Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: METHODIK

Schützen Sie sich vor professionellen gezielten Cyber-Angriffen

Stellen Sie sich vor, Sie besuchen eine internationale Produktmesse und erkennen zufällig bei einem der Anbieter ein Produkt, welches Ihrem bisherigen Verkaufsschlager auffallend ähnelt und zum halben Preis angeboten wird. Oder stellen Sie sich vor, Sie befinden sich mitten in den Verhandlungen zu einem Großauftrag oder versuchen ein strategisch wertvolles Unternehmen zu übernehmen und müssen erfahren, dass alle Ihre Angebote knapp unter- bzw. überboten werden. Und was wäre, wenn Ihr Produktionsleiter Ihnen gerade meldet, dass die Produktionslinie aufgrund eines unerklärlichen Computerfehlers ausgefallen ist und die Wiederherstellung mehrere Tage in Anspruch nehmen wird? Die genannten Beispiele sind keine hypothetischen Gedankenspiele, sondern reale Vorfälle, die bereits aufgetreten sind. Sie sind oftmals die Folge von Wirtschaftsspionage mittels professioneller gezielter Cyber-Angriffe.

Erfolgreiche Cyber-Angriffe verursachen mittelbare und unmittelbare Schäden, die sich letztlich finanziell auswirken. **Sie als Entscheidungsträger sind für den wirtschaftlichen Erfolg des Unternehmens verantwortlich** und müssen daher die ständige Überprüfung und Aktualisierung der IT-Sicherheitsmaßnahmen veranlassen und die Mittel dafür bereitstellen.

1 Gezielte Cyber-Angriffe

Im Zusammenhang mit professionellen gezielten Cyber-Angriffen hat sich der Begriff der „Advanced Persistent Threats (APT)“ eingebürgert, der eine spezielle Angriffsmethodik bzw. Ausprägungsform gezielter Cyber-Angriffe darstellt. Die konkrete Bedeutung variiert jedoch in verschiedenen Publikationen. In diesem Dokument wird folgende informelle Definition verwendet:

> *„Ein APT liegt dann vor, wenn ein **gut ausgebildeter Angreifer** mit Rückgriff auf große **Ressourcen** sehr **gezielt** ein Netz oder System angreift, sich dann in dem System ausbreitet, weitere Hintertüren einbaut und ggf. über **längere Zeit** Informationen sammelt oder Manipulationen vornimmt.“*

1.1 Opfer gezielter Cyber-Angriffe

Grundsätzlich stellen gezielte Cyber-Angriffe für jede Branche und jedes Unternehmen eine Bedrohung dar, das vertrauliche, geschäftskritische Informationen auf IT-Systemen verarbeitet oder dessen Erfolg von der Verfügbarkeit seiner IT-Systeme abhängt. Betriebsgeheimnisse, wie beispielsweise Forschungs- und Entwicklungsergebnisse, Herstellungsverfahren oder unternehmenspolitische Entscheidungen stehen dabei im Fokus der Angreifer. Das Bundesamt für Verfassungsschutz (BfV) stellt dies ebenfalls in Veröffentlichungen dar [1][2].

Aufgrund der Unterstützungsanfragen verschiedener Organisationen an das Bundesamt für Sicherheit in der Informationstechnik (BSI) und des aktiven Informationsaustausches, sowohl mit den Betroffenen als auch mit den in diesem Umfeld tätigen Experten (Computer Emergency Response Teams (CERT), Forensiker und Dienstleister), ist klar ersichtlich, dass ganze Branchen und deren Zulieferketten in Deutschland kompromittiert waren oder z. T. immer noch sind. Angegriffen werden nicht nur bekannte Großunternehmen sondern auch klein- und mittelständische Unternehmen (KMU), die beispielsweise in ihrem Marktsegment eine herausragende Position einnehmen oder die Rolle eines wichtigen Zulieferers für die zuvor genannten Großunternehmen innehaben.

Die vom BSI durchgeführte Cyber-Sicherheitsumfrage 2014 [3] stellt fest, dass etwa 56% aller befragten Unternehmen in den vergangenen 30 Monaten[1] Opfer eines Cyber-Angriffes wurden. Die Zuordnung der erfolgreichen Angriffe ist ohne intensive forensische Untersuchung schwierig, dennoch gehen 22% der befragten Unternehmen davon aus, eine Malware-Infektion aufgrund eines gezielten Cyber-Angriffes erlitten zu haben. 7% der befragten Unternehmen gaben an, Opfer eines expliziten APT-Hackings geworden zu sein.

