Fachhochschule
Kaiserslautern
University of Applied Sciences

Betriebswirtschaft
Zweibrücken

Handout

Fachbereich Betriebswirtschaft

Studiengang Information Management

Business Value of IT

WS 2013/2014

IT-Security:
Auswirkungen des NSA-Skandals

Vorgelegt von: Tim Beckmann

Thorsten Heck

Vorgelegt bei: Herr Prof. Dipl.-Ing. Klaus Knopper

Abgabe: 08.11.2013

1. Einleitung

Im Zeitalter der vernetzten Gesellschaft ist der Umgang und die damit einhergehenden Probleme, mit personenbezogenen Daten, seit langem ein Dauerthema, welches zur Verifizierung diverser Gesetze zum Schutz der selbigen führte. Deren Wirkungsgrad ist jedoch, aufgrund des urbanen Charakters des Internets, als äußerst beschränkt anzusehen. Die Enthüllungen des Whistleblowers Edward Snowden im Sommer 2013 verdeutlichten den massiven Umfang des Abhörens und der Speicherung von Daten die unter dem Schutzmantel der Terrorismusbekämpfung durchgeführt werden. Dabei beschränkt sich die Überwachung von Internet- und Telefondaten nicht nur auf die privaten Haushalte, sondern durchdringt auch die Unternehmenswelt und staatliche Stellen. Vor allem aus Unternehmenssicht hängt jedoch von der „Vertraulichkeit des Wissens“ die Wettbewerbsfähigkeit ab, welche zugleich die Existenzgrundlage des Unternehmens bildet. Dies erfordert unter Berücksichtigung des Kosten-Nutzen-Verhältnis eine Evaluation der bestehenden Informationssicherheit, insbesondere unter dem Aspekt der Wirtschaftsspionage, da es nicht auszuschließen ist, dass die von Geheimdiensten erhobenen und gespeicherten Daten, an Konkurrenzunternehmen weitergegeben werden.

2. Definitionen und Abgrenzungen

Mit IT-Sicherheit wird die Fähigkeit eines Systems, Informationen und Systemressourcen in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit zu schützen, bezeichnet.[1] Die Aufgaben des IT-Security-Managements sind dabei vielfältig und durchdringen den gesamten Organisationskomplex. Beispielsweise beschäftigt sich das IT-Risikomanagement u.a. mit der Notfallvorsorge, Berechtigungsvergabe oder die Entscheidung für und wider einer Softwareanschaffungen und durchdringt somit wiederum andere Teilbereiche der IT-Security.[2] Die Organisation, IT-Compliance, Awareness und Schulungen können zudem als Fundament der IT-Sicherheit angesehen werden, da gleich welche Maßnahmen auch zu implementieren sind oder welche Richtlinie durchgesetzt werden muss, immer wieder die Frage der Kommunikation und Schulung berührt ist und wie die IT-Security-Organisation auszusehen hat, um dies auch bewältigen zu können.[3]

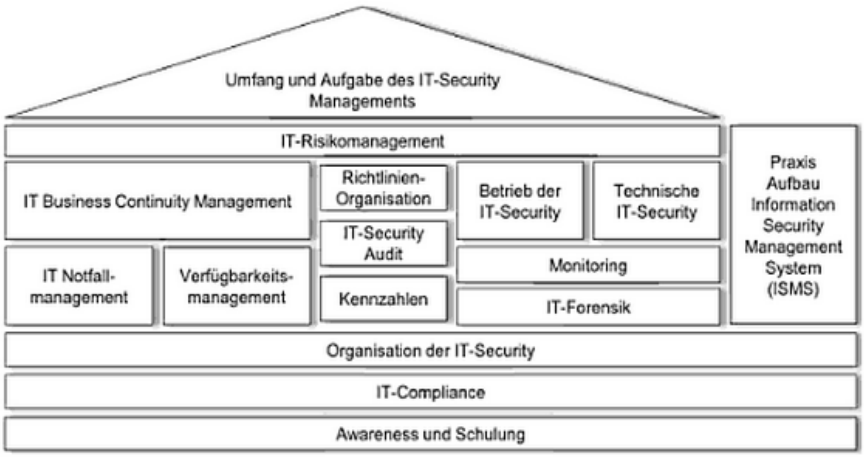

Abbildung 1: IT-Security-Management - Umfang und Aufgaben[4]

