Digitalisierung und das IT-Sicherheitsgesetz in der Praxis

Herausforderungen, Adressaten, Maßnahmen und Sanktionen

Hartmut Pohl[1], Sascha Rauschenberger[2] und Christian Slota[3]

Inhalt

Auch für kleine Betreiber von Webservern und erst recht für z. B. Online-Shops gelten seit dem 24. Juli 2015 ausnahmslos erhöhte Anforderungen an die technischen und organisatorischen Maßnahmen zum Schutz ihrer Kundendaten und den von den Betreibern und ihren Kunden genutzten IT-Systemen. Weiterhin sind Telekommunikationsunternehmen verpflichtet, ihre Kunden zu warnen, wenn ihnen auffällt, dass Systeme des Kunden - etwa als Teil eines Bot-Netzes - für IT-Angriffe missbraucht werden. Gleichzeitig sollen sie ihre Kunden auf mögliche Wege zur Beseitigung der Störung hinweisen. Erweitert werden mit Inkrafttreten des IT-Sicherheitsgesetzes außerdem die Befugnisse des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Untersuchung der Sicherheit von IT-Produkten sowie die Zuständigkeit im Bereich der IT-Sicherheit der Bundesverwaltung.

Seit diesem Tag gelten darüber hinaus für die Betreiber von Kernkraftwerken und Telekommunikationsunternehmen neue Pflichten zur Meldung erheblicher IT-Sicherheitsvorfälle.

Für sonstige Betreiber Kritischer Infrastrukturen aus den Bereichen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen gilt eine entsprechende Meldepflicht erst nach Inkrafttreten einer das IT-Sicherheitsgesetz konkretisierenden Rechtsverordnung, Diese wird derzeit im Bundesministerium des Innern vorbereitet. Ziel des Gesetzes st, die beim BSI zusammenlaufenden Informationen über IT-Angriffe auszuwerten und den Betreibern Kritischer Infrastrukturen zur Verbesserung des Schutzes (anonymisiert) zur Verfügung zu stellen. Mit Inkrafttreten der Rechtsverordnung gilt dann auch die Pflicht für Betreiber Kritischer Infrastrukturen zur Implementierung von IT-Sicherheits-Mindeststandards.

Die Zahl und der Schweregrad der IT-Angriffe durch militärische Einrichtungen, Sicherheitsbehörden und insbesondere Organisierte Kriminalität nimmt international – insbesondere auch in Deutschland - stark zu[4], weil von diesen Angreifern erkannt worden ist, dass jeder Angriff, der eine Sicherheitslücke ausnutzt, erfolgreich ist. Besonders erfolgreich ist die Ausnutzung von Sicherheitslücken, die noch gar nicht veröffentlicht sind: Zero-Day-Vulnerabilities. Demzufolge steigt weltweit das Interesse an diesen unveröffentlichten Sicherheitslücken in Standardsoftware, Open Source und Software-Entwicklungs-Tools (SDK) weiterhin überproportional(- und auch der Preis. Die zunehmende Digitalisierung, wird das Problem weiter verschärfen.

Gleichwohl beschränkt sich das IT-Sicherheitsgesetz[5] in unzulänglicher Weise auf die **Meldung** tatsächlicher und auch **möglicher erheblicher Störungen**[6] und orientiert sich nicht an den – den Störungen zugrundeliegenden - ursächlichen Sicherheitslücken; weiterhin werden **Mindestanforderungen** an die IT-Sicherheit in Unternehmen der Kritischen Infrastrukturen[7] und Webseiten-Betreiber formuliert.

Der deutsche Gesetzgeber versucht also, Defizite in der IT-Sicherheit abzubauen. Der Versuch muss begrüßt werden – allerdings kommt das Gesetz 10 Jahre zu spät. Der jährliche Schaden insbesondere durch IT-Spionage aber auch durch IT-Sabotage wird derzeit in Deutschland auf einen mittleren zweistelligen Milliardenbetrag geschätzt.

Ein Novum ist die Verpflichtung der Hersteller informationstechnischer Produkte und Systeme sich z.B. mit Sicherheitsupdates (Patches) an der Beseitigung oder Vermeidung einer Störung "in

---

[1] Prof. Dr. Hartmut Pohl, Geschäftsführender Gesellschafter soft5check GmbH Informationssicherheitsberatung www.it-sicherheitsgesetz.news

[2] Sacha Rauschenberger, Managing Partner Future Business Consulting Köln

[3] Dipl.-Volkswirt, RA, Stb. Christian Slota UHY Wahlen & Partner, Köln

[4] Der erfolgreiche Angriff auf die IT-Systeme des Bundestags ist nur ein Beispiel unter vielen für tägliche Angriffe auf Unternehmen und Behörden in Deutschland.

[5] ‚Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)' http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1368.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1438428576337

[6] Gemeldet werden müssen erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit informationstechnischer Systeme, Komponenten oder Prozesse.

[7] ‚Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.'

zumutbarem Umfang" zu beteiligen! Diese Verpflichtung geht in Richtung der im Koalitionsvertrag vereinbarten (Produkt-)Haftung der Hersteller für Datenschutz- und IT-Sicherheitsmängel.

BSI ist binnen 6 Monaten von Unternehmen und Verbänden eine (die eingehenden Meldungen von sicherheitsrelevanten Vorfällen anonymisierende und sammelnde) Kontaktstelle zu benennen. In der Verordnung und den darauf basierenden Regelungen muss auch überhaupt noch festgelegt werden, was tatsächlich ein Sicherheitsvorfall etc. ist.

Das BSI wird die gemeldeten erheblichen Störungen auswerten und die Ergebnisse den Adressaten zur Verbesserung des Schutzes ihrer Infrastrukturen schnellstmöglich zur Verfügung zu stellen. Mit Inkrafttreten der Rechtsverordnung gilt dann auch die Pflicht für Betreiber Kritischer Infrastrukturen und Webseiten-Betreibern zur Erarbeitung und Umsetzung von IT-Mindeststandards in ihrem Bereich. Es kann erwartet werden, dass das BSI die Auswertungsergebnisse der gemeldeten Vorfälle in die Verbesserungsvorschläge einarbeitet – anderenfalls gäbe es ja keinen Anreiz zur Meldung.

