Datenschutz und Datensicherheit in Krankenhaus und Praxis – Was tun im Falle der internen oder externen Bedrohung?

Markus Mohr, ManaThea GmbH, Regensburg

Selten wird im persönlichen Gespräch darüber berichtet, dass ein Sicherheitsleck im Kontext von Patientendaten ausgenutzt wurde. Noch seltener wird darüber auf Sicherheitskonferenzen oder in anderen geeigneten Medien referiert. Trotzdem sind Sicherheitsprobleme im Umgang mit Patientendaten jedoch immer wieder an der Tagesordnung, nicht zuletzt einer der Gründe, warum in Deutschland auf Datenschutz und Datensicherheit so viel Wert gelegt wird. Dieser Artikel geht von tatsächlichen Bedrohungen aus und widerspiegelt die langjährige Insider-Erfahrung des Autors als Arzt und IT-Sicherheitsexperte. In einer schematischen Übersicht bietet diese Umschau einen Überblick zu den häufigsten Bedrohungen von innen wie von außen und versucht, Strategien für deren Lösung zu geben. Auch für den Fall des „in den Brunnen gefallenen Kindes" werden Ansätze für eine Postphylaxe gegeben.

Ausgangssituation und Hintergründe

Seitdem Daten erhoben werden, besteht die Möglichkeit, dass sich Unbefugte dieser Daten bemächtigen. Dieser Prozess ist vom Medium der erhobenen Daten unabhängig. War es vor 20 Jahren noch einfach, sich als Arzt oder Angehöriger des medizinischen Personals verkleidet aus dem Archiv eines Krankenhauses nahezu in beliebigem Umfang Akten z. B. für Studienzwecke oder zur Nachuntersuchung im Rahmen einer Promotion aushändigen zu lassen, ist diese Situation heute durch die überwiegend digitale Speicherung der Daten wesentlich komplexer geworden und erfordert Einiges mehr an neu erworbenen Kenntnissen und Fähigkeiten.

Das Ausmaß an Datenschutz [1] und Datensicherheit [2] in einer medizinischen Einrichtung hängt nicht nur davon ab, wie unkompliziert jemand, der dazu nicht befugt ist, an Daten herankommt, sondern – in deren digitaler Form – insbesondere auch von grundlegenden Sicherheitsrichtlinien, die global, d. h. für alle Benutzer eines Systems, eingerichtet, gepflegt und auch gelebt werden (sog. Security Policies [3]). Aber auch weit jenseits technischer Belange bestehen Gefahren im Rahmen geschickt geführter Gespräche mit Mitarbeitern dieser Einrichtungen, die im Kontext logischer Erwägungen dazu gebracht werden, Informationen, die nicht preisgegeben werden sollen, eben doch preiszugeben (sog. Social Engineering [4]).

Dem Datenschutz lieget in Deutschland das Recht auf informationelle Selbstbestimmung zugrunde. Wegweisend ist hierbei das Bundesdatenschutzgesetz (BDSG).

Über das konkrete Ausmaß der Bedrohung von Datenschutz und Datensicherheit existieren keine verlässlichen Zahlen. Aus vielen Gesprächen mit einzelnen Betroffenen lässt sich rekonstruieren, dass es immer wieder stellenweise Angriffe aus der inneren (eigene Mitarbeiter bzw. sich im inneren Kreis aufhaltende Personen) wie aus der äußeren (rein abstrakte, digitale Angriffe durch Umsetzung bekannter oder noch nicht weit bekannter Technologien) Domäne gibt. Insofern lassen sich bestenfalls Schätzungen zu diesem Thema durchführen:

Die Majorität der internen Angriffe bezieht sich auf das nicht zugelassene Beziehen diagnostischer und therapeutischer Daten z. B. in der Öffentlichkeit stehender Personen mit dazu geeigneten technischen Hilfsmitteln oder untere Ausnutzen hausintern bekannter sicherheitsrelevanter Schwachstellen. Die meisten externen Angriffe beziehen sich auf das Cracken von Web-Servern bzw. das Defacement (Änderung von zentralen Inhaltsseiten) von Webauftritten medizinischer Einrichtungen. Auch Einbruchsversuche von außen nach innen, d. h. über einen Web-Server in die „Innereien" eines dahinterliegenden Computer-Netzwerkes sind bekannt, diese sind aber aufgrund der Tatsache, dass viele derartige Web-Server innerhalb einer sog. Demilitarisierten Zone (DMZ) liegen oder von einem öffentlichen Internet Service-Provider (ISP) gehostet werden, weniger erfolgreich und geeignet, um an sensible Daten heranzukommen.

Unter Angriff wird dabei jede wie auch immer geartete menschvermittelte Aktivität verstanden, die dazu geeignet ist oder sein soll, unbefugt an Daten überhaupt und insbesondere Daten Dritter heranzukommen.

Die häufigsten Angriffsszenarien

An dieser Stelle gibt es mehrere Unterscheidungen, die die Angriffe allesamt aus verschiedenen Blickwinkeln betrachten.

Zunächst einmal kann grob danach unterschieden werden, ob es sich um einen internen oder einen externen Angriff handelt.

Der interne Angriff stammt in der Regel aus dem eigenen Haus: Eigene Mitarbeiter, Zeitpersonal oder unbefugte Fremde sind die dafür in Frage kommenden Personenkreise. Bei allen Personen muss jedoch Zweierlei vorliegen, um einen erfolgreichen internen Angriff zu starten: Erstens das notwendige Maß an krimineller Energie, zweitens das technische Know-how bzw. das Verfügen über ausreichende Skills beim Social Engineering (v. i.).

Der externe Angriff geschieht im Wesentlichen abstrakt und anonym ausgetragen auf einer rein technischen Ebene, ausgehend von einem oder mehreren Rechnern aus einem oder verschiedenen Netzwerken, ohne dass man in aller Regel

Autor: Markus Mohr
Titel: Datenschutz und Datensicherheit in Krankenhaus und Praxis
In: Jäckel (Hrsg.) Telemedizinführer Deutschland, Bad Nauheim, Ausgabe 2009
Seite: 246-250

die dahinter stehenden Einzelpersonen zu Gesicht bekäme.

In der englischsprachigen Literatur wird dazu häufig dem Schwergrad nach unterschieden zwischen folgenden Angriffsformen:

- Koordinierter Angriff
- Direkter Angriff
- Indirekter Angriff
- Unstrukturierter oder unkoordinierter Angriff

Der koordinierte Angriff entspricht demselben taktischen Vorgehen wie im Kriegsfall: Mehrere Personen planen und führen einen Angriff z. B. unter Ausnutzung mehrerer (eigener oder fremder [gekaperter]) Computersysteme durch mit dem Ziel, ein spezifisches System und von diesem ausgehend möglicherweise in einer Kettenreaktion mehrere Zielsysteme auszuschalten oder in die eigene Gewalt zu bringen. Ein typischer Vertreter dieser Angriffsform ist der sog. Distributed Denial of Service (DDoS) Angriff [5].

Direkte Angriffe richten sich üblicherweise gegen eine oder mehrere bekannte Schwachstellen innerhalb einer IT-Infrastruktur, die noch nicht oder gar nicht durch Sicherheits-Updates ausgemerzt worden sind. Ein Beispiel für einen direkten Angriff bildet der sog. Ping of Death (PoD) Angriff [6]. Zu dieser Gruppe von Angriffen gehören insbesondere auch

- Angriffe gegen die Authentifizierung eines Computersystems,
- Angriffe gegen Datenbanken und
- Angriffe gegen einzelne Software-Produkte.