Dabei ist die IT-Sicherheit als ein Prozess anzusehen, der mittels Regelwerken durchgeführt und unterstützt werden kann.[5] Exemplarisch sind aus dem aktuellen Fundus einige der bekanntesten Rahmenwerke bzw. Normen in folgender Tabelle aufgeführt.

[1] Vgl. Jenkins (2010), S. 20.
[2] Vgl. Harich (2012), S. 17.
[3] Vgl. Harich (2012), S. 17.
[4] Harich (2012), S. 16.
[5] Vgl. Schoolmann/Rieger (2005), S. 388.

Framework/Norm[6]	Bezeichnung	Definition	Kurzbeschreibung
COBIT	Control Objectives for Information and Related Technology	IT-Governance Framework	Gliedert die Aufgaben der IT in Prozesse und Steuerungsvorgaben
ITIL	IT Infrastructure Library	Sammlung von Best Practices zur Umsetzung des IT-Service-Mangements	Beschreibung der zum Betrieb der IT-Infrastruktur notwendigen Prozesse, Aufbauorganisation und Werkzeuge
ISO-27001	Information technology Security techniques	Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, und Verbesserung eines ISMS	DIN-Norm spezifiziert Anforderungen für Implementierung von geeigneten Sicherheitsmechanismen zur Adaption an die Organisation
ISO-27002	s.o.	Empfehlung von Kontrollmechanismen für Informationssicherheit	Sammlung von Vorschlägen
BSI-Grundschutz	IT-Grundschutzkatalog	Dokumentensammlung des Bundesamt für Informationstechnik (BSI)	Erkennung und Bekämpfung sicherheitsrelevanter Schachstellen in IT-Umgebungen

Das BSI stellt u.a. mit Standard 100-2 in Verbindung mit dem IT-Grundschutz-Katalog ein umfassendes Rahmenwerk zur Umsetzung eines Informationssicherheitsmanagementsystems (ISMS) vor, welches in den Phasen des Sicherheitsprozesses z. B. auch die Relevanz von Leitlinien und die Integration der Mitarbeiter hervorhebt.

Mit eCrime wird die Ausführung von wirtschaftskriminellen Handlungen unter Einsatz von Informations- und Kommunikationstechnologien zum Schaden einer Einzelperson, eines Unternehmens oder einer Behörde bezeichnet.[7] Im Gegensatz zu Cybercrime, das sich mit Verbrechen bzw. Vergehen die in Zusammenhang mit dem Internet stehen beschäftigt und somit neben kriminellen wirtschaftlichen Handlungen auch strafbare Phänomene aus anderen Bereichen wie beispielsweise Stalking beinhaltet.[8] Jedoch beschränkt sich Cybercrime ausschließlich auf den Webspace. Die mit Internetkriminalität verbunden Kosten steigen seit Jahren kontinuierlich an und beliefen sich im Jahr 2012 laut KPMG in Deutschland auf vier Milliarden USD (113 Mrd. weltweit). Dabei wurden weltweit 38 % der User, welche ihre elektronischen Endgeräte sowohl privat als auch geschäftlich Nutzen (insgesamt 49%) Opfer eines Cybercrime. Jedoch insbesondere der Datendiebstahl konnte 2012 gegenüber 2010 drastisch reduziert werden.[9]