Das IT-Sicherheitsgesetz richtet sich an alle Unternehmen, die eine Webseite betreiben – auch Kleinstunternehmen[8]. Solche sind zwar aus dem Anwendungsbereich des BSI-Gesetzes ausgenommen und können daher nicht Betreiber einer Kritischen Infrastruktur im Sinne dieses Gesetzes sein; sie werden aber von den Änderungen im Telemediengesetz adressiert. Auch Unternehmen, die von Regelungen des IT-Sicherheitsgesetzes nicht unmittelbar betroffen sind, aber als Zulieferer für Adressaten des Gesetzes tätig sind, werden künftig die Erfahrung machen, dass ihre Auftraggeber vergleichbare Maßnahmen einfordern.

Als Stand der Technik von Sicherheitsmaßnahmen im Bereich Informationssicherheit kann die Norm ISO 27001 bezeichnet werden; sie schlägt ein risikobasiertes Vorgehen vor. Auf der Grundlage einer vom Bundesministerium des Innern noch zu erstellenden Rechtsverordnung[9] werden die gesetzlich geforderten Mindeststandards festgelegt[10]. Diese dürften sich im Rahmen (oder sogar darunter?) des vom Bundesamt für die Sicherheit in der Informationstechnik (BSI) herausgegebenen ‚Grundschutzes[11] mit seinen Katalogen und Standards bewegen. Die sich aus dem Gesetz ergebenden Forderungen können über eine Neu-Festlegung des Stands der Technik - orientiert an neuen (internationalen) Normen oder Überarbeitung des Grundschutzes – zeitnah aktualisiert werden[12]. Als einzige konkret bezeichnete Sicherheitsmaßnahme werden im Telemediengesetz als ‚sicher anerkannte' Verschlüsselungsverfahren' genannt.

1. Warum und wozu ein IT-Sicherheitsgesetz?

IT-Anwendungen auf Computern und Netzen wie dem Internet und lokalen Netzen werden vielfältig von Staat, Wirtschaft und Gesellschaft genutzt. Unternehmen und Behörden verlagern zunehmend bedeutende Teilbereiche ihrer Aktivitäten (Digitalisierung) „ins Netz" (Stichworte: Industrie 4.0, Internet of Things, Cloud etc.). Nach aktuellen Umfragen sind schon heute im Durchschnitt aller Branchen zahlenmäßig mehr als die Hälfte aller deutschen Unternehmen vom Internet abhängig – faktisch dürften es im wirtschaftlichen, gesellschaftlichen und individuellen Bereich über 99% sein – mit weiter steigender Tendenz in der Qualität der Abhängigkeit.

Gezielte Angriffe auf IT-Systeme können heutzutage von überall in der Welt aus gestartet werden – oft braucht es kaum mehr als ein Smart Phone mit Internetzugang. Entscheidend sind die technisch aufwändigen - zunehmend zielgerichteten - Angriffen (bis zu ca. 50 Mannjahre Vorbereitungsaufwand!) mit ökonomischem oder politischem Hintergrund. Die Angriffstechniken, die heute Nachrichtendienste beherrschen, nutzt binnen 2 Jahren die Organisierte Kriminalität; entsprechende Angriffstools und Attack Development Kits (ADK) sind innerhalb eines weiteren Jahres als Open Source allgemein im Internet erhältlich.

Insbesondere die folgenden 4 Schutzziele sollen mit Sicherheitsmaßnahmen erreicht werden:

- **Vertraulichkeit** der übermittelten und gespeicherten Informationen
- **Integrität** - Korrektheit der empfangenen und gespeicherten Informationen
- **Verfügbarkeit** der Computer und des Internet inkl. der Software
- **Authentizität** bei Übermittlung, Empfang und Speicherung von Informationen

Diese Schutzziele müssen im Internet und bei den angeschlossenen Systemen von Unternehmen, Behörden und Privaten erreicht werden, wenn eine Volkswirtschaft funktionieren soll. Angreifer lesen Daten aus (Spionage) und manipulieren Daten (Sabotage) - auch in industriellen Steuerungsprozessen - oder bereichern sich durch Social Engineering wie Phishing. Akteure sind bei weitem nicht nur die Nachrichtendienste aus Ost und West sondern insbesondere auch einzelne Kriminelle und die Organisierte Kriminalität, die einen durchaus vergleichbaren Wissensstand besitzen. Angegriffen werden große und kleine Unternehmen, Behörden und auch Private!

---

[8] Unternehmen mit weniger als 10 Beschäftigen und einem Jahresumsatz bzw. Jahresbilanzsumme von höchstens 2 Mio. EUR.
[9] Über diese Rechtsverordnung wird nach Veröffentlichung an dieser Stelle zeitnah berichtet.
[10] Eine FAQ wird vom BSI bereitgestellt https://www.bsi.bund.de/SharedDocs/FAQs/DE/BSI/IT-SiGesetz/faq_node.html;jsessionid=043264126B193F324937ABC4CCE21817.2_cid286
[11] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html
[12] Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.

Mit dem Gesetz soll eine signifikante Verbesserung der Sicherheit informationstechnischer Systeme (IT-Sicherheit) in Deutschland erreicht werden, um den aktuellen und zukünftigen Gefährdungen der IT-Sicherheit wirksam begegnen zu können. Ziel des Gesetzes ist also die Verbesserung der IT-Sicherheit von Unternehmen und Behörden.