Indirekte Angriffe werden meist durch sog. Schadsoftware (engl. Malware) ausgelöst und werden durch Presseberichte deshalb häufiger im öffentlichen Leben wahrgenommen. Hierzu zählen selbstverständlich auch alle Arten von Viren, Trojanern und anderen schadhaften Software-Programmen, die nur den einen Zweck haben, ein System von der ursprünglich angedachten Funktionsweise in einen anderen, vom Angreifer gewünschten Modus operandi überzuführen.

Neulinge im Angriffsgeschäft sind oft zu unerfahren, um echte Angriffe durchzuführen, und geben sich nicht selten mit kleineren „Tests“ zufrieden, um ihre Neugier nach „anderen Welten“ zu befriedigen. Die meisten dieser unstrukturierten oder unkoordinierten Angriffe, sind zwar lästig, stellen in der Regel aber weder eine intellektuelle Bedrohung für ein Computer-System noch eine Herausforderung für dessen Absicherung dar. Diese Angriffsarten sind üblicherweise weder auf ein direktes Ziel hin geplant noch entsprechend gut vorbereitet, um wirklichen Schaden zu induzieren.

Was wird eigentlich angegriffen?

Beantwortet man sich diese Frage strukturiert, so sind schon viele Ansatzpunkte für sinnvolle Gegenmaßnahmen gegeben:

- Bekannte (oder noch nicht weit bekannte) Sicherheitsmängel
- (Erreichbare) Sicherheitsgrenzen
- Hardware- und Softwarefehler

Sicherheitsmängel sind zumeist unbeabsichtigt, aber typischerweise (sollten sie den Herstellern von Hardware und Software auch bekannt sein) undokumentiert, und jemand, der viel Zeit darin investiert, „einfach einmal nachzusehen, wie so etwas funktioniert“, wird nicht selten dadurch belohnt, dass er eine Schwachstelle findet, die er – technisches Wissen und die entsprechende Motivation vorausgesetzt – versuchtermaßen zu seinen Gunsten ausnutzen kann.

Sicherheitsgrenzen entstehen immer dann, wenn ein Software-Produkt an dessen dokumentierte Grenze und darüber hinaus „gepusht“ wird. Nicht selten sind Software-Programme gegen solche Verfahren nicht ausgerüstet und liefern kein Modell, um mit dieser „neuartigen“ Situation umzugehen. Ist diese Grenze erst einmal überschritten, so reagiert das Software-Produkt auf unvorhersehbare Art und Weise und ermöglicht so ggf. den Boden für dessen eigene Kompromittierung.

Softwarefehler entstehen bei unbedachtem Programmieren, bei der Verwendung nicht passender oder veralteter Software-Bibliotheken und insbesondere in Anbetracht nicht ausgereifter Software-Architektur insbesondere bei großen Entwicklungsprojekten. Typischerweise machen sich solche Fehler durch sog. Puffer-Überläufe (engl. buffer overflows) bemerkbar, die es erlauben, beispielsweise Nutzerberechtigungen auszuhebeln und damit unbemerkt Schadsoftware auf einen fremden Rechner zu platzieren und von dort zu laden.

Was sind Ziele und Motivationen der Angreifer?

Ziele und Motivationen hängen hier sehr eng zusammen. Oft reicht es für den Angreifer aus, einen Angriff durchzuführen, wobei das Ziel ziemlich unwichtig ist. Dennoch gibt es eine klare Unterscheidung nach den einzelnen Motiven, die das Treiben des Angreifers bestimmen:

Intellektuelle Motivation:

Hier besteht am aller ehesten die Möglichkeit, zwischen Cracker [x] und Hacker [y] zu unterscheiden. Es geht darum, wer „härter drauf“ ist: Das System oder der Angreifer. Finanzielle Aspekte spielen hierbei typischerweise keine Rolle. Erfolgreiche Angreifer, insbesondere auch in den vergangenen 20 Jahren, sind heute gerne als Sicherheitsexperten in Firmen oder bei Behörden tätig und haben damit ihr Tun sozusagen ex post legalisiert. Das Schadenspotential bei dieser Form der Motivation ist in aller Regel, es sei denn unbeabsichtigt, sehr gering, oft geben die Ausführenden den Betroffenen die entsprechenden Hinweise, wie sie ihr System diesbezüglich sicher machen können.

