IT-gestütztes Management und Controlling: Verdeckte Kanäle – eine zunehmende Gefahr für Unternehmensdaten

Intro

Erfolgreiches Controlling benötigt vertrauenswürdige Informationen über eine Organisation als Grundlage für die Entscheidungsfindung. Dieser Artikel zeigt, dass mithilfe so genannter verdeckter Kanäle bestehende IT-Schutzmechanismen umgangen werden können und somit die Vertrauenswürdigkeit von Informationen für das Controlling kompromittiert werden kann.

Stichwörter

- Datenexfiltration
- Gebäudeautomation
- IT-Sicherheit
- verdeckter Kanal
- Vertraulichkeit

Summary

Successful controlling requires trustworthy information in order to enable a high-quality decision making. This article presents an emerging threat, namely covert channels, capable to bypass current IT security protection means and moreover able to influence the confidentiality of information used in controlling.

Keywords

- Building Automation
- Confidentiality
- Covert Channel
- Data Leakage
- IT Security

Autorenbeschreibung

Dr. Steffen Wendzel ist Head of Secure Building Automation am *Fraunhofer FKIE* in Bonn.

Prof. Dr. Jörg Keller ist Leiter des Lehrgebiets Parallelität und VLSI an der *FernUniversität in Hagen*.

1. IT-Sicherheitsaspekte in Unternehmen

Im Rahmen des Controllings werden Daten innerhalb und außerhalb eines Unternehmens gesammelt, analysiert und aggregiert. Somit werden aus den Daten Informationen, die der Unternehmensleitung zur Entscheidungsunterstützung dienen. Da die Tätigkeiten des Sammelns und Aggregierens sowie die Speicherung und Kommunikation dieser Daten und der Informationen IT-gestützt erfolgen, gelten hierfür die "klassischen" Schutzziele der IT-Sicherheit (*Eckert*, 2013). Diese sind (illustriert anhand von Controlling-nahen Beispielen):

Vertraulichkeit. Kein Unberechtigter soll von vertraulichen Daten und Informationen Kenntnis erlangen. Die Daten stellen in der Regel einen erheblichen Wert für das Unternehmen dar. Ein Konkurrent könnte ansonsten durch Industriespionage die aufwändig zusammengestellten Daten erhalten und kostenlos nutzen, vielleicht sogar die Entscheidung des Unternehmens darauf antizipieren und sich entsprechend positionieren.

Integrität. Es darf keine unbemerkte Veränderung der Daten erfolgen. Ansonsten könnte ein Konkurrent durch Veränderung der Daten versuchen, die Entscheidungen der Unternehmensleitung zu manipulieren, um sich selbst einen Vorteil zu verschaffen.

Authentizität. Es darf nicht vorkommen, dass Daten aus zweifelhaften Quellen als verlässlich angesehen werden. Ansonsten könnte ein Konkurrent per E-Mail Umsatzzahlen schicken, sich dabei als die vom Unternehmen beauftragte Firma ausgeben, und durch falsche Zahlen die Entscheidungen der Unternehmensleitung manipulieren. Falsche Zahlen führen generell zum Problem des "Garbage in, garbage out".

Verfügbarkeit. Die benötigten Daten und Informationen müssen verfügbar sein, wenn sie benötigt werden. Ansonsten könnte ein Konkurrent eine wichtige Datei vor einer Sitzung der Unternehmensleitung löschen, so dass keine qualifizierte Entscheidung getroffen werden kann. Liegt eine Frist vor, verstreicht diese eventuell, bevor die Daten wieder beschafft bzw. restauriert werden können.

Werden diese Schutzziele also unbemerkt verletzt, kann dem Unternehmen großer Schaden entstehen.