Besondere Bedeutung kommt im Bereich der IT-Sicherheit denjenigen Infrastrukturen zu, die für das Funktionieren unseres Gemeinwesens zentral sind. Der Schutz der IT-Systeme dieser sog. Kritischen Infrastrukturen und der für den Infrastrukturbetrieb nötigen Netze ist daher von größter Wichtigkeit (z.B.: Energie, Verkehr, Finanzbereich mit Zahlungssysteme).

Die Verteidigung der Bundesrepublik (mit allen Strukturen, Unternehmen, Behörden, Privaten) obliegt der Bundeswehr (Heer, Luftwaffe, Marine); die Streitkräfte wehren allerdings (bisher nur) territoriale Angriffe ab. Ein für 2016 erwartetes Weißbuch des BMVg soll den Inhalt des Begriffs Verteidigung erweitern und auch die Verteidigung gegen Angriffe aus dem Internet („Cyberwar") umfassen.

Weil die digitale Front aus der Sicht des Gesetzgebers nicht (nur) an den räumlichen (physischen) Grenzen der Bundesrepublik verläuft, sieht der Gesetzgeber (auf Vorschlag des Bundesinnenministeriums) den (zusätzlichen) Selbstschutz von Unternehmen und Privaten gegen Angriffe aus dem Internet als unverzichtbar an:

Am 25. Juli 2015 ist daher das IT-Sicherheitsgesetz als Artikelgesetz[13] (u.a. zur Änderung des Bundesbesoldungsgesetzes[14]) nach 6-monatiger Diskussion in Kraft getreten – nachdem es vom damaligen Innenminister Friedrich 2010 initiiert, damals von den Unternehmen aus Kostengründen abgelehnt und schließlich in der EU weiterverfolgt wurde; in der EU werden die Inhalte in der Cyberrichtlinie abgehandelt, die im Herbst 2015 verabschiedet werden soll[15]. Ggf. ergibt sich aus dieser europäischen Richtlinie eine Novellierung des deutschen IT-Sicherheitsgesetzes in wenigen Monaten.

Vergleichbare Regelungen finden sich in einigen Bereichen – so bei der ev. Kirche in Deutschland.[16]

2. Adressaten

Adressaten des Gesetzes sind die Betreiber von Webangeboten (z.B. Online-Shops, Unternehmenswebseiten) und Unternehmen[17] der Kritischen Infrastrukturen – d.h. der folgenden Branchen:

- Energie
- Informationstechnik und Telekommunikation
- Transport und Verkehr
- Gesundheit
- Wasser
- Ernährung sowie
- Finanz- und Versicherungswesen
- sowie Regierung und Verwaltung (Bundesbehörden) - womöglich als Reaktion auf die jüngsten Angriffe gegen den Bundestag.[18]

3. Forderungen des Gesetzes

Mit Inkrafttreten des IT-Sicherheitsgesetzes müssen Webseiten-Betreiber technische und organisatorische Maßnahmen nach dem Stand der Technik ergreifen, um sowohl unerlaubte Zugriffe auf ihre technischen Einrichtungen und Daten als auch Störungen zu verhindern.

Betreibern Kritischer Infrastrukturen entsteht Erfüllungsaufwand[19] wie folgt

---

[13] Dieses Artikelgesetz ändert u.a. die folgenden 7 Gesetze: BSI-Gesetz, Atomgesetz (Unternehmen sind sofort von den Regelungen des Gesetzes betroffen), Energiewirtschaftsgesetz, Telekommunikationsgesetz (Betreiber von öffentlichen Telekommunikationsnetzen und öffentlich zugänglichen Telekommunikationsdiensten müssen ab sofort nicht nur Ausfälle, sondern auch Beeinträchtigungen, die zu beträchtlichen Sicherheitsverletzungen führen können, an die Bundesnetzagentur melden. Sofern Telekommunikationsdienste-Anbietern Störungen auf den Systemen ihrer Nutzer bekannt werden, haben sie die unverzüglich darüber zu benachrichtigen. Sie müssen ihre Nutzer im Rahmen des Möglichen und Zumutbaren auch auf Hilfsmittel zur Erkennung und Beseitigung von Störungen hinweisen), Telemediengesetz (Anbieter geschäftsmäßig erbrachter Telemediendienste - also insbesondere Webseitenbetreiber - müssen ab sofort technische und organisatorische Maßnahmen nach dem Stand der Technik ergreifen, um sowohl unerlaubte Zugriffe auf ihre technischen Einrichtungen und Daten als auch Störungen zu verhindern), Bundeskriminalamtsgesetz.

[14] Die Stelle des Präsidenten des Bundesamtes für Sicherheit in der Informationstechnik wird von B6 nach B7 aufgewertet – vgl. aber die Einstufung der Präsidenten des Bundesamtes für Verfassungsschutz, des Bundeskriminalamtes und des Bundesnachrichtendienstes nach B9).

[15] Fioretti, J.: Internet Firms to be subject to new cybersecurity rules in EU. Reuters 6. Aug. 2015 http://uk.reuters.com/article/2015/08/06/us-eu-cybersecurity-idUKKCN0QB1ZD20150806

[16] Verordnung zur Sicherheit der Informationstechnik (IT-Sicherheitsverordnung - ITSVO-EKD) vom 29. Mai 2015 http://www.kirchenrecht-ekd.de/document/32147

[17] mit 10 und mehr Mitarbeitern, mit einem Umsatz oder einer Bilanzsumme von mehr als zwei Millionen Euro pro Jahr. Die tatsächlich betroffenen Unternehmen werden in einer vom Wirtschaftsministerium zu erarbeitenden Rechtsverordnung festgelegt.

[18] Der Deutsche Bundestag ist als Parlament der Bundesrepublik Deutschland ein Verfassungsorgan, ist damit keine Bundesbehörde und fällt daher auch nicht unter dieses Gesetz.

[19] Für Genehmigungsinhaber nach dem Atomgesetz und für Betreiber von Energieversorgungsnetzen und Energieanlagen entsteht darüber hinaus Erfüllungsaufwand für die Einhaltung zusätzlicher IT-Sicherheitsanforderungen.

