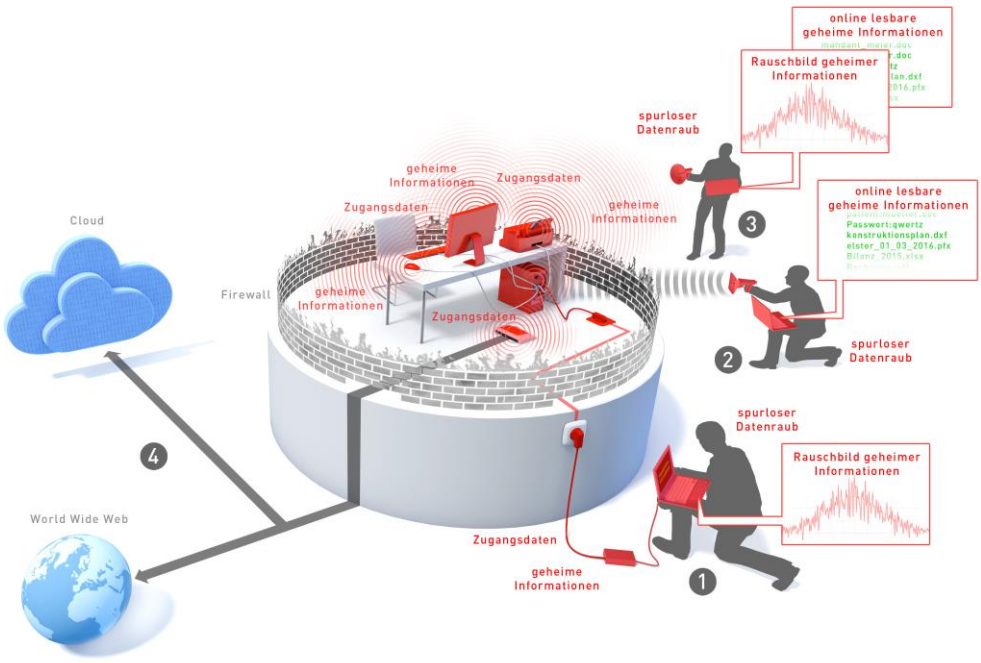
HOFFMANN LIEBS

# Cybersicherheit ist ohne geschützte IT-Hardware nicht möglich

Whitepaper:

## Gesetzliche Pflichten und Haftungsrisiken im Zusammenhang mit mangelnder Absicherung von IT-Hardware

### 1. „Spurloser Datenraub“ - unkontrollierter Abfluss von sensiblen Informationen und Nutzerdaten sowie die Notwendigkeit von Gegenmaßnahmen




Unter dem „spurlosen Datenraub“ verstehen sich hardwarebasierte Angriffsstrategien. Die Angreifer machen sich insbesondere die freie- und leitungsgebundene Abstrahlung von IT-Hardware zunutze, um Daten in der Eingabephase oder Verarbeitung abzufangen und somit an Informationen zu gelangen, ohne Spuren zu hinterlassen. Durch das Abfangen ungesicherter elektromagnetischer Signale (2 im Schaubild) der IT-Hardware (PC, Monitor, Scanner, Drucker oder ähnliche IT-Peripheriegeräte) in Form von „Rauschbildern“ ist es ihnen möglich, an sensible Informationen zu gelangen, indem sie diese in „Rauschbildern“ verborgenen Daten mit professionellen Analysemethoden wieder lesbar machen. Zudem ist es möglich, diese Informationen aus dem öffentlich zugänglichen Stromnetz (1 im Schaubild) abzugreifen, nachdem die Signale aus der

Hauptplatine eines PCs über dessen Netzteil hierhin gelangt sind. Ein weiteres Angriffsszenario bildet die Manipulation von Datenleitungen, indem bspw. ein Monitorkabel mit einem winzigen „Signalverstärker“ versehen wird, sodass Daten über die Anstrahlung mit handlichen Radarsystemen (3 im Schaubild) ausgespäht werden können.