Persönliche Motivation:

Hier geht es im Wesentlichen um persönliche Rachemotive z. B. eines entlassenen Mitarbeiters oder um jemanden, der die Kontrolle über eine andere Person ausüben möchte, indem er auf dessen Rechner z. B. einen Keylogger [x] installiert. Das Schadenspotential ist als mittel- bis hochgradig einzustufen.

Politische Motivation:

Hier werden typischerweise solche Gruppierungen gefunden, die sich durch „spektakuläre Einbrüche“ in der Öffentlichkeit gut darstellen möchten oder aber ihre politischen und anderweitigen Anschauungen einer weiteren Öffentlichkeit preisgeben (aufoktroyieren) möchten. Das

Schadenspotential ist primär eher immaterieller Natur, es gibt aber auch Szenarien für finanzielle Sekundärgewinne.

Finanzielle Motivation:

Hier ist am ehesten der Übergang in die Wirtschaftskriminalität zu sehen, aber auch Erpressungen sind an der Tagesordnung. Bei dieser Form der Motivation ist das Schadenspotential häufig sehr groß. Diese Form der Bedrohung ist derzeit die am weitesten verbreitete und zeigt im Laufe der vergangenen vier Jahre signifikant steigende Tendenz.

Egozentrische Motivation:

Die meisten dieser Angriffsformen sollen nur zum Ärgernis des Angegriffenen dienen und richten sonst typischerweise keinen spezifischen Schaden an.

Wichtig für das eigentliche Angriffsverhalten sind a priori durchgeführte Risiko-Analysen der Angreifer. Im Gegensatz zu früher sind die Gefahren des Angriffes bekannt, das, was ein Angriff beim Betroffenen auslösen kann und auch die legalen Konsequenzen, wenn der Angreifer bei seinem Tun überführt wird:

Wichtig für die ego-motivierten Angreifer ist in der Regel das Ausmaß, mit welchem sie von einer breiten Öffentlichkeit wahrgenommen werden.

Finanziell motivierte Angreifer richten sich nach denjenigen Zielen aus, bei denen der „Return on Invest“ als am höchsten zu erwarten ist.

Grundsätzlich riskieren Angreifer aber nicht mehr Kopf und Kragen, sondern richten ihr Tun häufig nach der Einfachheit des Zugriffs (durchaus auch nach entsprechender „Vorarbeit“)aus.

Wie führen Angreifer einen Angriff aus?

(Vorbereitete) Angriffe auf IT-Infrastrukturen und die daran anhängenden entsprechenden Assets laufen üblicherweise in drei kategorisierbaren Schritten ab:

- **Schritt 1:** Gewinnen eines Überblicks über mögliche Angriffsziele, entsprechende Angriffspunkte und Beginn der Überprüfung
- **Schritt 2:** Zugriff und Versorgung mit der entsprechenden Berechtigungsstufe
- **Schritt 3**: Angriff im Kontext verschiedener Intentionen

Bei **Schritt 1** kümmert sich der Angreifer zunächst um das Besorgen entsprechender Informationen, die geeignet sind, das Ziel, den Punkt des Angriffs, die Taktik und die dabei auftretenden möglichen Probleme vorab zu identifizieren. Hierzu werden multiple Verfahren und sog. Tools eingesetzt, um die entsprechenden Informationen zu erhalten.