Dieser Artikel befasst sich vorwiegend mit dem Bereich der Vertraulichkeit, d. h. dem Verhindern von ungewolltem Datenabfluss. Während bei der Speicherung und Übertragung Vertraulichkeit durch Verschlüsselung hergestellt werden kann, so sind die Daten zumindest bei der Verarbeitung in einem Rechner unverschlüsselt verfügbar. Ist dieser Rechner von einem Angreifer kompromittiert, d. h. mit einer Schadsoftware infiziert, so kann dieser Angreifer versuchen, vertrauliche Daten wie Kreditkartennummern, Kundendaten oder aggregierte Informationen wie Bereichs-Umsatzzahlen aus dem Unternehmen zu schleusen. Angreifer konnten beispielsweise

jüngst über eine Million Datensätze der Forbes-Website entwenden. Darunter befanden sich insbesondere E-Mail-Adressen und verschlüsselte Passwörter von Kunden (*Open Security Foundation, 2014*). Die Webseite http://datalossdb.org sammelt und listet zahlreiche Data Leakage-Fälle der letzten Jahre. In extremen Fällen wurden bis zu 152 Millionen Datensätze von einem einzigen Unternehmen gestohlen. Im Bereich Data Leakage hat es in den letzten Jahren Entwicklungen gegeben, die dieser Beitrag vorstellen möchte, da sie teilweise noch nicht im allgemeinen Blickfeld der IT-Sicherheit angekommen sind, gleichwohl aber eine nicht zu unterschätzende Relevanz besitzen. Kapitel 2 führt in das Thema Data Leakage und die damit verbundenen bisherigen Schutzmechanismen für Unternehmen ein. Kapitel 3 stellt die Thematik der verdeckten Kanäle vor, die eine bisher nicht vollständig verhinderbare Gefahr für die Vertraulichkeit von Daten darstellen. Insbesondere weist dieser Beitrag auf die Rolle der Gebäudeautomation in diesem Zusammenhang hin. In Kapitel 4 werden vorhandene Lösungen und Forschungsrichtungen für offene Punkte vorgestellt und Kapitel 5 geht auf eine Reihe von weiteren Herausforderungen der IT-Sicherheit im Unternehmenskontext ein, die zeigen, dass es sich hierbei um ein Querschnitts-Thema handelt, das technisch und organisatorisch angegangen werden muss. Insbesondere die Rolle der Mitarbeiter soll kurz beleuchtet werden. Kapitel 6 fasst zusammen und gibt einen kurzen Ausblick.

2. Data Leakage

Der Abfluss vertrauenswürdiger Informationen wird als Data Leakage bezeichnet. Dabei können Daten sowohl durch interne Angreifer (etwa Angestellte) als auch durch externe Angreifer exfiltriert werden. Data Leakage geschieht auf vielfältige Weise, sowohl mutwillig als auch unabsichtlich. Im einfachsten Fall werden vertrauliche Informationen per E-Mail verschickt oder auf einer externen Webseite gepostet. Auch möglich ist der Datenverlust durch USB-Sticks, Tablets, Smartphones oder Laptops, die in Taxen oder Hotelzimmern verloren gehen, gestohlen werden, mutwillig an Dritte übergeben, oder nach dem Austritt aus einem Unternehmen nicht zurück gegeben werden. Eine weitere Problematik stellen ungesperrte Computer und aufgeschriebene Passwörter dar, die ein Angreifer nutzt, um an sensible Daten zu gelangen.

Die Auswirkungen von Data Leakage sind ebenso vielfältig wie ihre Formen. So kann ein Verlust oder eine Veröffentlichung sensibler Informationen zu Reputationsverlust oder Missbrauch des Firmennamens führen. Geschäftsgeheimnisse (etwa Umsatzzahlen oder Quellcode) können an die Konkurrenz verkauft und sensible Kundendaten missbraucht werden, womit ein Verlust von Kunden einhergehen kann. Sind personenbezogene Daten betroffen, ist denkbar, dass diese für einen Identitätsdiebstahl ausgenutzt werden. Ein wichtiger Aspekt hierbei ist der, dass Daten, die einmal exfiltriert wurden, sich permanent der zukünftigen Kontrolle entziehen und somit einen permanenten Schaden darstellen können.