Die Einhaltung der nach dem Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) festgelegten Grenzwerte für die Abstrahlung von elektronischen Geräten reicht nicht aus, um das Abhören der sog. „bloßstellenden Abstrahlung“, also der informationsgetragenen Abstrahlung zu verhindern. Sollen Daten mit hohem Schutzbedarf verarbeitet werden, ist es daher immer sinnvoll, zusätzliche Schutzmaßnahmen zu ergreifen und diese regelmäßig dem Stand der Ausspähtechniken anzupassen. Dazu gehört auch die Überprüfung der Peripherie auf Manipulation. Insbesondere sollte der freie Zugang zu Rechnerschnittstellen wie USB-, Netzwerk-, Peripherie-Anschlüsse für Mikrofon und Kopfhörer und SD-Karten Slots immer blockiert sein. Besonders vorteilhaft ist der Einsatz „sicherer" Hardware, d.h. vom Internet entkoppelte Rechner mit Authentifizierungsmechanismen gegen unbefugte Zugriffe.

Alle Peripherie-Anschlüsse insbesondere die Stromversorgungsanschlüsse der IT-Komponenten sollten mit entsprechenden Filter-Elementen versehen werden oder wenn möglich direkt durch Glasfaser-Leitungen ersetzt werden. Eigenabstrahlung über Gehäusespalte und Leitungen sind zu minimieren. Gegen Einstrahlungen von außen, z.B. Radar, sollte spezielle Warn-Sensorik zum Einsatz kommen.

Die Möglichkeit von Angriffen auf die IT-Hardware ist im Grundsatz seit 1985 bekannt. So machen insbesondere diverse Geheimdienste seit geraumer Zeit von dieser Abhörmöglichkeit Gebrauch. In Anbetracht der rasanten technologischen Entwicklung ist davon auszugehen, dass die Regenerierung der Daten aus „Rauschbildern“ heute schon mit einem überschaubaren technischen und finanziellen Aufwand möglich ist, sodass entsprechende Angriffe nicht nur für staatliche Geheimdienste interessant sein dürften. Hierbei ist zu beachten, dass Geräte zur Ausspähung und Auswertung der bloßstellenden Abstrahlung in der Regel problemlos erworben werden können.

Daher ist es wichtig, dass Unternehmen nicht nur in die Absicherung ihrer Betriebs- und Applikations-Software und den Schutz ihrer Datenbestände, sondern auch in die Sicherheit ihrer Firmen-Hardware investieren. Die bereits im März 1996 vom BSI veröffentlichten „Schutzmaßnahmen gegen Lauschangriffe“ sehen z.B. folgende Maßnahmen vor:

- regelmäßige Überprüfung der Netz-, Telefon- und Datenleitungen auf Manipulation
- Verwendung von zugelassenen, abstrahlsicheren Geräten
- Verwendung von Netz-, Telefon- und Datenleitungsfiltern

## 2. Gesetzliche Pflichten zur Umsetzung der IT-Sicherheit nach der Datenschutz-Grundverordnung (DSGVO)

Die seit dem 25.05.2018 umzusetzende DSGVO ist anwendbar, wenn personenbezogene Daten (z.B. Mitarbeiter-, Kunden-, Lieferantendaten) verarbeitet werden. Dies trifft auf nahezu jedes Unternehmen zu, sodass den Vorschriften eine hohe Relevanz zukommt.

Die DSGVO verpflichtet die Unternehmen, geeignete und dem Stand der Technik entsprechende technische und organisatorische Maßnahmen („TOMs“) zur Umsetzung eines angemessenen datenschutzrechtlichen IT-Sicherheitsstandards zu treffen. Auch aus ihr ergibt sich, dass die unternehmerische Datenverarbeitung den klassischen Sicherheitszielen der IT-Sicherheit, insbesondere der Vertraulichkeit, entsprechen muss. Daher müssen Maßnahmen gegen den unbefugten Datenzugriff durch Ausspähung getroffen werden. Ob und in welchem Umfang die Unternehmen konkret verpflichtet sind, Maßnahmen zur Härtung von IT-Hardware zu implementieren, geht aus der Verordnung nicht vor. Wann von einem angemessenen Sicherheitsstandard ausgegangen werden kann, lässt sich im Wege einer umfassenden objektiven Risikoabwägung ermitteln, indem der Aufwand der Sicherheitsmaßnahme mit dem Risiko für die Datensicherheit abgewogen wird. Hierbei ist zu beachten, dass sich neben Cyberkriminellen auch staatliche Stellen unbefugten Datenzugang verschaffen können. Auch ist zu berücksichtigen, dass die Risiken mangelhaft gesicherter IT-Hardware seit langem bekannt sind und intensiv für Angriffe genutzt werden. Daher ist von einer mittleren bis hohen Eintrittswahrscheinlichkeit für das Risiko, dass die unzureichende IT-Hardware-Absicherung für einen Angriff genutzt wird, auszugehen.