Nach den Erkenntnissen des BSI, die aus der Bearbeitung von Vorfällen stammen, sind folgende Bereiche besonders gefährdet:

- Rüstungsindustrie
- Hochtechnologiebranche: Auto-, Schiffbau und Raumfahrt
- Forschungseinrichtungen
- Öffentliche Verwaltung

Wie auch das BfV in seinen Publikationen ausführt, ist dabei allerdings zu berücksichtigen, dass von einer sehr hohen Dunkelziffer ausgegangen werden muss.

1.2 Motivation der Angreifer

Professionelle gezielte Cyber-Angriffe verfolgen die Absicht, das **spezifisch ausgewählte Ziel** auszuspähen oder im Extremfall zu schädigen. Diese gezielten Cyber-Angriffe könnten sowohl aufgrund einer Konkurrenzsituation oder aus staatlichem Interesse erfolgen und werden mit allen zur Verfügung stehenden Ressourcen durchgeführt. Diese Ressourcen werden durchaus effizient eingesetzt, sodass ein stufenweiser Anstieg der Angriffsbemühungen bzw. der Angriffsqualität nachzuvollziehen ist.

Beispiele für die Absicht solcher gezielten Cyber-Angriffe sind:

- Wirtschaftsspionage
- Militärspionage
  Der Vorfall bei Lockheed Martin [4] verbindet sowohl Wirtschafts- als auch Militärspionage und verdeutlicht den finanziellen und zeitlichen Vorteil sowie den Wissenstransfer, der durch den Nachbau eines Kampfflugzeuges erzielt werden konnte.
- Politische Ausspähung
  Die NSA-Affäre [5] offenbart, dass gezielte Cyber-Angriffe aus allen Richtungen erfolgen können und eine Vielzahl verschiedener Zielsetzungen verfolgen.
- Sabotage
  Das Schadprogramm Stuxnet [6], dem die erfolgreiche Störung des iranischen Atomprogramms zugeschrieben wird, bleibt bis auf Weiteres das Paradebeispiel für einen Sabotageangriff.

1 Bezogen auf den Zeitraum der Umfrage vom 24.06.2014 bis 19.09.2014

1.3 Besonderheiten professioneller gezielter Cyber-Angriffe

Ein wesentlicher Aspekt der hier zugrundeliegenden Definition für APT ist die langfristige Ausrichtung des Angriffs. Der Angreifer beabsichtigt, so lange wie möglich im kompromittierten Netzwerk zu agieren. Um also keine Aufmerksamkeit zu erregen und eine Entdeckung zu vermeiden oder möglichst lange hinaus zu zögern, bereitet er sich sich umfassend vor und geht anschließend vorsichtig vor.

- Angriffsmethoden werden vor dem Einsatz modifiziert und geprüft, um sicher zu stellen, dass sie von aktuellen Standard-IT-Sicherheitsmaßnahmen nicht erkannt werden.
- Spuren werden verwischt.
- Offensichtliche Schäden oder Manipulationen werden zunächst vermieden.
- Für den Fall der Entdeckung werden Hintertüren vorbereitet.

Dies ist so erfolgreich, dass eine Kompromittierung meist erst nach mehreren Monaten und oft nicht durch den Betroffenen selbst, sondern in etwa 2/3 der Fälle [7] durch Externe aufgrund von Anomalien bemerkt wird. Studien zu diesem Thema sprechen von durchschnittlich 87 Tagen [8] – 229 Tagen [7] bis zur Feststellung des Angriffs. Dem BSI sind Einzelfälle bekannt, in denen die Angriffe 2-3 Jahre lang unentdeckt blieben. Während dieses Zeitraums ist ein kompromittiertes Netzwerk unter der vollen Kontrolle der Angreifer!

1.4 Vorgehensweise der Angreifer

Die Vorgehensweise der Angreifer lässt sich anhand der folgenden sieben Einzelschritte darstellen, die in der Fachliteratur [9] auch „Kill Chain“ genannt wird:

1. Aufklärung (Reconnaissance)
2. Erstellen eines Transportmediums für Exploit-Code (Weaponization)
3. Ausbringen des Exploits (Delivery)
4. Ausführen des Exploits (Exploitation)
5. Fußfassen im System (Installation)
6. Kontaktaufnahme zum Kontrollserver (Command and Control)
7. Daten sammeln oder Manipulationen vornehmen (Actions on Objective)

Dies macht deutlich, dass ein gezielter Cyber-Angriff gut vorbereitet und generalstabsmäßig durchgeführt wird. Es macht auch deutlich, dass der Angriff verschiedene Phasen umfasst, die jeweils unterschiedliche IT-Sicherheitsmaßnahmen erfordern. Einzelne Hersteller von IT-Sicherheitslösungen gehen daher dazu über, ihre Produkte zu erweitern und immer mehr verschiedene Schutzfunktionen zu integrieren.

