KRITIS) sind Einrichtungen, Anlagen oder Teile davon, die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

Digitalisierung im Fadenkreuz



Ziele des IT-SIG-Gesetzes:

Einhaltung eines Mindestniveau an IT-Sicherheit
- Verfügbarkeit
- Integrität
- Vertraulichkeit
- Authentizität

Den Nachweis der Erfüllung durch Sicherheitsaudits
- Audits

Meldung von IT-Sicherheitsvorfälle an BSI
- Die Einrichtung und Aufrechterhaltung von Verfahren für die Meldung erheblicher IT-Sicherheitsvorfälle an das BSI
- Das Betreiben einer Kontaktstelle

Digitalisierung im Fadenkreuz

LIEBENSTEIN LAW
KANZLEI FÜR WIRTSCHAFTS- UND GESUNDHEITSRECHT

Bearbeitungsstand: 24.05.2017 16:15 Uhr

Referentenentwurf

des Bundesministeriums des Innern

Erste Verordnung zur Änderung der BSI-Kritisverordnung

A. Problem und Ziel

Das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) ist am 25. Juli 2015 als Artikelgesetz in Kraft getreten. Als Kernbestandteil sehen die neu eingefügten §§ 8a und 8b des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetzes) vor, dass informationstechnische Systeme, die für die Funktionsfähigkeit von Kritischen Infrastrukturen maßgeblich sind,

Digitalisierung im Fadenkreuz

LIEBENSTEIN LAW
KANZLEI FÜR WIRTSCHAFTS- UND GESUNDHEITSRECHT

Teil 3 Anlagenkategorien und Schwellenwerte

Spalte A	Spalte B	Spalte C	Spalte D
Nummer	Anlagenkategorie	Bemessungskriterium	Schwellen-wert
1.	Medizinische Versorgung		
1.1	Krankenhaus	vollstationäre Fall-zahl/Jahr	30 000
2.	Versorgung mit Medizinprodukten, die Verbrauchsgüter sind		
2.1	Herstellung		
2.1.1	Produktionsstätte	Umsatz in Euro/Jahr	90,6 Millionen
2.2	Abgabe		
2.2.1	Abgabestelle	Umsatz in Euro/Jahr	90,6 Millionen

Digitalisierung im Fadenkreuz

LIEBENSTEIN LAW
KANZLEI FÜR WIRTSCHAFTS- UND GESUNDHEITSRECHT

Die Anzahl der im Gesetzentwurf der Bundesregierung zum IT-Sicherheitsgesetz genannten bis zu 2 000 Betreiber über alle sieben Sektoren wird abschließend wie folgt konkretisiert. Durch diese Änderungsverordnung werden in den Sektoren Finanz- und Versicherungswesen, Gesundheit sowie Transport und Verkehr 1205 Kritische Infrastrukturen erfasst.

Sektor	Dienstleistung	Anlagenkategorien	Geschätzte Anzahl der Anlagen
Gesundheit	Medizinische Versorgung	Krankenhäuser	110
	Versorgung mit Medizinprodukten, die Verbrauchsgüter sind	Produktionsstätte, Abgabestelle	2
	Versorgung mit verschreibungspflichtigen Medikamenten	Produktionsstätte, Anlage oder System zur Entnahme und Weiterverarbeitung von Blutspenden, Betriebs- und Lagerraum, Anlage oder System zum Vertrieb von verschreibungspflichtigen Arzneimitteln, Apotheke	151
	Laboratoriumsdiagnostik	Transportsystem, Kommunikationssystem zur Auftrags- oder Befundübermittlung, Labor	135

Digitalisierung im Fadenkreuz

LIEBENSTEIN LAW
KANZLEI FÜR WIRTSCHAFTS- UND GESUNDHEITSRECHT

KRITISCHE INFRASTRUKTUR

Verordnung mit Wechselwirkungen

Seit Juni ist der zweite Teil der „Kritis"-Verordnung zur Umsetzung des IT-Sicherheitsgesetzes in Kraft. Bis Dezember müssen sich 110 Kliniken bei der zuständigen Aufsichtsbehörde registrieren und binnen zwei Jahren eine ausreichende Absicherung nachweisen. kma sprach mit dem Medizinjuristen Prof. Hans-Hermann Dirksen über mögliche rechtliche Fallstricke.