Unternehmen haben zudem die Schwere eines möglichen Schadens zu ermitteln und in die Abwägung mit einzubeziehen. Hierbei sind folgende Faktoren zu berücksichtigen:

- Verarbeitung besonders schutzwürdiger Daten (z.B. Gesundheitsdaten, Religionszugehörigkeit) oder Personengruppen (z.B. Kinder, Beschäftigte)
- Verarbeitung nicht veränderbarer und eindeutig identifizierenden Daten

- automatisierte Verarbeitungen, die eine systematische und umfassende Bewertung persönlicher Aspekte (z.B. Profiling) beinhalten und auf deren Grundlage dann Entscheidungen mit erheblichen Rechtswirkungen für Betroffene gefällt werden
- der Schaden ist nicht oder kaum reversibel oder die betroffene Person hat mangels Kenntnis von der Verarbeitung nur beschränkte Möglichkeiten, diese zu prüfen oder sich ihrer zu entziehen
- die Verarbeitung ermöglicht eine systematische Überwachung
- Anzahl der betroffenen Personen, der Datensätze und der Merkmale in einem Datensatz sowie die geographische Reichweite der verarbeiteten Daten

Liegt einer oder liegen mehrere dieser Faktoren vor, ist das Unternehmen regelmäßig verpflichtet, Maßnahmen gegen die Informationsausspähung durch Auswertung der freien und leitungsgebundenen bloßstellenden Abstrahlung zu ergreifen. Dasselbe gilt für Unternehmen besonders sensibler Branchen (Banken, Versicherungen). Die Maßnahmen müssen sodann regelmäßig auf ihre Wirksamkeit hin überprüft werden. Soweit sie nicht mehr dem Stand der Technik entsprechen, sind sie durch verbesserte Mechanismen zu ersetzen.

Eine Verletzung datenschutzrechtlicher IT-Sicherheitspflichten kann mit einer Geldbuße von bis zu **10 Mio. EUR** oder **2 % des gesamten weltweit erzielten Jahresumsatzes** des vorangegangenen Geschäftsjahrs sanktioniert werden. Zudem kann die Datenschutzaufsichtsbehörde gegenüber den Unternehmen verbindliche Anordnungen oder Anweisungen aussprechen, deren Nichtbefolgung eine Geldbuße von bis zu **20 Mio. EUR** bzw. **4 % des weltweiten Jahresumsatzes** nach sich ziehen kann.

## 3. Gesetzliche Pflichten zur Umsetzung der IT-Sicherheit nach BSIG (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik)

Nach dem BSIG sollen Betreiber „kritischer Infrastrukturen“ („KRITIS“) ein dem Stand der Technik entsprechendes Mindestniveau an IT-Sicherheit einhalten und dieses mindestens alle zwei Jahre nachweisen. Als Betreiber einer kritischen Infrastruktur sind Unternehmen der Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung oder Finanz- und Versicherungswesen anzusehen, wenn durch einen Systemausfall Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit drohen. Der Regelschwellenwert, ab welchem ein Unternehmen als Betreiber einer kritischen Infrastruktur anzusehen ist, liegt bei 500.000 versorgten Personen. Es wird davon ausgegangen, dass bis zu 2.000

Unternehmen und Einrichtungen als Betreiber kritischer Infrastrukturen gelten und dementsprechend die Vorgaben des BSIG einzuhalten haben. Auch nachgelagerte Dienstleistungen und Prozesse unterliegen diesen Schutzmaßnahmen, sodass ebenso alle unmittelbar für die Funktionsfähigkeit der jeweiligen kritischen Anlage notwendigen IT-Systeme dem Sicherheitsstandard des BSIG entsprechen müssen. Die Regelungen des BSIG gelten auch für Online-Marktplätze und –Suchmaschinen sowie Cloud-Computing-Dienste („digitale Dienste“) einer normierten Größe.