1.5 Handlungsbedarf

Erfolgreiche Cyber-Angriffe verursachen mittelbare und unmittelbare Schäden, die sich letztlich finanziell auswirken. Bereits alleine die Bereinigung des Unternehmensnetzwerkes kann Monate in Anspruch nehmen und ist mit hohen Kosten verbunden. Diese Kosten sind individuell für jedes Unternehmen, können aber in der Regel kalkuliert werden. Der Schaden durch einen Informationsabfluss ist dagegen meist nicht bezifferbar. Er kann beispielsweise einen erheblichen langfristigen Verlust von Marktanteilen nach sich ziehen. Um diese Schäden zu verhindern oder wenigstens zu minimieren, müssen die IT-Sicherheitsmaßnahmen dieser Bedrohungslage angepasst werden.

Gezielte Cyber-Angriffe zeichnen sich dadurch aus, dass sie üblicherweise in der Lage sind, Standard-IT-Sicherheitsmaßnahmen zu umgehen. Daher müssen die bisherigen Lösungsansätze erweitert werden, um allen Phasen der „Kill Chain“ geeignete Gegenmaßnahmen gegenüber stellen zu können.

Dies bedeutet auch, die Möglichkeit zu akzeptieren, dass das Unternehmensnetzwerk bereits infiltriert sein könnte. Daraus folgt, dass neben der Abwehr der Angriffsversuche die schnellstmögliche Detektion und Eindämmung bereits erfolgreicher gezielter Cyber-Angriffe massiv an Bedeutung zunimmt und entsprechende Maßnahmen eingeführt bzw. verstärkt werden müssen.

2 Maßnahmen

Die nachfolgenden Ausführungen gehen davon aus, dass grundlegende Standard-IT-Sicherheitsmaßnahmen, wie beispielsweise die am Schutzbedarf orientierte Umsetzung der IT-Grundschutz-Kataloge [10] oder die Anwendung der Standards der ISO/IEC 2700x-Reihe [11] bereits vorhanden sind. Zusätzlich bietet die Cyber-Sicherheits-Veröffentlichung des BSI „Basismaßnahmen der Cyber-Sicherheit“ [12] einen pragmatischen Einstieg und liefert Anregungen für Standard-IT-Sicherheitsmaßnahmen. Sie werden daher in Kapitel 2.1 nur angerissen.

2.1 Standard-IT-Sicherheitsmaßnahmen

Die Schutzwirkung gegenüber gezielten Cyber-Angriffen kann zwar eingeschränkt sein, die Standard-IT-Sicherheitsmaßnahmen stellen aber auch dafür eine zusätzliche Hürde dar. Sie bilden somit einen verhältnismäßig einfach und kosteneffizient umzusetzenden Basisschutz, auf dem einige der erweiterten IT-Sicherheitsmaßnahmen aufsetzen können. Die Planung darüber hinausgehender Maßnahmen ist unzweckmäßig, solange den Angreifern aufgrund des fehlenden oder unvollständigen Basisschutzes eine offene Flanke präsentiert wird.

2.2 Strategische Entscheidungen durch das Management

Um erweiterte IT-Sicherheitsmaßnahmen etablieren oder anpassen zu können, die auch gegen gezielte Cyber-Angriffe wirken, müssen entsprechende Rahmenbedingungen geschaffen werden. Diese erfordern verschiedene strategische Entscheidungen durch das Management. Die folgenden „8 Leitfragen“ sind dafür exemplarische Beispiele:

- ✔ **Was muss geschützt werden? Was sind Ihre Kronjuwelen?**
  Die Einführung zusätzlicher oder die Anpassung bestehender IT-Sicherheitsmaßnahmen ist in der Regel mit hohen Kosten verbunden. Um einerseits eine angemessene Balance zwischen den Aufwänden und dem stets verbleibenden Restrisiko zu erreichen und um andererseits fundierte Entscheidungen treffen zu können, müssen die kritischen Geschäftsprozesse des Unternehmens, dessen kritische IT-Systeme und die schützenswerten Informationen identifiziert werden.
  Diese Analyse muss – abhängig von der Unternehmensstruktur und den IT-gestützten Geschäftsprozessen – auch Dienstleister, Zulieferer und Partner berücksichtigen.
- ✔ **Vor wem soll das Wissen und die Technik, die den Erfolg des Unternehmens ausmachen, geschützt werden?**
  Unternehmenspolitische Entscheidungen, wie der Abschluss von Großaufträgen, Joint Ventures oder die Ausgliederung von Unternehmenssparten bzw. die Übernahme fremder Unternehmen (-steile) können das Interesse von Konkurrenten oder Nachrichtendiensten wecken. Diese Entscheidungen sind nicht immer bei Ihrem IT-Sicherheitspersonal bekannt. Die Kenntnis derartiger Anlässe kann die Bewertung von Angriffsversuchen, wie beispielsweise von Spearphishing, entscheidend beeinflussen. Es ist also sinnvoll, eigene Planungen und Entscheidungen zu reflektieren und potenzielle Auswirkungen einer Risikoabschätzung zuzuführen und ggf. das IT-Sicherheitspersonal zu beteiligen.
- ✔ **Wer soll die Maßnahmen im täglichen Betrieb betreuen?**
  Auch bei überwiegend technisch realisierten IT-Sicherheitsmaßnahmen muss deren qualifizierte Betreuung sichergestellt werden. Die Effektivität einzelner Maßnahmen ist abhängig von der kontinuierlichen Aktualisierung der Detektionsparameter (Signaturen, Regelsätze). Darüber hinaus erfordern einzelne Produkte eine regelmäßige manuelle Auswertung und profitieren in besonderem Maße von eingesetzten Analyse-Spezialisten. Alternativ oder ergänzend kann die strategische

Entscheidung auch lauten, externe Dienstleister zu beauftragen. Es muss also die Frage der personellen Ressourcen geklärt sowie deren Befugnisse festlegt werden.

- ✔ **Wie viel ist dem Unternehmen der Schutz seines Erfolges wert?**
  Die wesentlichste Gestaltungs- und Einflussmöglichkeit, die Ihnen als verantwortlichem Entscheider innerhalb Ihres Unternehmens zur Verfügung steht, ist die Budgetierung der finanziellen Ressourcen für IT-Sicherheit. Negativ formuliert kann diese Entscheidung die Wirksamkeit der IT-Sicherheitsmaßnahmen massiv einschränken.

- ✔ **Welche Beschränkungen können den Mitarbeitern zugemutet werden, um den Erfolg des Unternehmens zu sichern?**
  Komfort und IT-Sicherheit korrespondieren nur schlecht miteinander. Um die identifizierten schützenswerten Informationen – bildlich gesprochen die Kronjuwelen des Unternehmens – zu verteidigen, sollte zumindest in besonders gefährdeten Teilbereichen die ausnutzbare Angriffsfläche minimiert werden. Dazu gehören auch die bei den Mitarbeitern eher unpopulären Entscheidungen, die Nutzerrechte zu beschränken, die Nutzung privater IT-Geräte (Bring your own Device (BYOD)) zu regeln oder ganze Netzbereiche voneinander oder vom Internet zu entkoppeln.

- ✔ **Welche organisatorischen und juristischen Vorbereitungen benötigt der Einsatz der (erweiterten) IT-Sicherheitsmaßnahmen?**
  In Kapitel 1.4 wurde geschildert, dass gezielte Cyber-Angriffe mehrere Phasen umfassen. Den einzelnen Schritten gelingt es häufig, die IT-Sicherheitsmaßnahmen zu umgehen oder aber sie werden nicht als Teil eines gezielten Cyber-Angriffes erkannt. Eines der wichtigsten Maßnahmenpakete ist daher das Monitoren, das Loggen und die Analyse / Korrelation der Einzelereignisse von möglichst vielen Sensoren.
  Dies erfordert jedoch verschiedene Vorbereitungen, wie die Berücksichtigung der Datenschutzbestimmungen, der Einbeziehung der Personalvertretung und klare Regelungen über die private Nutzung der unternehmenseigenen IT (Betriebsvereinbarung).
  Aufgrund der Komplexität des Themas kann es trotzdem dazu kommen, dass Indikatoren weder von den technischen Systemen noch von den eigenen Analysten erkannt werden. Dann ist es außerordentlich hilfreich, einer Information Sharing Initiative anzugehören, um relevante Benachrichtigungen zu erhalten oder anlassbezogen Fragen vertraulich stellen zu können.
  Dafür benötigt das eingesetzte IT-Sicherheitsteam wiederum die Befugnis, entsprechende Kontakte nutzen und ggf. (anonymisierte) Informationen zum eigenen Vorfall austauschen zu dürfen.