Stehen alle spezifischen Aspekte eines Angriffes fest, erfolgt im **Schritt 2** der Zugriff auf das zu kompromittierende System. Ist dieser Zugriff nicht erfolgreich, so wird er so oft mit veränderten Techniken solange wiederholt, bis er erfolgreich wird oder wegen Erfolglosigkeit eingestellt wird. Bei Erfolg muss der Angreifer sichergehen, dass er sich zum einen die für den Angriff notwendigen Rechte verschafft, zum anderen wird er alles daran legen, seine Spuren entweder zu verwischen („I was not there!“) oder so geschickt darzustellen, dass selbst ein unbedarfter Systemadministrator irgendwann einmal darüber stolpern muss („I definitively was there!“).

In **Schritt 3** schließlich wird die Umsetzung der eigentlichen Motivation versucht: Datendiebstahl, Datenmanipulation, Datenverfälschung, Datenlöschung, Defacement etc. stehen jetzt an und werden bis zum jeweils intendierten Erfolg vorangetrieben.

Prophylaxe und Postphylaxe

Es gibt nahezu unbegrenzte Möglichkeiten, Systeme vermeintlich sicher zu gestalten. In der Regel sind diese wohl beschriebenen Technologien den durchschnittlichen Angreifern jedoch eben so wohlbekannt, so dass sie nur in ungeübter Hand ein echtes Hindernis darstellen.

Gegen koordinierte Angriffe können folgende grundlegende Maßnahmen ergriffen werden:

- Implementierung der Filterung des einwärts wie auswärts gerichteten Netzwerkverkehrs
- Limitierung des Netzwerkverkehrs mittels IP-Routern oder sog. Intrusion Prevention Systemen (IPS)
- Implementierung und Monitoring des Netzwerksverkehrs mit Intrusion Detection Systemen (IDS)

Direkte Angriffe erfordern zunächst einmal die prinzipiellen Sicherungsmaßnahmen wie für die koordinierten Angriffe. Beunruhigend ist, dass die Ausdehnung der Angriffsszenarien auch auf normale IT-Services (z. B. E-Mail) hier am allergrössten ist (Phishing, Pharming etc.), so dass diese Angriffe an der Grenzlinie zu koordinierten und indirekten Angriffen ein sehr weites Spektrum potentieller Opfer betreffen kann, weshalb die spezifische Eindämmung umso schwieriger wird.

Indirekte Angriffe können zumindest durch den individuellen oder systemweiten Einsatz entsprechend geeigneter Anti-Malware-Software so weit reduziert werden, dass das tatsächliche Bedrohungsrisiko unter deren konsequenter Anwendung signifikant reduziert werden kann. (Die Sprache der statistischen Analyse zeigt jedoch, dass derzeit genau das Gegenteil der Fall ist.)

Durch öffentliche Aufklärung, aber auch durch das Verhindern der unbedachten Verbreitung von Skripten, die von sog. Script Kiddies zu einem unstrukturierten oder unkoordinierten Angriff umfunktioniert werden können, ist hier eine gute Chance zu sehen, langfristig zumindest auf der pädagogischen Ebene etwas zu erreichen.

Auf allgemeiner Basis können folgende zu behebende Schwachstellen identifiziert werden:

- Reduzierung der Information, die ein Computer oder ein Netzwerk nach innen oder nach aussen hin abgibt. Diese Informationen sind in der Regel nur für den internen Administratorenkreis relevant und können von diesen unter Einsatz geeigneter Tools auch ohne Interaktion des Nutzers erhalten werden. Auch Informationen, welches Betriebssystem Verwendung findet, sollen nicht nach aussen abgegeben werden.
- Schließen nicht benötigter Ports und Überwachen von Ports, die benötigt werden oder sich nicht anderweitig überprüfen lassen.
- Verhindern der Möglichkeit, an auch verschlüsselte Passwörter zu gelangen.