Herr Prof. Dirksen, die seit Juni gültige Kritis-Rechtsverordnung zwingt betroffene Kliniken dazu, einen Mindestschutz bei der IT-Sicherheit auf „Stand der Technik" nachzuweisen. Eine Formulierung, die viel Interpretation zulässt. Wie ist „Stand der Technik" juristisch definiert?

Nun, es gibt verschiedene Möglichkeiten. Der Nachweis kann nach den Regeln des BSI-Grundschutz oder durch Zertifizierung nach ISO 27001 erfolgen. Es besteht auch die Möglichkeit, einen branchenspezifischen Standard (B3S) zu entwickeln. Interessanterweise orientiert sich der neue Bran-

Foto: Silke Brenner

Prof. Dr. Hans-Hermann Dirksen ist Anwalt für Wirtschaftsrecht in Frankfurt am Main und hat sich besonders auf das Recht der Digitalsierung spezialisiert. Er berät dazu Verbände, Ärzte und und medizinische Einrichtungen.

gehabt, das trifft uns nicht." So wird die gute Idee eines flächendeckenden Mindeststandards verpuffen. Dass

konform war, könnte sie damit einer Beweislastumkehr begegnen.

1. Fazit:

1. Das IT-SiG ist ein erster Schritt in die richtige Richtung. Auch ein Vorbild?

2. Schwierig ist die kurze Frist zur Umsetzung der erforderlichen Maßnahmen.

3. Der Aufwand bei den Mitarbeitern wird oftmals unterschätzt und ohne externe Hilfe mit fundierten Kenntnissen wird kaum die Zertifizierungsfähigkeit nicht erreichbar sein.

4. In der Furcht der finanziellen Aufwendungen, besteht die Gefahr, dass die Unternehmen an anderer Stelle bei der IT-Sicherheit Kürzungen vornehmen.

Digitalisierung im Fadenkreuz

LIEBENSTEIN LAW
KANZLEI FÜR WIRTSCHAFTS- UND GESUNDHEITSRECHT

IT-COMPLIANCE

Digitalisierung im Fadenkreuz

LIEBENSTEIN LAW
KANZLEI FÜR WIRTSCHAFTS- UND GESUNDHEITSRECHT

„Sicherheit ist kein Zustand, den man irgendwann erreicht und dann vergessen kann, sondern eine permanente Aufgabe. Sie muss als formeller Management-Prozess aufgesetzt werden, wodurch sich einerseits die Permanenz der Aufgabe darstellen lässt, andererseits die Teilprozesse alle wesentlichen Aktivitäten des Sicherheitsmanagements widerspiegeln können."

Compliance und Managerhaftung

Compliance ist die Pflicht der Unternehmensleitung, die Einhaltung der Gesetze durch das Unternehmen (und ggf. der Tochtergesellschaften) sicherzustellen.

Risikomanagement: Pflicht für Kapitalgesellschaften folgt aus §§ 317, 322 Abs. 6 i.V.m. § 289 Abs. 2 und 5 HGB sowie für die Aktiengesellschaft aus § 91 Abs. 2 AktG.

Missachtung führt zu zivilrechtlichem und strafrechtlichem Haftungsrisiko Pflichtverletzung / Verletzung der Sorgfaltspflicht / Strafnormen/ Owi.

Gesamtschuldnerische Haftung des Vorstands/Aufsichtsrats bei AktG, Genossenschaft und Geschäftsführung der GmbH („Härte der Organhaftung“). Kenntnis der Anforderungen an einzelnes Organmitglied bzgl. Kontrollpflichten unabdingbar.

Allerdings keine unmittelbare umfassende gesetzliche Pflicht nach h.M. Im juristischen Schrifttum dennoch abgeleitet aus § 91 Abs. 2 oder aus §§ 76, 93 AktG.