- ✔ **Was ist zu tun, wenn der Angriff dennoch erfolgreich war?**
  Auch wenn im Fall der Fälle Aufklärung, Eindämmung und Bereinigung eines Vorfalls Wochen oder sogar Monate in Anspruch nehmen können, so würde es zu unnötigen Verwirrungen und Komplikationen führen, wenn grundlegende Entscheidungen erst im Laufe des Vorfalls getroffen werden. Die Details eines Vorfalls sind nur begrenzt zu antizipieren. Trotzdem sollten Notfallpläne vorbereitet werden. Es sollten im Vorfeld sowohl Prozesse, Zuständigkeiten und Befugnisse festlegt als auch Unterstützungsmöglichkeiten eruiert werden.
  Dazu zählt einerseits die Einbindung interner Stellen, wie die des Datenschutzbeauftragten oder der Personalvertretung – soweit Mitarbeiter betroffen sind – andererseits aber auch externer Stellen, wie beispielsweise Provider, Sicherheits- und/oder Strafverfolgungsbehörden sowie spezialisierte Dienstleister (Forensik, Computer Emergency Response Team (CERT) u.a.).

- ✔ **Ist das inzwischen erreichte Schutzniveau immer noch ausreichend?**
  Um diese Leitfrage beantworten zu können, muss sowohl die allgemeine Bedrohungslage als auch die konkrete Gefährdung der IT-Sicherheit des Unternehmens bekannt sein. Die Nachbereitung erfolgreicher Cyber-Angriffe und die Auswertung abgewehrter Cyber-Angriffe bilden hierzu eine nicht zu vernachlässigende Voraussetzung. Dem gegenüber steht die regelmäßige Re-Evaluierung der IT-Sicherheitsmaßnahmen, beispielsweise in Form von Penetrationstest, Audits oder anlassunabhängigen, forensisch orientierten IT-Sicherheitsüberprüfungen. Anhand dieses Inputs kann dann die Risikoabschätzung aktualisiert und der Anpassungsbedarf bewertet werden.

2.3 Erweiterte IT-Sicherheitsmaßnahmen

Die konkrete Zusammenstellung der erweiterten IT-Sicherheitsmaßnahmen ist abhängig von den lokalen Gegebenheiten und der individuellen Gefährdungsanalyse. Dennoch gelten einige grundlegenden Empfehlungen.

- ✔ **Angriffsfläche reduzieren**
  Der Übergang von Standard-IT-Sicherheitsmaßnahmen zu erweiterten Maßnahmen ist bei dieser Empfehlung fließend. Sie beinhaltet verschiedene Ansätze. Beispielsweise sollte die Bekanntgabe interner technischer oder organisatorischer Informationen vermieden werden (Metainformationen in Dokumenten; Antwortverhalten von Diensten; etc.), um potenziellen Angreifern wenige Ansatzpunkte zu liefern. Dieses Ziel verfolgen auch solche Maßnahmen, die Schwachstellen und Sicherheitslücken schließen bzw. deren Ausnutzung verhindern sollen. Einen umfassende Systemhärtung rundet dieses Maßnahmenpaket ab.
- ✔ **Defense in Depth – Layered Defense**
  Wie in den Kapiteln 1.4 und 1.5 beschrieben versucht ein Angreifer bei gezielten Cyber-Angriffen immer tiefer in das Unternehmensnetzwerk einzudringen, um seinen Auftrag auszuführen. Da die Erfolgswahrscheinlichkeit hinsichtlich der Überwindung der Standard-IT-Sicherheitsmaßnahmen hoch ist, sollte eine vielschichtige IT-Sicherheitslösung, die auch eine laterale Ausbreitung im Netz detektiert, implementiert werden. Die verschiedenen Sensortypen und Einzelmaßnahmen sollten dabei den unterschiedlichen Phasen der „Kill Chain“ entgegen wirken.
- ✔ **Korrelation von Sensordaten**
  Durch die langfristige Ausrichtung der gezielten Cyber-Angriffe fällt es schwer, Einzelereignisse einem solchen Angriff zuzuordnen. Die Vielfalt der im vorhergehenden Aufzählungspunkt empfohlenen unterschiedlichen Ansätze sollte genutzt werden, um eine gemeinsame Korrelation zu ermöglichen und somit auch zeitlich voneinander abhängige Ereignisse zu erkennen.
- ✔ **Manuelle Auswertung**
  Gezielte Cyber-Angriffe sind oft individuell auf das Einsatzziel abgestimmt und können über neuartige Merkmale verfügen. Spezifische, eindeutige Signaturen stehen daher nur selten sofort zur Verfügung. Strebt man eine möglichst geringe Quote von False Negatives an, so führen die notwendigerweise offener definierten Detektionsparameter zu einer erhöhten Quote von False Positives. Die technische Erfassung und Bewertung von Ereignissen sollte daher unbedingt um eine manuelle Auswertung durch Spezialisten ergänzt werden.