Das Ausspähen „wertvoller" Informationen ist keineswegs ein Phänomen des Internetzeitalters, sondern geht einher mit der Staatenbildung und der Bildung von wirtschaftlichen Organisationen. Dabei gilt es die Wirtschaftsspionage, als staatlich gelenkte oder gestützte Ausforschung von Wirtschaftsunternehmen oder Forschungseinrichtungen von der Konkurrenzspionage, welche die Ausforschung von Wirtschaftsunternehmen oder Forschungseinrichtungen durch privatwirtschaftliche Institution oder Privatpersonen bezeichnet, abzugrenzen.[10] Während die Wirtschaftsspionage durch fremde Geheimdienste initiiert wird, kann die Industriespionage, von allen anderen Individuen bzw. Organisationen ausgehen. Im Rahmen der Prävention ist bei der Wirtschaftsspionage primär der Verfassungsschutz zuständig, während bei der Konkurrenzspionage die Unternehmensleitung geeignete Maßnahmen veranlassen muss.[11]

3. IT-Sicherheit aus rechtlicher Sicht

Neben den o.g. Rahmenwerken und Normen stellt die geltende Rechtsprechung in Deutschland einen weiteren Schutz wirtschaftlicher Interessen dar. Wobei rechtliche Aspekte auch in den genannten Frameworks Berücksichtigung finden. Das IT-Sicherheitsrecht umfasst alle Regelungen und Bestimmungen, deren Ziel die Sicherheit von Daten und IT-Systeme ist. Die sind im Detail die Aspekte Verfügbarkeit, Vertraulichkeit und Integrität

[6] Vgl. BSI (2009), S. 9ff.
[7] Vgl. KPMG (2013), S. 11.
[8] Vgl. Gabler Wirtschaftslexikon.
[9] Vgl. Symatec-Norton Report (2013), o.S.; KPMG (2013), S. 15.
[10] Vgl. Bundesamt für Verfassungsschutz (2008), S. 5; Hlavica (2011), S. 58.
[11] Vgl. Hlavic (2011), S. 58.

von Daten.[12] Die folgende Tabelle zeigt einen Ausschnitt der zahlreichen gesetzlichen Bestimmungen im Rahmen der IT-Security.

Gesetze[13]	**Auszug**
Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)	Pflicht eines Früherkennungssystem für Risiken
Bundesdatenschutzgesetz (DBSG)	Angemessener Schutz personenbezogener Daten
Teledienstedatenschutzgesetz (TDDSG)	Technische und organisatorische Sicherstellung der Dienstnutzung gegen Kenntnisnahme Dritter
Telekommunikationsgesetz (TKG)	Fernmeldegeheimnis Es ist untersagt, sich Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation, über das für die geschäftsmäßige Erbringung erforderliche Maß hinaus, zu verschaffen.
Wertpapierhandelsgesetz (WpHG)	Führen von Verzeichnissen über Personen mit Insiderwissen
Singnaturgesetz (SigG)	Schutz vor unberechtigter Kenntnisnahme, Fälschung und Manipulation elektronischer Dokumente
Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS)	Vollständigkeit, Richtigkeit, Zeitgerechtigkeit, Ordnung, Nachvollziehbarkeit, Unveränderlichkeit Sensible Daten sind gegen unberechtigte Kenntnisnahme zu sichern

Im Kontext des Strafgesetzbuches (StGB) und des Gesetzes gegen den unlauteren Wettbewerb (UWG) finden sich zahlreiche Paragrafen, welche die Problematik der IT-Security aufgreifen und die Grundlage der strafrechtlichen Verfolgung darstellen. Insbesondere der § 99 des StGB bezieht sich auf die geheimdienstliche Agententätigkeit und kann bis zu 10 Jahre Freiheitsstrafe in besonders schweren Fällen (z. B. Weitergabe von Erkenntnissen einer amtlichen Stelle, Geheimnisse die eine verantwortliche Stellung impliziert oder bei schweren Nachteilen für die BRD) führen.[14] Üblich sind jedoch bei den im Folgenden aufgeführten Gesetzen bzw. bei einem Verstoß Geldstrafen aber auch Haftstraßen von bis zu 5 Jahren. Jedoch beweisen die historischen Vorfälle (Enercon), das eine Verfolgung durch die Strafbehörden bzw. durch den Bundesverfassungsschutz insbesondere bei NSA-Agenten keine adäquaten Lösungen für Unternehmen darstellen und deren notwendiger Schutz in Frage gestellt werden kann.[15]