Da KRITIS-Betreiber essentielle Versorgungsdienstleistungen erbringen, ist auch der Schutz der IT-Hardware umfassend sicherzustellen. Sie haben daher unter Einhaltung des technischen Standes angemessene technische und organisatorische Vorkehrungen („TOV“) zur Vermeidung von Sicherheitsvorfällen zu treffen. Angemessen sind diese, wenn der erforderliche Aufwand nicht außer Verhältnis zu den Folgen etwaiger IT-Ausfälle steht. Allein finanzielle Erwägungen können keine Einschränkung des Sicherheitsniveaus begründen, da das angemessene Schutzniveau nur unter Berücksichtigung der Versorgung der Bevölkerung mit der kritischen Dienstleistung erfolgen kann. Das Ziel einer lückenlosen Versorgung ist daher mit dem notwendigen Umsetzungsaufwand abzuwägen.

Durch eine unzureichende Härtung der IT-Hardware wird insbesondere das IT-Schutzziel der Vertraulichkeit betroffen. Hiermit ist der Schutz vor Informationsausspähung insoweit, als dass nur befugte Personen in zulässiger Art und Weise auf die entsprechenden Daten zugreifen können, gemeint. Daher ist der Datenzugriff durch Ausspähung der freien und leitungsgebundenen Abstrahlung mit dem Stand der Technik entsprechenden Schutzmaßnahmen, z.B. durch Verwendung abstrahlarmer bzw. abstrahlgeschützter Geräte und Netzleitungen, zu unterbinden. Unter dem Stand der Technik sind die im Waren- und Dienstleistungsverkehr verfügbaren Verfahren, Einrichtungen oder Betriebsweisen, deren Anwendung die Erreichung der jeweiligen gesetzlichen Schutzziele am wirkungsvollsten gewährleisten kann, zu verstehen. Aus nationalen und internationalen Standards und Normen (DIN, ISO, ISO/IEC) ergeben sich konkretere Vorgaben.

Die fehlende Umsetzung der für die KRITIS-Betreiber gesetzlich vorgesehenen Sicherheitsvorkehrungen kann ein Bußgeld von bis zu **50.000,00 EUR** zur Folge haben.

## 4. Haftung der Geschäftsleitung

Setzt die Geschäftsleitung die vorgeschriebenen Maßnahmen zur IT-Sicherheit nicht um und entsteht hierdurch dem Unternehmen ein Schaden, kommt auch eine zivilrechtliche Haftung der Geschäftsleitung gegenüber dem Unternehmen in Betracht. Die Verpflichtung des Vorstands zur Risikovorsorge ergibt sich für die Aktiengesellschaft aus §§ 91, 93 AktG. Zudem trifft den Vorstand aufgrund seiner allgemeinen Leistungs- und Sorgfaltspflicht auch eine allgemeine Compliance-Pflicht, welche die Etablierung effektiver IT-Sicherheitsmaßnahmen mit einschließt. Der Umfang der Compliance-Pflicht richtet sich nach der Sensibilität der Daten, den möglichen Schadensszenarien sowie (sofern überhaupt möglich) den Kosten einer Schadensbeseitigung. Aufgrund der regelmäßig hohen Bedeutung der betrieblichen Daten für das Unternehmen sind die Anforderungen an die IT-Sicherheit hoch. Zudem trifft die Geschäftsleitung in prozessualer Hinsicht die Darlegungs- und Beweislast. Sie muss nachweisen, dass taugliche Maßnahmen getroffen wurden, bzw. dass kein Verschulden gegeben ist. Die Pflichten der §§ 91, 93 AktG haben eine „Ausstrahlungswirkung“ auf andere Gesellschaftsformen und gelten daher bspw. entsprechend für die Geschäftsleitung einer GmbH. Da die Inanspruchnahme des Geschäftsleiters für das durch einen Cyberangriff geschädigte Unternehmen eine geeignete Maßnahme zur Schadensmilderung darstellt, ist umso mehr zu empfehlen, die gesetzlich geforderten Maßnahmen zur Härtung von IT-Hardware umzusetzen.

**Peter Huppertz, LL.M.**
Rechtsanwalt und Partner
Fachanwalt für Informationstechnologierecht

**Hoffmann Liebs**
Partnerschaft von Rechtsanwälten mbB
Kaiserswerther Straße 119
40474 Düsseldorf

Telefon +49 211 51882 – 197
Fax +49 211 51882 – 220
E-Mail peter.huppertz@hoffmannliebs.de
Internet www.hoffmannliebs.de

Partnerschaft mit beschränkter Berufshaftung / Partnership with
Limited Professional Liability
Sitz / Seat: Düsseldorf
Amtsgericht Essen PR 1139