IT-Risikomanagement

Für die zivilrechtliche Haftung gelten die allgemeinen Vorschriften des Gesellschaftsrechts, hier insbesondere die Rechtspflicht zur Gewährleistung einer effizienten IT-Sicherheit, die sich ableitet aus dem Gebot zur Einrichtung, Dokumentation und Kontrolle eines in jeder Hinsicht aktuellen und effizient arbeitenden Risikomanagementsystems.

Die Rechtsprechung sieht im Fehlen, der Unvollständigkeit, der Ungeeignetheit und sogar bereits in der fehlenden Dokumentation eines Risikomanagementsystems einen erheblichen Gesetzesbruch:

So wurden etwa die außerordentliche Kündigung eines AG-Vorstandsvertrages wegen Fehlens eines Risikomanagementsystems für wirksam gehalten (Landgericht Berlin, Urteil vom 03.07.2002) und in der unterbliebenen Dokumentation eines Risikofrüherkennungssystems ein wesentlicher Gesetzes-verstoß gesehen, der zur Anfechtbarkeit des Beschlusses über die Haftungsentlastung des Vorstandes führt (Landgericht München I, Urteil vom 05.04.2007).

Digitalisierung im Fadenkreuz

LIEBENSTEIN LAW
KANZLEI FÜR WIRTSCHAFTS- UND GESUNDHEITSRECHT

Nach ständiger **Rechtsprechung** gehört eine zuverlässige IT-Sicherheit in Bezug auf Firmen- und Personendaten zu den unternehmerischen Selbstverständlichkeiten (OLG Hamm, 01.12.2003; OLG Karlsruhe, NJW-RR 1997, 554; OLG Köln, 22.04.1994, 1262).

Eine „Delegierbarkeit“ der Haftung durch Übertragung von IT-relevanten Aufgaben und Maßnahmen kommt nicht in Betracht.

2. FAZIT

- Welche Rechtsnormen und sonstigen Regelwerke sind für die IT des Unternehmens relevant?
- Welche IT-gestützten Prozesse und Anwendungen sind betroffen und welche Anforderungen müssen sie erfüllen?
- Welche Risiken resultieren in welcher Höhe aus fehlender oder mangelhafter IT-Compliance?
- Welche Compliance-Anforderungen müssen die einzelnen IT-Bereiche (Infrastruktur, Datenhaltung, Betrieb, Prozesse) erfüllen?
- Welche technischen, organisatorischen und personellen Maßnahmen müssen für die Gewährleistung von IT-Compliance ergriffen werden?

HAFTUNGSRISIKEN

Haftungsrisiken erkennen

Das gestiegene Anforderungsprofil, gepaart mit einem stark erhöhten Bedrohungsszenario durch Wirtschaftsspionage, Sabotage aber auch durch die verschärften Compliance-Treiber Datenschutz und die Datensicherheit führen dazu, dass Geschäftsführer Risiken für die Infrastruktur ihres Unternehmens, dessen geistiges Eigentum sowie für die „Persönlichkeitsrechte“ des Unternehmens (Reputation, Image) und der im Unternehmen tätigen Mitarbeiter sehr frühzeitig erkennen, wenn nicht vorausahnen muss, um die – ggf. auch persönlichen – Haftungsfallstricke zu vermeiden.

Haftungsrisiko 1

Für denjenigen, der das **Lizenzmanagement** verantwortet, besteht ein erhebliches Haftungspotenzial. Insbesondere muss eine illegale Softwarenutzungen verhindert werden.

Die Lizenzschadenshaftung bei Unterlizenzierung ist erheblich, eine persönliche Verantwortlichkeit bei Lizenzverstößen im strafrechtlichen Sinne nicht auszuschließen.

Das OLG Karlsruhe hat am 23.04.2008 entschieden, dass im Bereich des Lizenzwesens schon die bloße Kenntnis vom Einsatz einer nicht ordnungsgemäß lizenzierten Software Auslöser für eine persönliche haftungsrechtliche Inanspruchnahme sein kann.

LIEBENSTEIN LAW
KANZLEI FÜR WIRTSCHAFTS- UND GESUNDHEITSRECHT

Haftungsrisiko 2

Mit der neuen EU-Datenschutz-Grundverordnung (DSGVO) soll das Datenschutzrecht innerhalb Europas vereinheitlicht werden, um dem Einzelnen mehr Kontrolle über seine Daten zu verschaffen.