Paragraf und Gesetz im Kontext der IT-Security[16]	
Paragraf/Gesetz	**Titel**
Allgemein	
§ 99 StGB	Geheimdienstliche Agententätigkeit
§ 17 II UWG	Betriebsspionage
§ 18 UWG	Verwertung von Vorlagen
§ 19 UWG	Verleiten und Erbieten zum Verrat
Vertraulichkeit	
§ 202a StGB	Unbefugtes Ausspähen von Daten
§ 202b StGB	Abfangen von Daten
§ 202c StGB	Vorbereiten des Ausspähens und Abfangen von Daten
§ 203 StGB	Verletzung von Privatgeheimnissen
§ 17 I UWG	Verrat von Geschäfts- und Betriebsgeheimnissen (beschäftigte Personen im UN)
§17 II UWG	Die unbefugte Geheimnisverwertung (Jedermann)
Integrität und Authentizität	
§ 263a StGB	Computerbetrug
§ 265a StGB	Erschleichen von Leistungen
§ 268 StGB, § 269 StGB	Fälschung technischer Aufzeichnungen, Fälschung beweiserheblicher Daten
§ 270 StGB	Täuschung im Rechtsverkehr bei der Datenverarbeitung
§ 303a StGB	Datenveränderung
Verfügbarkeit	
§ 303b StGB	Computersabotage

[12] Vgl. SAP AG (2007), S. 10ff.
[13] Vgl. SAP AG (2007), S. 11ff.
[14] Vgl. Bundesministerium der Justiz (2011), o.S.
[15] Vgl. Zeit Online (1988), o.S.
[16] Vgl. Bundesministerium der Justiz (2004/2011), o.S.

4. Staatliches eCrime

Durch Enthüllungen werden immer mehr staatliche Programme zur globalen Überwachung des gesamten Datenverkehrs bekannt. „Echelon“ ist ein globales elektronisches Aufklärungssystem, welches den gesamten E-Mail-, Telefon-, Fax- und Telexverkehr ungefiltert abhört, der weltweit über Satelliten weitergeleitet wird.[17] Auch „PRISM“ dient der Überwachung der weltweiten Onlinekommunikation (E-Mails, Bilder, Videos etc.) von Nutzern der US-Internetdienste wie z. B. Google (YouTube, Gmail), Facebook und Microsoft (Skype). Die National Security Agency der USA Verwendung dazu vermutlich „Ausleitungsschnittstellen“, welche eine Weitergabe der Daten an den Geheimdienst ermöglichen. Es wird davon ausgegangen, dass die NSA somit direkter Zugriff auf die Daten erhält.[18] Das System „XKeyscore“ der NSA dient wahrscheinlich der Durchsuchung Inhalte digitaler Kommunikation. Die Daten können dabei in Echtzeit erfasst werden und darüber hinaus durch eine automatische Indexierung von Mitarbeiter der NSA durchsucht werden. Ziel soll es bei diesem System sein, Zusammenhänge bei der weltweiten Kommunikation herzustellen.[19] Der britische Geheimdienst betreibt mit dem Spionageprogramm „Tempora“ vermutlich ein Gegenstück zu PRISM, welches dieses in den Ausmaßen sogar übertreffen könnte. Auch hier werden Internetknotenpunkte angezapft um bis zu 95% des weltweiten Datenverkehrs abhören zu können. Großbritannien ist darüber hinaus Teil einer Spionageallianz zwischen den USA, Großbritannien, Kanada, Australien und Neuseeland.[20] Es wird vermutet, dass all diese Spionageprogramme nicht nur zum Schutz vor Terrorismus eingesetzt werden, sondern auch einen wichtigen Teil zur Wirtschaftsspionage beitragen.