In einer von *CISCO* durchgeführten Studie wurden im Kontext von Data Leakage sogenannte

Insider Threats untersucht (vgl. *Cisco Systems*, 2008), dabei handelt es sich um Data Leakage, die insbesondere durch Beschäftigte durchgeführt wird. Von den 2.000 befragten Angestellten und IT-Professionals aus zehn Ländern gaben 33 % an, sich mit der Problematik gestohlener bzw. verlorener USB-Sticks befasst zu haben, 39 % waren mehr mit Data Leakage durch interne als durch externe Personen befasst und 27 % wussten zum Zeitpunkt der Befragung nichts über neuere Trends im Bereich von Data Leakage. Interessant ist zudem, dass tatsächlich 9 % der Angestellten Unternehmensgeräte gestohlen wurden oder diese verloren haben. Zudem empfiehlt *CISCO* die Umsetzung von „Best Practices" zur Data Leakage Prevention (DLP), das sind Data Leakage-Gegenmaßnahmen. Zu diesen Best Practices zählt, dass zuständige Mitarbeiter das Sicherheitsbewusstsein in der Organisation fördern, Awareness-Schulungen anbieten und Angestellte nach Aufenthaltsort und ausgesetzter Gefahr einordnen. Eine Person, die mit sensiblen Daten in ein Land reist, in dem ein Datenverlust wahrscheinlicher erscheint, wird entsprechend intensiver geschult als eine Person, die kaum Zugriff auf sensible Daten hat und nicht verreist. Die entsprechende Einordnung sollte kontinuierlich erfolgen und zusätzlich die Interaktionsrisiken zwischen Benutzern, Netzwerken und Anwendungen einbeziehen. Zudem wird empfohlen, Policies nicht nur zu erstellen, sondern auch plausibel und verständlich zu halten sowie Zeit in deren Kommunikation zu investieren. Nicht zuletzt sollte Wert darauf gelegt werden, die Erwartungen zum Schutz vor Data Leakage klar zu nennen und als Führungskraft ein korrektes Verhalten vorzuleben.

Problematisch ist bei der Umsetzung von DLP generell der Trade-Off zwischen Benutzbarkeit, Sicherheit, Kosten und Performance. Wird eine DLP-Maßnahme in ein Unternehmensnetz integriert, so ist diese zunächst einmal mit Anschaffungs-, Integrations- und Wartungskosten verbunden und kann Prozesse im Unternehmen verlangsamen (Performance) oder verkomplizieren (Benutzbarkeit), während sie Data Leakage eindämmt (Sicherheit). Aktuelle Maßnahmen adressieren diese Probleme zwar, können und werden sie jedoch nie vollständig eliminieren, da DLP immer ein zusätzlicher Prozessschritt ist und immer Analysezeit kostet, bei der Administration und Interaktion mit dem DLP-System Prozesse verkompliziert und Kosten niemals komplett eliminiert werden können.

DLP-Maßnahmen versuchen dabei mithilfe von Mustererkennung und statistischen Analysen eine Detektion von sensiblen und vor der Exfiltration zu bewahrender Daten zu erreichen. Dabei werden Datenübertragungen im Netzwerk etwa nach Programm-Quellcode, Office-Dokumenten, Kreditkarten- und Sozialversicherungsnummern sowie elektronischen Gesundheitsdaten (ePHI, eletronic protected health information) durchsucht (*IBM*, 2013). Auch adressieren aktuelle Maßnahmen DLP für Heimarbeit und für die Cloud. Die letzten Jahre brachten insbesondere Fortschritte im Bereich der lernfähigen Systeme, d. h. Systeme, die erlernen, welche legitime Kommunikation im Unternehmensnetz erlaubt ist, und daraus automatisch Regelsätze für die Kommunikation generieren können. Ein typischer Regelsatz könnte etwa das Hochladen oder Versenden von Excel-Dateien bestimmter Größe durch die Finanzabteilung verhindern (*CISCO*,

2013).