Künftig sollen Nutzer leichteren Zugang zu ihren Daten haben. Jeder hat damit das Recht zu erfahren, welche Daten über ihn gesammelt werden. Zudem wird der Nutzer Anspruch auf klare und leicht verständliche Informationen darüber haben, wer seine Daten zu welchem Zweck wie und wo verarbeitet.

Dazu gehört auch, dass der Nutzer künftig noch ausführlicher darüber informiert werden muss, wenn seine Daten gehackt wurden. Damit soll es dem Nutzer noch früher möglich sein, Maßnahmen zu seinem Schutz einzuleiten.

Beispiel: Die **Datenschutz-Folgenabschätzung** gilt als verpflichtend, sobald abzusehen ist, dass Rechte und Freiheiten des Betroffenen durch die Verarbeitung einem Risiko ausgesetzt sind. Dies trifft ganz besonders dann zu, wenn neue Technologien angewandt werden.

Ein Risiko liegt vor, wenn mindestens eines der folgenden vier Kriterien erfüllt ist.

- Die Daten gelten als besonders schützenswert (z.B. biometrische Daten oder Daten von Minderjährigen).
- Es findet eine intensive Datenverarbeitung statt (z.B. in Form einer weit reichenden Datenverknüpfung).
- Die Verarbeitung unzulässig sein könnte
- Die Verarbeitung tiefgreifende Auswirkungen für den Betroffenen hat

Haftungsrisiko 3

Beim **Outsourcing** geschäftskritischer Prozesse und Daten entsteht die Verpflichtung den beauftragten Dienstleister zu überwachen und zu kontrollieren.

Dies betrifft:
die Einhaltung der Vorschriften der Datensicherheit
Die Handhabung von Auftragsdatenverarbeitungsverträgen
Probleme der Aufbewahrung, Archivierung, Backup

Vertrags-Check:
Die Geschäftsleitung sollte die vertraglichen Beziehungen und Haftungsverhältnis in Bezug auf IT-Outsourcing-, Geschäftsprozess-Outsourcing- und Cloud Computing-Anbieter einer genauen Prüfung unterziehen.

Viele Verträge mit Dritten sind bezüglich der Verantwortung für den Schutz der kritischen Informationen der Organisation ungenau und daher riskant.

Haftungsrisiko 4

Selbstverständlich muss die technisch-administrative IT-Sicherheit auch auf **Belegschaftsebene** ihren Niederschlag finden.

Aufklärungs- und Sensibilisierungsmaßnahmen,
Arbeitsverträge anpassen
Verabschiedung von Policies
Einrichtung effizienter Schutzmechanismen auf Nutzerebene
Installation von Software, die Sicherheitslücken im System schließt

Rechtlich-organisatorische Vorgaben der Geschäftsführung für den Umgang mit der Telekommunikation und den Telemedien, insbesondere bei der Nutzung von Internet, E-Mail und sozialen Medien sowie der dienstlichen Verwendung privater Endgeräte veranlassen.

Haftungsrisiko 5

Personalmanagement:

- Umgang mit enttäuschten, demotivierten Mitarbeitern
- Handhabung von vertraulichen Gesprächsnotizen
- Funktionswechsel

Enttäuschte Mitarbeiter stellen ein nicht unerhebliches Risiko dar. Das Risiko ist auch unter dem Aspekt gravierend, dass es sich bei demotivierten Mitarbeitern oft kurz zuvor noch um vertrauenswürdige Mitarbeiter handelte, die mit entsprechenden Befugnissen und Rechten ausgestattet waren.