5. Erkennung und Prävention

In Deutschland wird von Schäden durch eCrime für die Unternehmen, nach einer Umfrage durch KPMG, von mehr als 1 Million Euro pro Einzelfall ausgegangen. Ein Viertel davon wird durch Ermittlungs- und Folgekosten verursacht. Dabei besteht in den Unternehmen teilweise eine hohe Diskrepanz zwischen Empfunden Risiko und der tatsächlich festgestellten Schadenshöhe. Besonders das Risiko von Systembeschädigungen, Computersabotage und Erpressung wird unterschätzt.[21] Als Täter des eCrime lassen sich mit 75 Prozent vor allem unbekannte Externe feststellen. Aber auch interne Mitarbeiter der betroffenen Abteilung sind zu 25 Prozent an der Tat beteiligt.[22]

Bei der Prävention muss zwischen technischen und menschlichen Faktoren unterschieden werden. Allem voran ist eine Bereichsübergreifende Zusammenarbeit und eine zentrale Steuerung der Maßnahmen bei der Bekämpfung von eCrime unerlässlich. Auf der Mitarbeiterseite ist es besonders wichtig, eine Sensibilisierung gegen Unachtsamkeit und fehlendes Risikobewusstsein vorzunehmen. Dabei muss eine Sicherheitskultur im Unternehmen geschaffen werden, welche in Verhaltensgrundsätzen verankert wird, um die Gefahr durch menschliche Fehler und Unachtsamkeit zu minimieren. In direkter Verbindung dazu stehen die technischen Einrichtungen. Die IT-Systeme müssen bestmöglich vor Angriffen geschützt werden. Besonders kritische Unternehmensbereiche, wie z. B. die Forschung und Entwicklung, sollten komplett von öffentlichen Netzen getrennt werden. Darüber hinaus sind allgemeine Vorschriften für den Umgang mit den Unternehmensdaten notwendig. So zum Beispiel, dass die Zugriffsmöglichkeiten und die Weitergabe von Daten technische beschränkt werden.[23] Ist es dennoch notwendig, Daten an die Unternehmensumwelt weiterzuleiten, sollten hierzu Sicherheitskonzepte beachtet werden.

Beispielhaft lassen sich hier vier grundsätzliche Konzepte aufführen.[24] Bei der symmetrischen Verschlüsselung werden die Daten mit einem zuvor ausgetauschten geheimen Schlüssel ver- und entschlüsselt. Die benötigte

[17] Vgl. Radic (2001), S. 101.
[18] Vgl. Beuth/Biermann (2013), o.S.
[19] Vgl. Lischka/Stöcker (2013), o.S.
[20] Vgl. Handelsblatt (2013), o.S.
[21] Vgl. KPMG (2013), S. 23.
[22] Vgl. KPMG (2013), S. 26.
[23] Vgl. BSI (2012), S. 40ff.
[24] Vgl. Lauert (2010), o.S.

Rechenleistung ist hierbei gering. Bei der asymmetrischen Verschlüsselung kommt ein zusammengehörendes Schlüsselpaar zum Einsatz. Dazu gibt der Empfänger dem Sender seinen öffentlichen Schlüssel bekannt, mit dem dieser eine Nachricht verschlüsseln kann. Nur der Empfänger mit dem passenden privaten Schlüssel kann diese Nachricht wieder entschlüsseln.

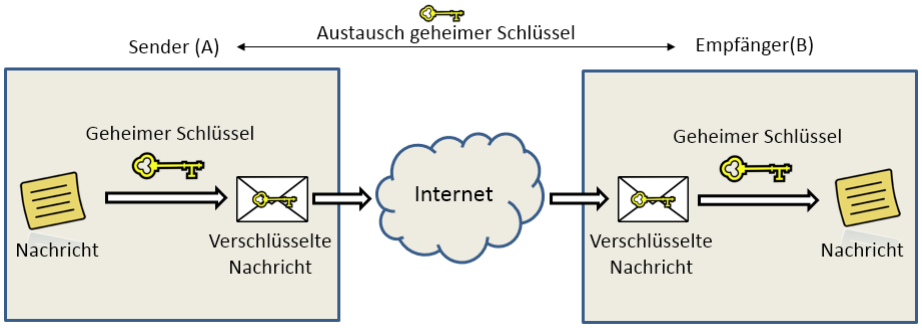

Abbildung 2: Symmetrische Verschlüsselung[25]