1. Einhaltung eines Mindestniveaus an IT-Sicherheit
2. Nachweis der nachhaltigen Erfüllung des Mindestniveaus durch Sicherheitsaudits, Prüfungen oder Zertifizierungen (Höchstabstand 2 Jahre). Bei Mängeln können detaillierte Unterlagen nachgefordert und ihre Beseitigung verlangt werden
3. sowie die Überprüfung der Einhaltung dieser Sicherheitsanforderungen
4. Einrichtung und Aufrechterhaltung von Verfahren für die Meldung erheblicher IT-Sicherheitsvorfälle an das BSI sowie
5. Betreiben einer Kontaktstelle zum BSI

Um den Schutz der Bürgerinnen und Bürger zu verbessern, werden die Telekommunikationsanbieter, die eine Schlüsselrolle für die Sicherheit des Cyberraums haben, verpflichtet, IT-Sicherheit nach dem Stand der Technik nicht nur zum Schutz des Fernmeldegeheimnisses und zum Schutz personenbezogener Daten, sondern auch im Hinblick auf die Verfügbarkeit ihrer Telekommunikations- und Datenverarbeitungssysteme zu gewährleisten. Die Umsetzung der zugrunde liegenden IT-Sicherheitskonzepte in den Unternehmen wird von der Bundesnetzagentur regelmäßig überprüft. Damit wird die Widerstandsfähigkeit der Kommunikationsinfrastruktur insgesamt verbessert und die Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit datenverarbeitender Systeme sowie der dort vorgehaltenen Daten gesichert. Mittelbar steigt so auch die Verantwortung der Hersteller zum Angebot entsprechender Produkte. Telekommunikationsanbieter sollen zudem IT-Sicherheitsvorfälle, die zu einem unerlaubten Zugriff auf die Systeme der Nutzerinnen und Nutzer oder einer Beeinträchtigung der Verfügbarkeit führen können, unverzüglich über die Bundesnetzagentur an das BSI melden und betroffene Nutzerinnen und Nutzer über bekannte Störungen informieren, die durch Schadprogramme auf den datenverarbeitenden Systemen der Nutzerinnen und Nutzer hervorgerufen werden. Die Betroffenen müssen auf Möglichkeiten zur Problembehebung („zugängliche technische Mittel") hingewiesen werden.

Die Betreiber und Anbieter profitieren, da sie auch die Auswertung dieser Meldungen durch das BSI erhalten.

4. Änderung des Telemediengesetzes: Anbieter von Telemediendiensten wie Webseiten

Hierunter fallen alle Unternehmen, die eine Webseite betreiben – ggf. auch nur mit Informationen für Interessierte! Unter Webseitenbetreiber fallen auch die Unternehmen, die Apps zur Nutzung im Internet bereitstellen.

Um die Verbreitung von Schadsoftware über das Internet einzudämmen (z.B. Drive-by-Downloads), sollen Webseitenbetreiber angebotene Sicherheitskorrekturen (Patches) einspielen.

Kompromittierte Werbebanner sollen durch organisatorische Maßnahmen (Verträge) unterbunden werden.

Diensteanbieter sollen durch technische und organisatorische Vorkehrungen sicherstellen, dass

- kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und
- diese gegen Verletzungen des Schutzes personenbezogener Daten und gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind,

gesichert sind. Vorkehrungen müssen den Stand der Technik berücksichtigen. Eine Maßnahme ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens.

Hier dürfte es sich allein um 3.000.000 betroffene Unternehmen handeln. Verstöße gegen die Pflichten werden mit einem Bußgeld bis zu 50.000 Euro bewehrt.

5. Bußgelder

Bei Zuwiderhandlungen gegen die Meldepflichten und bei Verstößen gegen die Einhaltung angemessener Sicherheitsmaßnahmen drohen den Unternehmen Bußgelder bis zu 50.000 Euro. Bei Verstößen gegen die Anordnung zur Beseitigung eines Sicherheitsmangels kann das Bußgeld bis zu 100.000 Euro betragen.[20]

Diese Bußgeldvorschriften waren im ursprünglichen Entwurf für das IT-Sicherheitsgesetz nicht vorgesehen und sind erst im Laufe des Gesetzgebungsverfahrens auf Intervention des Bundestags-Innenausschuss in das BSI-Gesetz aufgenommen worden. Hierbei wurde versäumt, in den anderen vom IT-Sicherheitsgesetz betroffenen Spezialgesetzen vergleichbare Verschärfungen vorzunehmen. Wenn es dem Gesetzgeber mit seinem Vorhaben tatsächlich ernst ist, wird er diese Lücken in den Bußgeldvorschriften bald schließen. Dann müssen nicht nur große Infrastrukturunternehmen wie Kraftwerk- und Energienetzbetreiber, sondern auch Kleinstunterneh-

20 Angesichts der möglichen Schäden gewiss ein moderater Betrag – insbesondere im Vergleich zu den im BDSG festgelegten Bußgeldern von bis zu 300.000 Euro bei allgemeinen Verstößen.

men, die als Telemediendiensteanbieter eine Website unterhalten, mit einer Erweiterung der Bußgeldkataloge in den für sie einschlägigen Gesetzen rechnen.

Dies könnte insbesondere für Start-ups und KMUs eine erhebliche finanzielle Belastung bedeuten.

6. BSI

Nationale Meldestelle und internationaler Ansprechpartner

Das BSI wird zentrale Meldestelle für Betreiber Kritischer Infrastrukturen in allen Angelegenheiten der Sicherheit in der Informationstechnik und internationaler Ansprechpartner im Bereich der IT-Sicherheit. Das BSI wird dazu nationale Aufsichtsbehörde über die Betreiber von Kritischen Infrastrukturen.