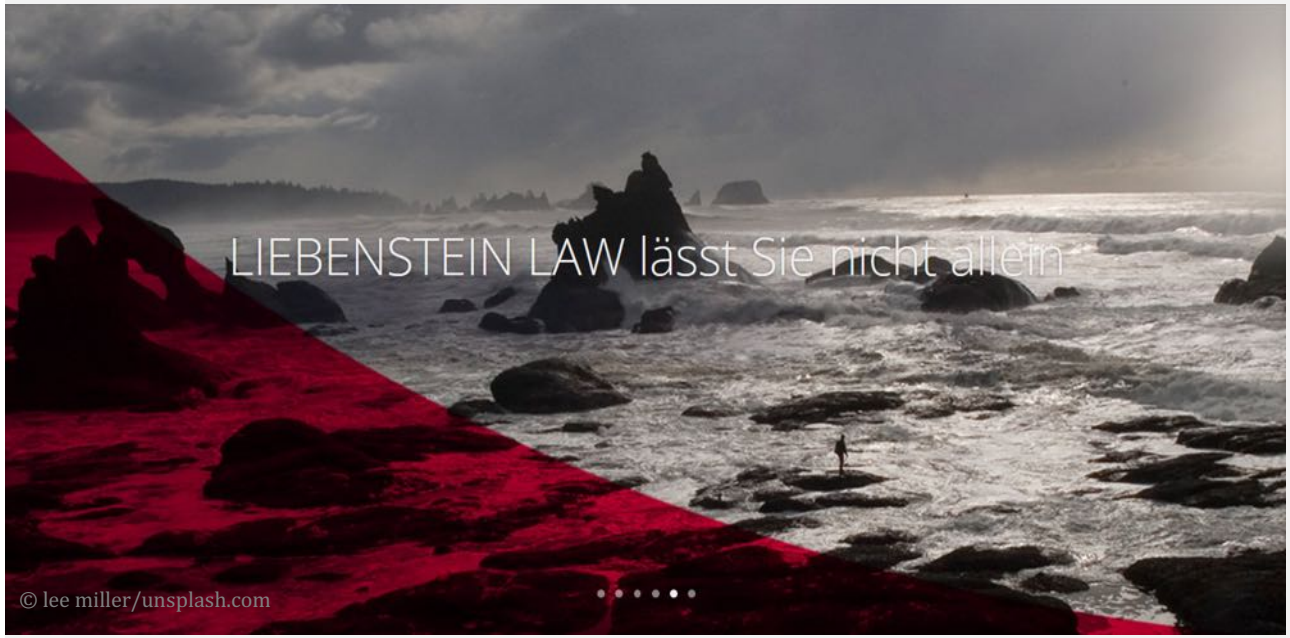
Dem Mitarbeiter ist es in der Regel nicht anzumerken, wann sich der Wandel vom loyalen Firmenangehörigen zur Bedrohung für die Informationssicherheit vollzieht. Zur Minimierung dieses Risiko sollten alle Anzeichen auf eine Verschlechterung des Arbeitsumfeldes und Enttäuschung bei den Mitarbeitern ernst genommen und offen kommuniziert werden.


ACT NOW!

3. FAZIT

- Cybersicherheit ist ein Compliance- und Risikomanagementthema, kein Technologiethema.
- IT-Sicherheit ist „Chefsache“ und gehört als Teil der „Corporate Governance“ zu den unternehmerischen Lenkungs- und Leitungsaufgaben.
- Mitglieder der Unternehmensleitung müssen die rechtlichen Aspekte der Cybersicherheit kennen. Eine Datenschutzverletzung setzt Organisationen dem Risiko zivil- und strafrechtlicher Disziplinarmaßnahmen und Bußgelder durch Aufsichtsbehörden, Sammelklagen durch Kunden und Aktionäre und rechtlicher Maßnahmen betroffener Partnerunternehmen aus.
- Mitglieder der Unternehmensleitung müssen annehmbare Risikoniveaus für geschäftliche Abläufe identifizieren. Sicherheitsrichtlinien müssen im Unternehmen an jedermann kommuniziert werden.

Ich bedanke mich sehr herzlich für Ihre Aufmerksamkeit!



Prof. Dr. Hans-Hermann Dirksen
Rechtsanwalt | Hochschullehrer

LIEBENSTEIN LAW
Kanzlei für Wirtschafts- und Gesundheitsrecht
Aystettstr. 3 - Holzhausenviertel
60322 Frankfurt/M.
mail@liebenstein-law.de
www.liebenstein-law.de
+49 69 9592 – 8027