Durch moderne Methoden und die derzeit verfügbare Rechnerkapazität wird das Cracken von Passwortlisten eher zum Sport denn zur intellektuellen Herausforderung.
- Verhindern von externen Datenbankzugriffen. Insbesondere das Cross-Site-Scripting und das Injizieren fremden Codes in Datenbank-Abfragen ist eine beliebte Methode, um sich unerlaubt Zugang zu fremden Systemen zu verschaffen.
- Verhindern, dass Software Informationen über sich abgibt. Abgesehen von wenigen Ausnahmen sind Versions- oder Kompilationsfragen einzig für Softwareentwickler relevante Informationen, für Angreifer, die in der Regel sehr gut über versionsabhängige Schwachstellen Bescheid wissen, sind diese Informationen jedoch ein „gefundenes Fressen".

Was tun, wenn das Kind doch schon in den Brunnen gefallen ist?

An dieser Stelle helfen nur noch die Verfahren der Computer-Forensik [y]. Nach dem sog. S-A-P-Modell lässt sich die dann notwendige Ermittlung in drei Phasen einteilen:

- Secure-Phase (S)
- Analyse-Phase (A)
- Present-Phase (P)

In der **Secure-Phase** werden alle Informationen, die für die weiterführende Analyse der Daten vonnöten sind, abgesichert. Dabei muss strikt darauf geachtet werden, dass die vorliegenden Daten keiner von innen oder von außen zuzuschreibenden Veränderung durch den Prozess der Absicherung ausgesetzt werden, d. h. wie auch immer geartete Schreibzugriffe auf ein zu sicherndes System müssen a priori (z. B. unter Verwendung eines sog. Write Blocker) ausgeschlossen sein.

In der **Analyse-Phase** werden alle Daten auf Spuren hin sorgfältig analysiert und die so erhaltenen Ergebnisse objektiv bewertet.

In der **Present-Phase** schließlich werden die so erhaltenen Ergebnisse so zweifelsfrei wie möglich dargestellt, wobei zu berücksichtigen ist, wem ein solcher Bericht gegeben werden soll: Technisch meist unbedarften Entscheidern oder dem IT-Personal, welches sich in der Regel ein Bild vom eingetretenen Schaden machen kann.

Die sog. Incident Response setzt dabei eine intime Kenntnis moderner Angriffsmethodiken unter allen Betriebssystemen voraus. Aufgrund der Notwendigkeit, in praxi mindestens 10 Jahre Erfahrungen auf unterschiedlichen Betriebssystemen gesammelt zu haben, und aufgrund der beruflichen Superspezialisierung sind Computer-Forensik-(CF)-Experten eher rar gesät.

Derartige CF-Teams werden nunmehr versuchen, ein evtl. kompromittiertes System während des aktuellen Laufes (z. B. bei Unmöglichkeit der Abschaltung eines Krankenhaus-Informations-Systems) oder aber nach Herunterfahren desselben und nach Erstellen eines sog. forensischen Duplikats der zu untersuchenden Datenbasis (sog. Post-mortem-Analyse) zu untersuchen und die daraus ableitbaren Ergebnisse in einem Bericht (in Deutschland Empfehlungen, in den USA Level-I- bis –III-Assessment) zusammenzufassen. Dieser Bericht hat nicht nur die Aufgabe höchstmöglicher Objektivität der Interpretation der gefundenen Ergebnisse herzustellen, sondern auch u. U. für juristische Auseinandersetzungen vor Gericht tauglich zu sein.

Man muss sich aber dessen wohl bewusst sein, dass selbst die besten CF-Teams nicht immer erfolgreich in der Lage sind, die Kompromittiertheit eines Computer-Systems nachzuweisen, insbesondere dann nicht, wenn a priori keine oder nur unzureichende Security Policies verabschiedet waren oder aber der interne Umgang mit einem solchen System dermaßen viel Raum zu eigenständigem, unobservierten Handeln geboten hat, dass es für den Angreifer ein Leichtes gewesen sein musste, seine Spuren vollständig zu verwischen.