Beratungsaufgaben

Das Bundesamt für Sicherheit in der Informationstechnik kann informationstechnische Produkte und Systeme unter Sicherheitsaspekten untersuchen (lassen) und kann (nicht muss!)

- Warnungen vor Sicherheitslücken in Produkten und Diensten und
- vor Schadprogrammen etc.

veröffentlichen.

Entscheidend ist hier die Möglichkeit der Veröffentlichung von Sicherheitslücken. Dies war bisher auch schon so geregelt. Tatsächlich hat das BSI noch nie eine – bis dahin unveröffentlichte - Sicherheitslücke veröffentlicht. Allerdings stellen gerade die Zero-Day-Vulnerabilities ein Einfallstor in unternehmensweite IT-Systeme dar.

Das BSI kann Betreiber Kritischer Infrastrukturen auf deren Ersuchen bei der Sicherung Ihrer Informationstechnik beraten und unterstützen oder auf qualifizierte Sicherheitsdienstleister verweisen.

7. Maßnahmen der Adressaten

Auch wenn die internationale Norm ISO 27001 als Stand der Technik bezeichnet werden kann, reicht es für viele Unternehmen aus, einfache Standards wie ISA+, ISIS12 anzuwenden. Diese Maßnahmen sollten sofort ergriffen werden, da sie grundlegend für jedes weiterführende Digitalisierungsprojekt sind und die bestehende Struktur absichern.

Sofortmaßnahmen für Telemediendiensteanbieter

- Einspielung von **Sicherheitskorrekturen (Patches**) für alle Produkte (z.B. Standardsoftware wie Betriebssystem, Datenbank etc.), die im Rahmen der Telemediendienste wie Webseiten eingesetzt werden
- IT-Sicherheitsgesetz **Quick Check**: Kurze Prüfung des Sicherheitsniveaus der Telemediendienste wie z.B. eine Webseite mit dem Ziel, die Einhaltung des IT-Sicherheitsgesetzes zu überprüfen
- TLS-**Verschlüsselung** bei Webseiten einsetzen (HTTPS)

Sofortmaßnahmen für Kritische Infrastrukturen

1. Erstellen Sie eine vollständige Risikoanalyse aller Daten und Anwendungen in Ihrem Unternehmen.
2. Lassen Sie von einem unabhängigen (!) Dritten das Sicherheitsniveau Ihrer Anwendungssoftware, Apps und Systeme von Innen und Außen sorgfältig untersuchen. Sorgfältig heißt auf der Basis der ISO 27034 ‚Application Security': Nicht nur Penetration Testing, sondern auch Bewertung des Sicherheitsarchitektur Ihrer Netze, Systeme und Anwendungen wie Webserver etc. sowie Code Reading und Fuzzing.
3. Lassen Sie gleichermaßen auch die Sicherheitsprodukte selbst untersuchen auf zielführende Parametereinstellungen: Firewalls, Verschlüsselung, Intrusion Detection und Protection. Häufig genug ist z.B. eine Firewall oder Verschlüsselung installiert - per Parameter sind aber sicherheitsrelevante Funktionen abgeschaltet.
4. Chef-Thema: Beschäftigen Sie sich persönlich mit IT-Sicherheit. Es ist genauso wichtig wie Ihre Finanzierung und Ihr Cash-Flow! Letztlich hängt dies wiederum zunehmend von der Sicherheit Ihrer Systeme ab.

Weitergehende Maßnahmen aus dem IT-Sicherheitsgesetz

- Warten Sie nicht erst die 2-Jahresfrist ab, bis zu der Sie agieren müssen. Warten Sie aber die Veröffentlichung der Rechtsverordnung ab, die festgelegt, welche Unternehmen überhaupt unter das Gesetz fallen und welche Anforderungen an die Prüf- und Zertifizierungsverfahren sowie die zu erbringenden Nachweise gestellt werden.

- Schauen Sie sich die Empfehlungen Ihres Branchenverbandes[21] an. Gemäß Gesetzestext können Betreiber Kritischer Infrastrukturen und ihre Branchenverbände branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen dem BSI vorschlagen und deren Eignung feststellen lassen.
- Betreiber von Kernkraftwerken und Telekommunikationsanbieter müssen bereits jetzt erhebliche IT-Sicherheitsvorfälle melden. Für sonstige Betreiber kritischer Infrastrukturen aus den Bereichen Energie, Informationstechnik, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen gilt dies erst, wenn die Einzelheiten regelnde Rechtsverordnung in Kraft tritt. Das Bundesinnenministerium bereitet dazu nach eigenen Angaben derzeit einen Entwurf vor. Parallel sollen gemeinsam mit der Wirtschaft Mindeststandards zur IT-Sicherheit erarbeitet werden.
- Drängen Sie in Ihrem Branchenverband auf die Entwicklung Branchen-einheitlicher Mindestmaßnahmen, die der Verband auch mit dem BSI abstimmen könnte.

Kosten

Für kleine und mittlere Unternehmen werden als erste Maßnahme speziell auf die Anforderungen des IT-Sicherheitsgesetzes zugeschnittene Quick-Checks der Webseite oder einer App schon für dreistellige Beträge angeboten.

Bei größeren Unternehmen – besonders im Umfeld Kritischer Infrastrukturen muss eine individuelle Kostenabschätzung mit individuellem Leistungsumfang vorgenommen werden.

Aufwand der Meldepflicht

Die konkrete Berechnung der Gesamtkosten kann erst mit Erlass der Rechtsverordnung erfolgen, da in ihr der Adressatenkreis der entsprechenden Verpflichtungen hinreichend konkret eingegrenzt und eine entsprechende Zahl meldepflichtiger Betreiber Kritischer Infrastrukturen benannt werden kann. Nach aktuellen Schätzungen wird die Zahl der meldepflichtigen Betreiber Kritischer Infrastrukturen auf maximal 2.000 Betreibern beziffert.