Im Falle einer erkannten Data Leakage werden entsprechende Meldungen an die verursachende und an die verantwortliche Person gesendet und E-Mails in Quarantäne gestellt. Falls notwendig, wird ein Data Leakage-Fall automatisch an einen zuständigen Mitarbeiter delegiert.

3. Verdeckte Kanäle

Bereits in den frühen 1970er Jahren wies *Lampson* auf das Problem verdeckter Kanäle (covert channels) hin (vgl. *Lampson*, 1973). *Lampson* definierte verdeckte Kanäle als Kommunikationspfade, die im Design eines Systems gar nicht vorgesehen, jedoch vorhanden sind. In den 1980er Jahren fügte das amerikanische *Department of Defense* (DoD) der Definition verdeckter Kanäle einen Sicherheitsaspekt hinzu; seitdem werden verdeckte Kanäle primär als nicht vorgesehene Kommunikationskanäle betrachtet, die Sicherheitsregeln einer Organisation verletzen (*Department of Defense*, 1985). Im Kontext des Controllings ermöglichen verdeckte Kanäle etwa den illegitimen Abfluss vertrauenswürdiger Daten an Dritte, also Data Leakage.

Im Gegensatz zu herkömmlichen Data Leakage-Verfahren zeichnen sich verdeckte Kanäle dadurch aus, dass sie bestehende DLP-Maßnahmen umgehen können und eine äußerst geringe Aufmerksamkeit erzeugen. Dies macht verdeckte Kanäle für zukünftige Data Leakage-Angriffe äußerst attraktiv. Nicht ohne Grund wies *AT&T* CSO *Ed Amoroso* bereits 2010 darauf hin, dass Forschung im Bereich verdeckter Kanäle wieder aufgenommen werden muss (vgl. *Amoroso*, 2010).

Selbst wenn ein Angreifer seine Datenexfiltration verschlüsselt, damit ihr Inhalt nicht direkt ersichtlich ist, ist die stattfindende Kommunikation an sich trotz Verschlüsselung sichtbar. Verdeckte Kanäle sind als Teilgebiet der sogenannten Information Hiding-Forschung in der Lage, die stattfindende Kommunikation an sich zu verbergen, wozu sensible, zu exfiltrierende Daten in einer legitimen Datenübertragung versteckt werden.

Bereits früh wandten Menschen steganografische Techniken an, bei denen Nachrichten in anderen Nachrichten versteckt wurden, etwa mithilfe von Geheimtinte oder linguistischer Steganografie, also dem Verstecken von Text in Texten (zum Beispiel durch Verwendung von Synonymen, Satzbauten, Rechtschreibfehlern). In den letzten Jahrzehnten kamen zunehmend digitale Verfahren auf, bei denen Daten in Audiodateien und Videodateien untergebracht wurden und schließlich – in Form verdeckter Kanäle – im Netzwerk übertragen wurden.

Prinzipiell lässt sich in allen Datenübertragungen eine geheime Information verstecken. Allein durch die Tatsache, ob zu einem Zeitpunkt kommuniziert wird oder nicht, kann eine geheime Information weitergegeben werden. Skype-Übertragungen, E-Mail-Informationen, WiFi-Übertragungen, Webseiten-Verhalten; es gibt praktisch kein relevantes Anwendungsfeld, für das keine Technik zur Umsetzung verdeckter Kanäle vorliegt oder zumindest denkbar ist. Allein für das

Verstecken von sensiblen Informationen in Netzwerkdaten liegen bereits über Hundert verschiedene Techniken vor, wobei hier keine der zahlreichen Techniken mitgezählt wurden, die sich auf Nutzdaten (d. h. Anwendungsdaten wie E-Mails, Webseiten-Inhalte, Audio- und Videoinhalte, Dokumenteninhalte etc.) beziehen.