Die beispielhaften Empfehlungen können durch eine Vielzahl von Produktlösungen, organisatorische und administrative Maßnahmen sowie durch extern erbrachte Dienstleistungen realisiert werden. Entscheidend ist jedoch, dass der eigene Bedarf möglichst präzise eruiert wird und kommerzielle Advanced Threat Protection (ATP)-Lösungen und ATP-Konzepte, die wiederum eine große Anzahl verschiedener Funktionalitäten beinhalten, genau dahingehend geprüft werden, wie gut der eigene Bedarf abgedeckt wird.

3 Fazit

Wie auch bei anderen Auseinandersetzungen entwickeln sich die Methoden der Cyber-Angreifer laufend weiter. Vorgehensweisen oder Tools, die ursprünglich bei gezielten Cyber-Angriffen eingesetzt werden, können später Anwendung bei ungezielten Angriffen finden. Die Konzeption und Umsetzung von Schutzmöglichkeiten kann dieser Entwicklung nur mit einer entsprechendem Verzögerung folgen. Um ein jederzeit ausreichendes Schutzniveau aufrecht zu erhalten, muss also die Risikoabschätzung zyklisch wiederholt und die IT-Sicherheitslösung ggf. angepasst werden.

IT-Sicherheit stellt also keinen statischen Zustand dar, sondern muss als ein ständiger Regelkreislauf, als ein andauernder Prozess verstanden werden!

4 Quellen und weiterführende Informationen

[1] BfV Arbeitsfeld Elektronische Angriffe , „Elektronische Angriffe mit nachrichtendienstlichem Hintergrund“,
http://www.verfassungsschutz.de/download/broschuere-2014-07-elektronische-angriffe-mit-nachrichtendienstlichem-hintergrund.pdf

[2] BfV Arbeitsfeld Wirtschaftsschutz, „Elektronische Attacken auf Informations- und Kommunikationstechnik“,
http://www.verfassungsschutz.de/download/faltblatt-2014-04-elektronische-attacken.pdf

[3] BSI-Veröffentlichung, „Ergebnisse der Cyber-Sicherheitsumfrage 2014“,
http://www.allianz-fuer-cybersicherheit.de/umfrage

[4] US Justizministerium, „Los Angeles Grand Jury Indicts Chinese National in Computer Hacking Scheme Allegedly Involving Theft of Trade Secrets“,
http://www.justice.gov/usao/cac/Pressroom/2014/105.html

[5] Zeit Online, „Snowden-Enthüllungen: Alles Wichtige zum NSA-Skandal“,
http://www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal/komplettansicht

[6] Symantec, „W32.Stuxnet Dossier“,
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[7] Mandiant, „M-Trends® 2014: Beyond the Breach“,
http://www.mandiant.com

[8] Trustwave , „Trustwave Global Security Report 2014“,
http://www2.trustwave.com/rs/trustwave/images/2014_Trustwave_Global_Security_Report.pdf

[9] M. Cloppert, "Security Intelligence: Attacking the Kill Chain,"
http://computer-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain/

[10] BSI-Veröffentlichung IT-Grundschutz, „IT-Grundschutz-Kataloge“,
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

[11] International Organization for Standardization, „ISO/IEC 27001 - Information security management“,
http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

[12] BSI-Veröffentlichung zur Cyber-Sicherheit, „Basismaßnahmen der Cyber-Sicherheit“,
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/risikomanagement/BSI-CS_006.pdf?__blob=publicationFile

[13] Mandiant, Veröffentlichung zu APT1,
https://www.mandiant.com/blog/mandiant-exposes-apt1-chinas-cyber-espionage-units-releases-3000-indicators/

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **info@cyber-allianz.de** gesendet werden.