Weiterhin wird geschätzt, dass pro Betreiber maximal sieben Meldungen von IT-Sicherheitsvorfällen pro Jahr erfolgen. Auf Grund von Angaben aus der Wirtschaft auf der Grundlage von Berechnungen nach dem Standardkostenmodell werden die Kosten für die Bearbeitung einer Meldung derzeit mit 660 Euro pro Meldung (11 Stunden Zeitaufwand bei einem Stundensatz von 60 Euro) beziffert. Legt man den Berechnungen eine Anzahl von 2.000 Betreibern Kritischer Infrastrukturen zugrunde, die jeweils sieben IT-Sicherheitsvorfälle pro Jahr melden, für deren Bearbeitung jeweils ein zusätzlicher Aufwand von 660 Euro pro Meldung entsteht, so entsteht den Betreibern Kritischer Infrastrukturen für die Erfüllung der Meldepflicht ein jährlicher Erfüllungsaufwand von insgesamt 9,24 Millionen Euro. Zum Teil werden solche Vorfälle allerdings schon heute dem BSI gemeldet.

Dies sind naturgemäß Schätzungen. Auch die Stundensätze von 60 Euro sind eher illusorisch, da die Personalkosten in der IT deutlich ansteigen werden. Weiterhin ist mit weiter fortschreitender Digitalisierung ein überproportionaler Anstieg der Meldungen zu erwarten.

Insgesamt wird die juristische und gleichermaßen auch die technische Prüfung darauf unverzichtbar, ob ein Unternehmen vom Gesetz betroffen ist und ob die Qualität der getroffenen Sicherheitsmaßnahmen den Forderungen des Gesetzes angemessen entspricht.

Haftung

Es ist zu erwarten, dass Kunden und Vertragspartner Schadenersatz für Störungsfolgen fordern, wenn die aus dem Gesetz folgenden Sicherheitsmaßnahmen nicht oder nur unzulänglich umgesetzt wurden.

Geschäftsführer und Vorstände dürften aus § 43 GmbHG und § 91 ff. AktG (KonTraG) persönlich haften.

8. Kritik und Verbesserungsvorschläge

Ob das IT-Sicherheitsgesetz in seiner derzeitigen Form geeignet ist, einen erheblichen Beitrag zur Verbesserung der IT-Sicherheit zu leisten, wird insbesondere von IT-Sicherheitsexperten bezweifelt.

Auch datenschutzrechtlich stößt das IT-Sicherheitsgesetz auf Bedenken, da es durch die Änderung in § 100 Abs. 1 TKG eine weitgehende Erlaubnis für Telekommunikationsanbieter vorsieht, Daten über das Verhalten der Nutzer zu speichern. Es wird befürchtet, dass auf diesem Wege eine Vorratsdatenspeicherung „durch die Hintertür" eingeführt wird.

[21] Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifisch Sicherheitsstandards zur Gewährleistung der Anforderungen vorschlagen. Auf Antrag stellt das BSI fest, ob sie geeignet sind.

Seit der Gründung 1991 wird dem Bundesamt für Sicherheit in der Informationstechnik unterstellt, wichtige Informationen wie z.B. unveröffentlichte Sicherheitslücken den Unternehmen und generell der Öffentlichkeit zum Eigenschutz vorzuenthalten zugunsten anderer Sicherheitsbehörden wie dem Bundesamt für Verfassungsschutz, dem Bundeskriminalamt und dem BND – demzufolge können sich Unternehmen nicht gegen Spionage- und Sabotageangriffe schützen!

Insgesamt wird leider nur ein unzureichendes Sicherheitsniveau erreicht – insbesondere in den wichtigen Unternehmen der Kritischen Infrastrukturen aber auch bei Privatpersonen: Nach wie vor hält der Gesetzgeber es nicht für nötig, bisher unveröffentlichte Sicherheitslücken (Zero-Day-Vulnerabilities) zu veröffentlichen. Das BSI hat nach dem Gesetz zwar die Aufgabe, Sicherheitslücken zu sammeln und auszuwerten, muss sie aber nicht veröffentlichen und tut es auch nicht.

Durch Ausnutzung von Sicherheitslücken werden Hacking-Angriffe, Phishing-Attacken, Wirtschaftsspionage und -sabotage erst möglich mit der Folge von Verlusten in Unternehmen in Milliarden Euro Höhe – und mit der mittelbaren Folge des Wegfalls von Arbeitsplätzen und Steuern!

Während international die organisierte Kriminalität Millionen-fache Gewinne mit dem Insider-Handel unveröffentlichter Sicherheitslücken auf dem schwarzen Markt einstreicht, bleibt der Gesetzgeber also auf seinem Standpunkt, Sicherheitslücken müssten nicht veröffentlicht werden. Dies führt dazu, dass deutsche Unternehmen und Privatpersonen den IT-Angriffen schutzlos ausgeliefert sind und bleiben.

Inzwischen haben die 70 weltgrößten Softwareunternehmen erkannt, dass IT-Angriffe erfolglos sind, wenn keine ausnutzbaren Sicherheitslücken vorhanden sind, und fördern konsequenterweise die Veröffentlichung bislang nicht erkannter Sicherheitslücken!

Zur Erreichung eines angemessenen Sicherheitsniveaus – insbesondere in den Unternehmen der Kritischen Infrastrukturen ist die Veröffentlichung der den Sicherheitsbehörden bekannten bislang unveröffentlichten Sicherheitslücken unverzichtbar. Nur so können sich Unternehmen und Privatpersonen nachhaltig gegen die derzeit ständig zunehmenden IT-Angriffe schützen. Hier sollte der Gesetzgeber zeitnah nachbessern!

Eine Regulierung der IT-Sicherheit bei Kritischen Infrastrukturen ist schon lange überfällig – dies zeigen die vielfältigen Angriffe durch Nachrichtendienste und insbesondere die Organisierte Kriminalität. Auch der Ausbau der Kompetenzen des BSI und dessen zentrale Rolle bei der Prävention, Auswertung und Bekämpfung von Angriffen erscheint im Grundsatz unverzichtbar.