Eine weitere Möglichkeit, verdeckte Kanäle zu etablieren, besteht in der Ausnutzung der derzeit stark an Verbreitung zunehmenden smarten Technologien (z. B. Smart Cities und Smart Buildings). Bereits vor einigen Jahren konnten wir zeigen, dass durch smarte Gebäude, d. h. über die Gebäude-Automation, eine Datenexfiltration auf Netzwerkebene leicht umsetzbar ist (*Wendzel* et al., 2012). Gebäude-Netze sind oft ohne Schutzfunktion direkt mit dem Internet oder anderen Unternehmensstandorten verbunden und eignen sich daher gut, um herkömmliche DLP-Maßnahmen zu umgehen.

Selbst wenn die Netzwerkverbindung der Gebäude-Automation nicht in die Data Leakage-Technik einbezogen wird, so ergeben sich sehr simple Exfiltrationsmöglichkeiten, die aufzeigen, wie schwer die Unternehmensleitung und IT-Administration dem Thema Herr werden kann. Nehmen Sie beispielsweise an, ein externer Angreifer beobachtet durch einen Sensor automatisch (oder als Person mit dem bloßen Auge) zu einem nächtlichen Zeitpunkt ein bestimmtes Fenster eines Firmengebäudes. Mithilfe der Gebäude-Automation lassen sich Morse-Signale durch Ein- bzw. Ausschalten einer Bürolampe generieren und somit auf Dauer (etwa jede Nacht für 5 Minuten) sensible Daten exfiltrieren, die zuvor von einem Angreifer in eine bösartige Software eingespeist wurden oder von diesem manuell signalisiert werden. Selbiges funktioniert mit anderen Komponenten, etwa Rollläden. Im Falle einer Netzwerkverbindung des Gebäudes, die nicht für Jedermann sichtbar ist, lassen sich hingegen viel mehr Daten einfacher und in zugleich unauffälligerer Weise übertragen.

4. Fortgeschrittene Techniken und Stand der Forschung

Aus der Vielfalt der bestehenden verdeckten Kanäle ergibt sich das Problem, dass in der Praxis nur wenige dieser Kanäle verhindert werden können. Diese Tatsache begründet sich dadurch, dass verdeckte Kanäle praktisch alle Kommunikationsattribute von Netzwerken ausnutzen können und eine Einschränkung dieser Attribute umfassende, funktionale und nichtfunktionale Auswirkungen auf den Netzbetrieb haben würde. Aktuelle DLP-Lösungen betrachten, wenn überhaupt, nur sehr simple verdeckte Kanäle. Dies bezieht sich sowohl auf die Detektion als auch auf die Prävention und Limitierung der Kanäle.

Erschwerend kommt hinzu, dass es in den letzten Jahren diverse Weiterentwicklungen verdeckter Kanäle gab. Verdeckte Kanäle übertragen nicht mehr ausschließlich zu exfiltrierende Informationen an sich, sondern sichern die Übertragung vielfältig ab. Zum einen wurden verdeckte Kanäle derart erweitert, dass sie Meta-Informationen (sog. Kontrollprotokolle) übertragen, also Daten, die exfiltrierende Daten beschreiben (*Wendzel/Keller*, 2014), wodurch insbesondere

Übertragungsprobleme, die durch Störungen hervorgerufen werden, ausgeglichen werden können. Genauso bedeutend ist zum anderen die Fähigkeit, verdeckte Kanäle adaptiv zu gestalten (*Yarochkin* et al., 2008), d. h. ihnen die Möglichkeit zu geben, sich automatisch an verändernde Umgebungen anzupassen. Blockiert etwa ein Netzwerkadministrator einen verdeckten Kanal, re-konfiguriert sich dieser Kanal, um automatisch mithilfe anderer Verfahren zu kommunizieren. In einer Weiterentwicklung konnten wir zeigen, dass es mithilfe der genannten Meta-Informationen zudem möglich ist, durch Firewalls zu kommunizieren bzw. diese mithilfe dynamischer Verfahren auf nicht-herkömmliche Weise (etwa via Google Translator) zu umgehen (*Backs,* 2012).