Zusammenfassung

Berücksichtigt man die unterschiedlichen Aspekte von Datenschutz und Datensicherheit nach dem Buchstaben des Gesetzes ebenso wie nach dem Grundsatz der Praktikabilität, lassen sich über den aktiven Einsatz von Security Policies sehr viele Bedrohungsszenarien dann ausschließen, wenn nicht nur die technischen Voraussetzungen dafür gegeben sind, sondern insbesondere auch das Bewusstsein des einzelnen Nutzers für das, was er tut und was er nicht tun darf, geschärft wird. Der informierte Nutzer ist ein wesentlicher erster Schritt zur Vermeidung von Bedrohungen.

Besteht die IT-Infrastruktur einer medizinischen Einrichtung nur aus der Sicherstellung zu bewältigender Software-Produktanforderungen, ist dies für einen aktiven Datenschutz und insbesondere die Datensicherheit nicht ausreichend. Nur durch die geplante Architektur prophylaktischer Massnahmen gegen möglichst jede Art von Bedrohungsszenario lassen sich Risiken nicht nur identifizieren, sondern auch minimieren. Hier leisten insbesondere die Grundlagen von ITIL [11] hervorragende Dienste.

Abschließend muss eingeräumt werden, dass sich trotz optimaler Vorbereitung nicht alle potentiellen Bedrohungen ausschließen lassen. Versagen alle Sicherungsmaßnahmen und tritt der Schadensfall eines erfolgreichen Angriffs ein, besteht nur noch die Möglichkeit, immediat mit einem Computer-Forensik-Team des Vertrauens zu reagieren, um Schlimmeres zu vermeiden. So besteht wenigstens die Chance, die übersehen Schwachstelle zu identifizieren und anhand der Sachlage in manchen Fällen sogar juristische Schritte zu erwägen.

Fußnoten

[1] Datenschutz: Aktuelle Definition nachzulesen unter http://de.wikipedia.org/wiki/Datenschutz

[2] Datensicherheit: Aktuelle Definition nachzulesen unter http://de.wikipedia.org/wiki/Datensicherheit

[3] Security Policies: Nachzulesen unter http://de.wikipedia.org/wiki/Security_Policy

[4] Social Engineering: Kevin D. Mitnick: Die Kunst des Einbruchs. MITP-Verlag, März 2006. ISBN-10: 3826616227 - ISBN-13: 978-3826616228; Kevin D. Mitnick: Die Kunst der Täuschung. MITP-Verlag, März 2006. ISBN-10: 3826615697 - ISBN-13: 978-3826615696.

[5] DDoS: Nachzulesen unter http://de.wikipedia.org/wiki/Denial_of_Service
[6] PoD: Nachzulesen unter http://de.wikipedia.org/wiki/Ping_of_Death
[7] Cracker: McKenzie Wark: Das Hacker-Manifest - A Hacker Manifesto. Beck-Verlag, März 2005. ISBN-10: 3406528759 - ISBN-13: 978-3406528750.
[8] Hacker: vgl. [7].
[9] Keylogger: Nachzulesen unter http://de.wikipedia.org/wiki/Keylogger http://de.wikipedia.org/wiki/Keylogger
[10] Computer Forensik: Alexander Geschonneck: Computer Forensik. dpunkt Verlag, 3. aktualisierte und erweiterte Auflage, 28. April 2008. ISBN-10: 3898645347 - ISBN-13: 978-3898645348-
[11] ITIL: Nachzulesen unter http://de.wikipedia.org/wiki/IT_Infrastructure_Library

Kontakt
Dr. Markus Mohr
CEO
ManaThea GmbH
Josef-Engert-Strasse 11 / II
BioPark 2
D-93053 Regensburg
Tel: +49 (0) 9 41 / 9 10 69 - 1 54
Fax: +49 (0) 9 41 / 9 10 69 - 1 69
info@manathea.de
www.manathea.de