Völlig unbestimmt ist der Begriff der „Störung", die Meldepflicht auslöst. Hier hätte der Gesetzgeber eine Meldung der ursächlichen Sicherheitslücken festschreiben müssen. Tatsächlich kann ein Angriff ja nur erfolgreich sein, wenn er eine Sicherheitslücke ausnutzt. Der Gesetzgeber tut sich hier offensichtlich schwer, weil insbesondere die dem BSI bekannten unveröffentlichten Sicherheitslücken (Zero-Day-Vulnerabilities) an das BKA etc. zur Durchführung der ‚heimlichen Online-Durchsuchung' und der Quellen-TKÜ – auch mit dem sog. Bundestrojaner weitergegeben werden; dies widerspricht natürlich einer Veröffentlichung. Letztlich muss sich der Gesetzgeber aber entscheiden, ob er den Schutz der Unternehmen und damit der Arbeitsplätze und des Steueraufkommens niedriger einschätzt als die Überwachungsmöglichkeit durch die Sicherheitsbehörden in Bereichen.

All dies ist im Vorfeld bereits kritisiert worden, zu einer klaren und überzeugenden Antwort konnte sich der Gesetzgeber gleichwohl nicht durchringen. Damit bleibt das Gesetz nur Stückwerk und wird (hoffentlich bald) novelliert werden.

Wieweit das BSI über seine im Grundschutz-Handbuch bzw. der ISO 27000-Familie beschriebenen Sicherheitsforderungen tatsächlich hinausgeht bleibt abzuwarten. Eine ganze Reihe von Unternehmen der Kritischen Infrastrukturen weisen jedenfalls bereits heute ein angemessenes IT-Sicherheitsniveau auf.

Darüber hinaus enthält das IT-Sicherheitsgesetz viele Formulierungen und Verpflichtungen deren praktische Auswirkungen ungewiss sind und die in ihrer Unbestimmtheit dem BSI letztlich einen sehr weiten Interpretationsspielraum zugestehen.

Zusammenfassend kann gesagt werden, dass das Gesetz einen Einstieg in die Absicherung gegen Angriffe aus dem Internet bietet – allerdings auch nicht mehr.

"Freiwillige Vorratsdatenspeicherung"

Auch datenschutzrechtlich stößt das IT-Sicherheitsgesetz auf Bedenken, da es durch die Änderung in § 100 Abs. 1 TKG eine weitgehende Erlaubnis für Telekommunikationsanbieter vorsieht Daten über das Verhalten der Nutzer zu speichern. Es steht zu befürchten, dass auf diesem Wege eine Vorratsdatenspeicherung „durch die Hintertür" eingeführt wird. Die sich daraus entwickelnde politische Diskussion und ggf. verfassungsrechtliche Klärung könnte Verzögerungen ergeben.

Provider dürfen zudem Verbindungsdaten speichern, um Störungen abzuwehren. Dies führt derzeit zu einer "freiwilligen Vorratsdatenspeicherung" zwischen drei Tagen und sechs Monaten, die Bürgerrechtler seit Langem scharf kritisieren. Diese Befugnis hat der Bundestag trotzdem auf Fälle ausgedehnt, in denen Probleme mit Cyberattacken oder Spam nur am Horizont auftauchen können. Dem Bundesrat war diese Bestimmung zunächst ein Dorn im Auge, er ließ sie aber Anfang Juli trotzdem passieren.

Hier bleibt derzeit nur zu hoffen, dass sich eine einheitliche und handhabbare Aufsichtspraxis des BSI herausbildet, die das BSI dann auch offen kommuniziert – vergleichbar der MaRisk im bankaufsichtsrechtlichen Bereich oder der ‚Orientierungshilfe Cloud Computing' im datenschutzrechtlichen Bereich.

Wenig glücklich erscheint darüber hinaus, dass das IT-Sicherheitsgesetz unabhängig von der sich abzeichnenden EU Richtlinie zur Netz- und Informationssicherheit (NIS)[22] beschlossen wurde. Soweit die NIS mit von dem IT-Sicherheitsgesetz abweichenden Inhalten beschlossen wird, könnte schon kurz nach dessen Inkrafttreten eine Revision des IT-Sicherheitsgesetzes notwendig werden.

9. Zur Zukunft der Arbeit unter dem IT-Sicherheitsgesetz

Die Zukunft der Arbeit wird in Deutschland zunehmend von zwei Aspekten geprägt sein, die beide der Digitalisierung unterliegen werden. Einerseits den älter werdenden Mitarbeitern, die diese Digitalisierung noch mitgestalten werden (müssen!) und denen, die als digital natives bezeichnet werden und mit nichts anderes groß geworden sind als der Illusion alles wäre a) sicher und b) umsonst.[23]

Wir werden in den nächsten zehn bis fünfzehn Jahren nicht nur alternde Belegschaften haben, die zunehmend empfindlicher auf Stress reagieren werden und damit für Fehler und „Routinedelikte" in der IT-Sicherheit anfälliger werden, sondern auch damit, dass durch die Digitalisierung zahlreiche bisher nicht betroffene Berufsgruppen im Fokus genau dieser Digitalisierung stehen werden. Durch künstliche Intelligenz werden nun auch kognitive Berufe, wie Buchhalter, Versicherungskaufleute und Bankangestellte zunehmend überflüssiger werden, soweit Dienstleistungen auch virtuell/online erbracht werden können. Dieser Prozess wird schleichend sein. Genauso schleichend aber selbstverständlich, wie wir uns an Telefoncomputer und Onlinehandel gewöhnt haben. Oder was das betrifft an Apps und die mobile Version des Internets. Sie haben unsere Gesellschaft verändert. Und mit ihr die Wirtschaft.