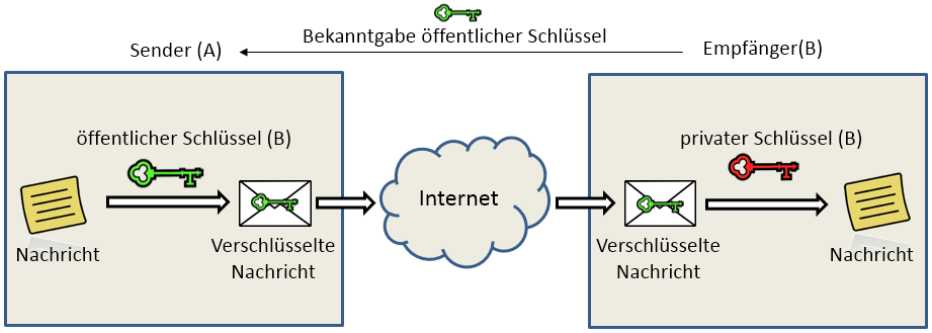

Abbildung 3: Asymmetrische Verschlüsselung[26]

Das Hybride Verfahren verbindet diese beiden Verfahren. Der Sender erhält einen öffentlichen Schlüssel vom Empfänger, mit dem er den geheimen Schlüssel (Session Key), der zur Verschlüsselung der eigentlichen Nachricht verwendet wurde, verschlüsselt und an den Empfänger überträgt. Dieser kann mit seinem passenden privaten Schlüssel den Session Key entschlüsseln, welcher zur Entschlüsselung der Nachricht benötigt wird. Der Rechenaufwand bei der asymmetrischen Verschlüsselung innerhalb des Hybriden Verfahrens ist geringer, da nur der symmetrische Schlüssel (Session Key) verschlüsselt wird.

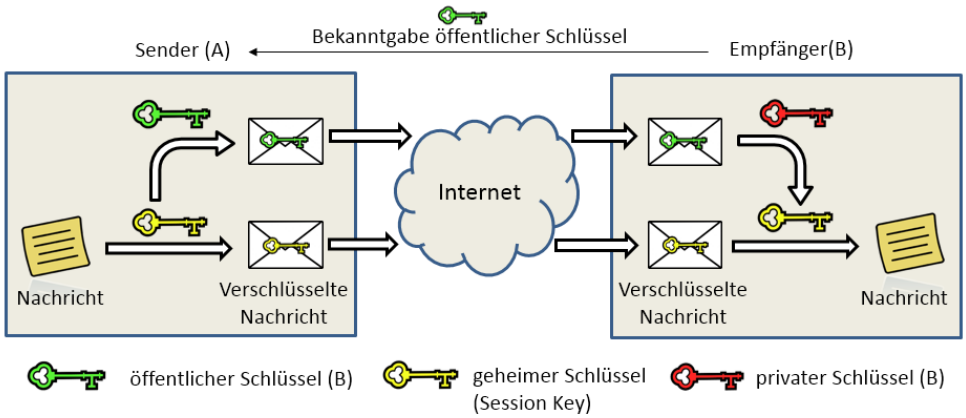

Abbildung 4: Hybride Verfahren[27]

[25] Vgl. Lauert (2010), o.S.
[26] Vgl. Lauert (2010), o.S.

Ein weiteres Konzept ist die digitale Signatur, bei der der Empfänger seinen für eine Nachricht ermittelten Fingerabdruck mit einem vom Sender verschlüsselt übertragen Fingerabdruck auf Gleichheit überprüft. Bei Abweichungen des digitalen Fingerabdrucks kann auf eine Manipulation der Nachricht während der Übertragung geschlossen werden. Der vom Sender übermittelte Fingerabdruck wird mit dem privaten Schlüssel des Senders verschlüsselt, um dessen Authentizität für den Empfänger sicherzustellen.