Aus Sicht der Angreifer stellen verdeckte Kanäle für Angreifer eine zunehmend attraktive Enabling-Technologie für zukünftige und zudem langfristige Data Leakage dar, gegen die derzeit fast keine Protektionsmaßnahmen, vor allen Dingen keine hinreichenden, vorhanden sind.

Derzeit konzentriert sich die Forschungslandschaft stark auf die Entwicklung wirksamer Maßnahmen gegen verdeckte Kanäle. Viel versprechend ist es dabei, Muster verdeckter Kanäle zu entdecken. Diese Muster sind besonders dann relevant, wenn sie möglichst vielen verdeckten Kanälen entsprechen. Statt einen einzigen verdeckten Kanal zu verhindern bzw. zu detektieren, ermöglicht die Entwicklung von Muster-basierten Gegenmaßnahmen das parallele Verhindern bzw. Detektieren einer Vielzahl verdeckter Kanäle. Erste Verfahren befinden sich in sehr frühen Stadien der Erforschung und werden vermutlich erst in mehreren Jahren in Produkte münden.

5. Herausforderungen der IT-Sicherheit im Unternehmenskontext

In Kapitel 4 haben wir eine spezifische Gefahr aufgezeigt, die spezifische Maßnahmen erfordert. Allerdings existiert eine Vielzahl an Angriffsformen, die teilweise aufeinander aufbauen, und die eine Fülle aufeinander abgestimmter Maßnahmen erfordern. Insgesamt gilt für die IT-Sicherheit die alte Regel "Eine Kette ist nur so stark wie ihr schwächstes Glied". Viele gut umgesetzte Schutzmaßnahmen können entsprechend durch eine Komponente geringer Qualität zunichte gemacht werden.

In vielen Fällen stellt der Mensch als Benutzer das schwächste Glied dar. Dies liegt daran, dass Benutzer Gefahren der IT-Sicherheit nicht sehen, oder dass Maßnahmen der IT-Sicherheit den Arbeitsablauf weniger angenehm oder flüssig gestalten. Beispielsweise erfordert das Signieren einer E-Mail (die die Ergebnisse einer Datenanalyse weiterleiten könnte), womit die Echtheit des Absenders und die Unversehrtheit des Inhalts garantiert wird, in manchen E-Mail-Systemen einen oder zwei zusätzliche Clicks. Der Aufwand für diese Clicks ist der Grund, weshalb Benutzer das Signieren auslassen, oft mit der Entschuldigung "Die E-Mail ist sicher, da sie nur intern versendet wird". Vielen Benutzern ist allerdings nicht bewusst, dass einmal eingeschleuste Schadsoftware, die beispielsweise über einen verdeckten Kanal gesteuert sein könnte, E-Mails intern versenden kann. Bei diesen durch Schadsoftware generierten Mails kann der Absender gefälscht werden, so dass der Empfänger die Nachricht als authentisch annimmt, wenn er die fehlende Signatur aus

Unkenntnis, Gewöhnung oder Bequemlichkeit nicht bemängelt, obwohl der Inhalt nicht vom vorgeblichen Absender stammt und falsche Daten enthält. Um solche Verhaltensweisen zu ändern, sind Awareness-Schulungen notwendig, die die Gefahren vor Augen führen, und einen möglichst effizienten und gleichzeitig sicheren Umgang mit IT-Sicherheitsmaßnahmen vermitteln.

Ein anderes Beispiel zeigt auch hier die oft schlecht gesicherte und kaum betrachtete Gebäude-Automation auf. Viele Unternehmen sichern den Remote-Zugang zu ihrem IT-Netzwerk hochqualitativ ab. Ist allerdings die Gebäude-Automation (etwa zwecks Outsourcing der Steuerung und Überwachung an eine Sicherheitsfirma) mit dem Internet und zugleich mit dem Firmennetzwerk verbunden, so stellt sie ein Einfallstor zur Umgehung der starken Glieder der Schutzkette dar.