Die Tendenz, kostenverursachende Maßnahmen ohne (bilanziell) erkennbare Gewinnrealisierung erst bei hinreichender Gesetzesnotwendigkeit anpacken zu wollen, hat schon bei der Einführung von beispielsweise SEPA zu unerfreulichen Erkenntnissen geführt. IT-Sicherheit ist nämlich nicht nur ein Problem der IT-Abteilung. Es ist ein Problem der Wahrnehmung als Risikofaktor für den Unternehmenserfolg. Dieser wird gerade in der Anfangsphase der Gesetzgebung und im zu erwartenden weiteren Gründungsschub im Bereich der Digitalisierung kaum abzuschätzen sein, wenn sich Geschäftsmodelle mit Betreibern Kritischer Infrastrukturen verknüpfen.

Die Digitalisierung wird Prozesse und Abläufe zum Teil drastisch beschleunigen. Datenmengen werden durch Komprimierung und große Leitungsquerschnitte innerhalb von Sekundenbruchteilen transferiert werden können. Daten, die mitunter sicherheitsrelevant, vertraulich und geschäftsgefährdend sind, sobald sie in falsche Hände kommen. Nicht falls. Denn wer ein „Falls" diskutieren will, muss verstehen, dass das, was das IT-Sicherheitsgesetz in der aktuellen Version vorgibt, bestenfalls ein Vorstopper ist. Ein Vorstopper auf etwas, was mit wachsender Vernetzung/Digitalisierung wie eine Lawine auf uns zu rollen wird. Eigentlich schon jetzt zurollt. Uns überrollt.

Das IT-Sicherheitsgesetz hat noch nicht einmal die Qualität eines einfachen Fangzauns. Risikotechnisch gesehen ist es eine bessere Absichtserklärung auf spätere grundlegende Verbesserungen. Aber ohne den Betreiber aus der Haftung zu nehmen.

Da wir alle, als Menschen wie auch als Wirtschaft, gewinnorientiert arbeiten und denken, ist die Digitalisierung zuallererst eine Chance auf bessere Erlöse, schnelleren Kapitalfluss, bessere Kundennähe, höhere Kundenfreundlichkeit/-akzeptanz und insgesamt besser vernetzte interne Prozesse.

Im DACH-Raum bedeutet es auch, alternden Belegschaften Hilfsmittel an die Hand zu geben, die einerseits ein Arbeiten im Alter von immer rarer werdenden Fachkräften überhaupt erst möglich zu machen und ihren dann späteren Totalwegfall aufzufangen. Allein in Deutschland werden in 40 Jahren bis zu 15 Millionen Menschen fehlen. Das produktionstechnisch aufzufan-

---

22 ‚Vorschlag für eine Richtlinie des europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union' Brüssel 2013 http://www.bundesanzeiger-verlag.de/fileadmin/Betrifft-Recht/Dokumente/externe%20dokumente/COM_2013__48_final.pdf

23 Vgl.: Prof. Dr. Hartmut Pohl / Sascha Rauschenberger: Future Work und IT-Sicherheit: Verdrängte Risiken für die Arbeitswelt der Zukunft - Das Dilemma moderner Arbeitsorganisationen, Conplore Media (2015); https://conplore.com/future-work-und-it-sicherheit-verdraengte-risiken-fuer-die-arbeitswelt-der-zukunft-future-work-and-it-security/

gen und erlöstechnisch zu gestalten wird ein Punkt sein, der durch Digitalisierung sicher gestaltbar ist.

Doch diese Gestaltung muss unter dem gleichen Gesichtspunkt erfolgen, wie eine Absicherung der Produktionsstätte an sich. Kein Unternehmer verzichtet daher auf einen Zaun um das Produktionsgelände, Überwachungs- und Alarmanlagen und Türschlösser. Doch im abstrakten Wahrnehmungsumfeld der IT wird eben das gern und schnell vergessen.

Datenverluste sind heute genauso vorhanden wie die Inventurverluste im klassischen Handel. Nur werden sie nicht durch eine Inventur erfasst. Zum Teil daher auch gar nicht erkannt. Und diese Verluste werden zunehmen, weil die Angriffspunkte drastisch zunehmen. Nur ein einziges Beispiel sind hier die Apps![24]

Daher ist Digitalisierung und IT-Sicherheit erst zusammen das, was Visionäre gerne als die Chance verkaufen: Umsatzsteigerung, Flexibilität, Marktnähe, Prozessoptimierung und Produktivitätssteigerung.

Der Bundestag hat dies nun scheinbar herausgefunden, der noch nicht einmal mehr seine Admin-Rechte im Griff hatte und auch nicht Frau Kanzlerin Merkel, deren „sicheres" Handy wohl doch nicht so ganz sicher war.

Und das wird nicht besser werden, solange sich nicht jeder klar macht, dass er mitverantwortlich ist für das, was am Ende rauskommt. Und diesen Job, kann Ihnen auch die Digitalisierung nicht abnehmen: die Eigenverantwortlichkeit für das Risikomanagement; immer, überall und gegen jeden!

Es ist erfreulich, dass dieses Ziel nun eine gesetzliche Grundlage gefunden hat. Es wurde höchste Zeit, trotz aller o.g. Mängel/Herausforderungen. Es wurde Zeit, den oft wenig beliebten IT-Sicherheitsmanagern auch eine gesetzliche Handhabe zu geben und auch ein kaufmännisches Argument: Die vollumfängliche Haftung für Verstöße und Vorkommnisse. Es ist also höchste Zeit, dass sich die Chefetagen neben den Chancen der Digitalisierung auch die Risiken bewusst machen, die diese Technik zwangsläufig mit sich bringt.

[24] Vgl.: Pohl, Hartmut; Rauschenberger, Sascha: Future Work und mobile Arbeitsplattformen mit Apps: Risiken für die Wirtschaft, Conplore Media (2015); https://conplore.com/future-work-und-mobile-arbeitsplattformen-mit-apps-risiken-fuer-die-wirtschaft/