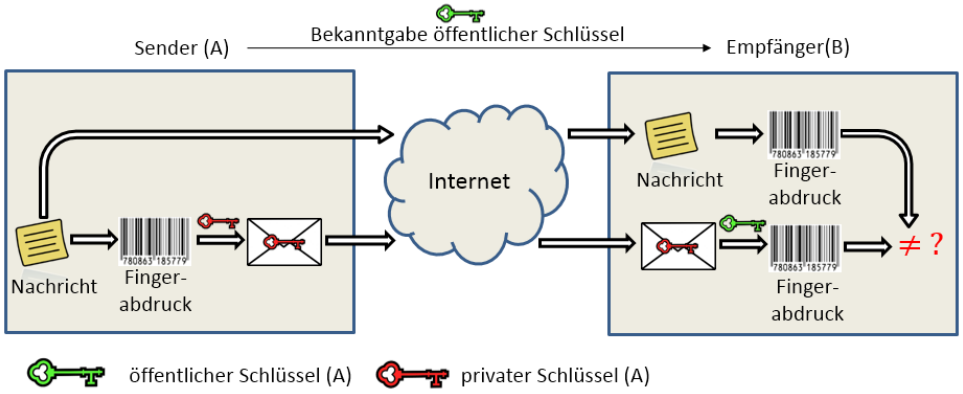

Abbildung 5: Digitale Signatur[28]

6. Fazit

Die Schäden für Unternehmen durch Cybercrime werden auch in Zukunft immer weiter ansteigen. Dazu trägt nicht zuletzt die ständig steigende Komplexität der IT-Infrastruktur des Unternehmens bei. So müssen Aspekte wie das Outsourcing von Daten und Anwendungen ebenso betrachtet werden, wie die Verwaltung von privaten Geräten von Mitarbeitern, die mit dem Firmennetzwerk in Verbindung kommen. Deswegen ist es umso wichtiger, geeignete Maßnahmen für den Schutz von Angreifern von innen und außen zu finden. Neben technischen Sicherheitskonzepten, wie der Verschlüsselung, sind hier auch besonders geeignete Richtlinien für den Umgang mit Daten durch die Mitarbeiter zu schaffen. Ziel sollte es sein, eine Sicherheitskultur im Unternehmen zu schaffen, bei der von allen Beteiligten die Bedeutung und die Gefahren die mit dem fahrlässigen Umgang mit Unternehmensdaten und Unternehmenswissens einhergehen, verinnerlicht werden. Dennoch wird es nie auszuschließen zu sein, dass es zu einem Diebstahl von Daten und damit dem Wissen des Unternehmens kommt, da sich bei allen Präventionsmaßnahmen und Sicherheitskonzepten Lücken auftun können.

[27] Vgl. Lauert (2010), o.S.
[28] Vgl. Lauert (2010), o.S.

Quellenverzeichnis

Beuth, P., Biermann, K., Das Spionagesystem Prism und seine Brüder. Online unter: http://www.zeit.de/digital/datenschutz/2013-06/nsa-prism-faq, Abruf am 2013-10-30.

Bundesamt für Sicherheit in der Informationstechnik – BSI (Hrsg., 2012), Leitfaden Informationssicherheit - IT-Grundschutz kompakt, Bonn. Online unter: https://www.bsi.bund.de/SharedDocs/ Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile, Abruf am 2013-10-29.

Bundesamt für Verfassungsschutz (Hrsg.): Spionage gegen Deutschland – Aktuelle Entwicklungen. Online unter: www.verfassungsschutz.de/download/thema-0811-spionage.pdf, Abruf am 2013-10-29.