IT-Sicherheit ist also ein Querschnittsthema, das sowohl technische als auch organisatorische Maßnahmen umfassen muss, und das der Rückendeckung der Unternehmensleitung bedarf: denn wenn diese erlaubt oder duldet, IT-Sicherheitsmaßnahmen zugunsten anderer Ziele zu umgehen, dann können auch die besten Programme zur Nutzer-Awareness nicht wirken.

6. Fazit und Zusammenfassung

Für die Unternehmenssteuerung stellen Geschäftsdaten und daraus gewonnene Informationen eine wichtige Entscheidungsunterstützung dar. Verlieren diese Daten ihre Vertraulichkeit durch Data Leakage oder werden Entscheidungen auf Basis gefälschter Daten getroffen, so kann einem Unternehmen großer Schaden entstehen.

Dieser Artikel hat neuere Entwicklungen, vornehmlich verdeckte Kanäle, vorgestellt, die etablierte Maßnahmen zur Informationssicherheit umgehen können und damit weitere, im Wesentlichen noch zu erforschende Schutzmaßnahmen erfordern. Zum Schutz vor verdeckten Kanälen ist es wichtig, dass diese Gefahr ins Blickfeld der IT-Abteilung, aber auch der Unternehmensleitung und der Nutzer von Unternehmensdaten, zum Beispiel in das Controlling, gerückt wird.

Wie in anderen Fällen ergibt sich für die Nutzer ein Spannungsfeld zwischen Sicherheit und Benutzbarkeit bzw. Bequemlichkeit, wobei ein Gewinn an Sicherheit für den Nutzer keinen unmittelbaren Vorteil bringt. Hier sind Maßnahmen zur Awareness vonnöten, um die Benutzerakzeptanz von IT-Sicherheitsmaßnahmen und damit auch die Datensicherheit zu erhöhen.

Literatur

Amoroso, E., Covert Channel Research Must be Resumed, *AT&T* Tech Channel, 2010, http://techchannel.att.com/play-video.cfm/2010/3/12/Security-Tips-Covert-Channel-Research-Must-be-Resumed, Stand: 24.02.2014.

Backs, P., Wendzel, S., Keller, J., Dynamic routing in covert channel overlays based on control

protocols, in: Proc. International Workshop on Information Security, Theory and Practice (ISTP-2012), IEEE, 2012, S. 32-29.

Cisco Systems, Data Leakage Worldwide: The High Cost of Insider Threats, Cisco, 2008, http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-506224.html, Stand: 24.02.2014.

CISCO, Web Security Technology Overview: Cisco IronPort Web Data Security and Data Loss Prevention, White Paper, 2013.

Department of Defense (DoD), Trusted computer system evaluation criteria (TCSEC, DoD 5200.28-STD, orange book), 1985.

Eckert, C., IT-Sicherheit, 8. Aufl., Oldenbourg 2013.

IBM, Fidelis Network Data Loss Protection: Reduce risk efficiently by helping to prevent data loss across the network without compromising business needs, IBM 2013, http://www-935.ibm.com/services/us/en/it-services/fidelis-security-systems-appliances-and-support.html, Stand: 24.02.2014.

Lampson, B. W., A Note on the Confinement Problem, in: Communications of the ACM 16 Jg. (1973), H. 10, S. 613-615.

Open Security Foundation: DataLossDB – Forbes Data Breach Impacts Over 1 Millions Accounts, *2014,* http://datalossdb.org/incident_highlights/61-forbes-data-breach-impacts-over-1-millions-accounts, Stand: 28.02.2014.

Wendzel, S., Keller, J., Hidden and Under Control: A Survey on Covert Channel-internal Control Protocols, Annals of Telecommunications, Springer Paris 2014 (to appear).

Wendzel, S., Kahler, B., Rist, T., Covert Channels and their Prevention in Building Automation Protocols – A Prototype Exemplified Using BACnet, in: Proc. 2nd Workshop on Security of Systems and Software Resiliency, Besançon, France, IEEE 2012, S. 731-736.

Yarochkin, F. V., Dai, S. Y. et al., Towards adaptive covert communication system, in: Proc. 14th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC 2008), IEEE Computer Society 2008, S. 153-159.