Bundesministerium der Justiz (Hrsg.): Gesetz gegen den unlauteren Wettbewerb. Online unter: http://www.gesetze-im-internet.de/uwg_2004/17.html, Abruf am 2013-11-01.

Bundesministerium der Justiz (Hrsg.): Strafgesetzbuch. Online unter: http://www.gesetze-im-internet.de/stgb/, Abruf am 2013-10-31.

Gabler Wirtschaftslexikon – Stichwort Cybercrime. Online unter: http://wirtschaftslexikon.gabler.de/Fokus/Stichwort/Cybercrime.html; Abruf am 2013-10-29.

Handelsblatt (2013), Auch britischer Geheimdienst späht Daten aus. Online unter: http://www.handelsblatt.com/politik/international/abhoerskandal-auch-britischer-geheimdienst-spaeht-daten-aus/8391120.html, Abruf am 2013-10-30.

Harich, W. (2012), IT-Sicherheitsmanagement: Arbeitsplatz IT Security Manager, Heidelberg et al.

Hlavica, C. et al. (2011), Wirtschafts- und Industriespionage – Eine Bedrohung für Unternehmen. In: Hülsenberg, F. (Hrsg.): Tax Fraud & Forensic Accounting – Umgang mit Wirtschaftskriminalität. Gabler, Wiesbaden 2011, S. 58.

Jenkins Samuel P., Director Defence Privacy Office – U.S. Department of Defence (2010), Privacy and IT-Security. Online unter: http://search.defense.gov/search?affiliate=DEFENSE_gov&query=it-security&x=-1412&y=-68 dpclo.defense.gov/.../2010%20Privacy

Kersten, H., Klett, G. (2008), Der IT Secutity Manager – Expertenwissen für jeden IT Security Manager, 2. Auflage, Wiesbaden.

KPMG(Hrsg., 2013), Forensic – e-Crime – Computerkriminalität in der deutschen Wirtschaft mit Kennzahlen für Österreich und Schweiz. Online unter: http://www.kpmg.com/CH/de/Library/ArticlesPublications/Documents/Advisory/ pub-20130327-e-crime-studie-de.pdf, Abruf am 2013-10-29.

KPMG(Hrsg., 2013), Forensic – e-Crime – Computerkriminalität in der deutschen Wirtschaft mit Kennzahlen für Österreich und Schweiz. Online unter: http://www.kpmg.com/CH/de/Library/Articles-Publications/Documents/Advisory/pub-20130327-e-crime-studie-de.pdf, Abruf am 2013-10-29.

Lauert, A. (2010), Elektronisches Bezahlen. Online unter: http://ddi.cs.uni-potsdam.de/Lehre/e-commerce/elBez2-5/page04.html, Abruf am 2013-10-30.

Lischka, K., Stöcker, C. (2013), NSA-System XKeyscore: Die Infrastruktur der totalen Überwachung. Online unter: http://www.spiegel.de/netzwelt/netzpolitik/xkeyscore-wie-die-nsa-ueberwachung-funktioniert-a-914187.html, Abruf am 2013-10-30.

Radic, C. (2001), Der Fall „Echelon“: Verschlusssache Wirtschaftsspionage. In: Monitor, 7-8, S. 101.

SAP AG (Hrsg., 2007): IT-Sicherheitsrecht – Einführung in die deutsche und europäische IT-Rechtsprechung. Online unter: https://www.sicher-im-netz.de/files/documents/06_02_IT_Sicherheitsrecht.pdf, Abruf am 2013-11-01.

Schoolmann, J.; Rieger, H. (Hrsg., 2005): Praxishandbuch IT-Sicherheit – Risiken, Prozesse, Standards. Symposion Publishing, Ettlingen, S. 388.

Schulzki-Haddouti, C.: Hintertür für Spione. In: Die Zeit, Jrg. 1998, Ausgabe 39. Online unter: http://www.zeit.de/1998/39/199839.c_krypto_.xml

Symantec (Hrsg., 2013), 2013 Norton Report . Online unter: http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013, Abruf am 2013-11-01.