INSIDERS KNOWLEDGE

Jahresrückblick 2012

1 Einleitung

In unserem Jahresrückblick 2012 fassen wir sich fortsetzende Trends und neue Entwicklungen im Bereich Informations- und IT-Sicherheit zusammen. Die durch zunehmende Vernetzung wachsende Komplexität von Systemen führt zu neuen Sicherheitslücken, möglichen Fehlern und einem höheren Anspruch an deren Nutzer. Gleichzeitig steigt der Wert von Informationen, Angriffe und Wirtschaftsspionage werden attraktiver. Diese Entwicklungen spiegeln sich in einer besseren Organisation von Cyberkriminellen und einer Zunahme von Sicherheitsvorfällen wieder.

Der Anspruch, sich mit Informationssicherheit zu beschäftigen, steigt für alle Nutzer, ob Privatperson, Mittelständler oder Großunternehmen. Auch auf zwischenstaatlicher Ebene gewinnt das Thema an Relevanz, denn es lässt sich ein Wettrüsten für einen möglichen "Cyberwar" beobachten. Neue Spionagetrojaner wie Duqu und Flame haben gezeigt, dass Stuxnet kein Einzelfall, sondern viel mehr der Beginn einer neuen Ära der verschleierten Kriegsführung war.

2 Schatten-IT, Risiken der Cloud und Eingebettete Systeme

2.1 Schatten-IT

Unter Schatten-IT versteht man im klassischen Sinne IT Komponenten die nicht die Unternehmens-IT bereitgestellt und administriert, welche jedoch dennoch im Rahmen von Geschäftsabläufen eingesetzt werden. Häufig werden Cloud-Dienste wie DropBox und Google Docs dieser Kategorie genauso zugeordnet wie z.B. selbst aufgesetzte Server in einer Entwicklungsabteilung.

Die Risiken, die von diesen Komponenten für ein Unternehmen ausgehen dürfen nicht unterschätzt werden:

- Die Verlagerung von Geschäftsprozessen auf externe (Cloud-)Dienstleister ohne eine hinreichende Evaluierung durch die IT- und die Rechtsabteilung gefährdet die Vertraulichkeit, die Integrität und langfristig auch die Verfügbarkeit und Wiederverwendbarkeit von unternehmenseigenen Daten
- Daten und Prozesse außerhalb des Geltungsbereichs der IT-Abteilung können nicht in Prozesse zur Gewährleistung der Informationssicherheit (Backups, Softwareaktualisierungen, Überprüfung von Zugriffsberechtigungen, etc.) eingebunden werden
- Von der IT nicht gewartete Geräte, die an das Unternehmensnetzwerk angeschlossen werden, bringen nicht kalkulierbare Risiken mit sich. Sie können bereits mit Viren oder Trojanern infiziert sein, oder durch veraltete Softwareversionen Einfallstor für diese Schädlinge sein
- Schatten-IT Komponenten werden häufig von einer oder wenigen Personen installiert und gepflegt, sollte diese Person ausfallen ist nicht gewährleistet, dass diese Dienste weiter genutzt werden können

2.2 Globalisierte Ausfälle von Cloud-Diensten

Sobald der Zugriff auf kritische Daten von der Verfügbarkeit einer Verbindung zu einem externen Server oder Dienstleister abhängt entstehen neue, nicht steuerbare Risiken. Ausfälle der lokalen Internetverbindung können die Durchführung von Geschäftsprozessen verzögern oder verhindern. Hurricane Sandy verursachte an der

Ostküste der USA weitreichende Stromausfälle, die zu Störungen in den Rechenzentren von Amazon und anderen Cloud-Dienstleistern führten. Dadurch konnten Kunden und Dienstleister, die von diesen Diensten abhängig waren, über längere Zeiträume ihre Arbeit nicht fortsetzen. Eine lokale Katastrophe führte so zum globalen Ausfall einer Vielzahl von Diensten.

2.3 Eingebettete Systeme als neue Form der Schatten-IT

Gibt es auch Hardware- und Softwarekomponenten, die von der IT ausgerollt werden, jedoch trotzdem Eigenschaften von Schatten-IT teilen? Leider ja, und besonders das letzte Jahr hat die Risiken einiger dieser Komponenten sehr deutlich aufgezeigt. Viele moderne Bürogeräte vom Voice-over-IP Telefonen über Drucker bis zu Stechkartengeräten, die über IP mit dem Netzwerk verbunden sind, bringen ähnliche Risiken mit sich. Rein technisch sind diese Geräte kleine Multi-Purpose Computer, die zur Steuerung entsprechender Geräte dienen. In diesem Umfeld wird das Thema Sicherheit oft vernachlässigt, was häufig zu unentdeckten Risiken führt:

- Ende 2011 stellte der Forscher Ang Cui einige Angriffe auf HP-Drucker [2] vor, mit denen es möglich war, einen Netzwerkdrucker in eine persistente Hintertür in einem Unternehmensnetzwerk zu verwandeln. Der Angriff setzt lediglich voraus, dass ein modifiziertes Dokument auf dem Drucker ausgedruckt wird, danach beginnt der Drucker - für den Anwender unsichtbar - Kontakt zum Angreifer aufzunehmen und Verbindungen in das Unternehmensnetzwerk zu ermöglichen
- Ende April wurde ein undokumentierter Administrator Account [5] in Netzwerkequipment des Herstellers RuggedCom bekannt, dieses Equipment ist speziell für Industrieanwendungen wie Anlagensteuerung und Verkehrsleitsysteme ausgelegt
- Im Juli entdeckte Sicherheitsforschers Collin Mulliner [3] tausende Geräte im europäischen Mobilfunknetz, darunter GPRS Ethernet Router, Smart Meter, IP-Kameras, Straßenverkehrssysteme und KfZ-Ortungshardware deren Administrationsoberfläche nicht einmal passwortgeschützt war
- Ende 2012 stellte Ang Cui einen weiteren Angriff [4] vor, sein Ziel diesmal: Die weit verbreiteten Cisco VoIP Telefone. Der Angriff setzt zwar einen kurzen physikalischen Zugriff auf das Gerät voraus, erlaubt aber nicht nur dauerhaften Zugriff von außen, sondern auch das Abhören von Telefonaten und der direkten Umgebung des Telefons

Diese Beispiele zeigen, dass auch bei der Bereitstellung von Hardware verstärkt auf Sicherheit geachtet werden muss. In fast keiner Organisation werden Drucker, Telefone, Netzwerkequipment und andere eingebettete Systeme regelmäßig aktualisiert und überprüft. Auch bei der Entsorgung dieser Geräte, die zum Teil auch Speichermedien mit sensiblen Firmendaten enthalten, darf der Sicherheitsaspekt nicht vernachlässigt werden.

Für alle der oben genannten Beispiele haben die Hersteller bereits Sicherheitsupdates zur Verfügung gestellt. In den meisten Unternehmen wurden diese jedoch bis heute nicht ausgerollt.

3 Hacking as a Service & Malware Inc.

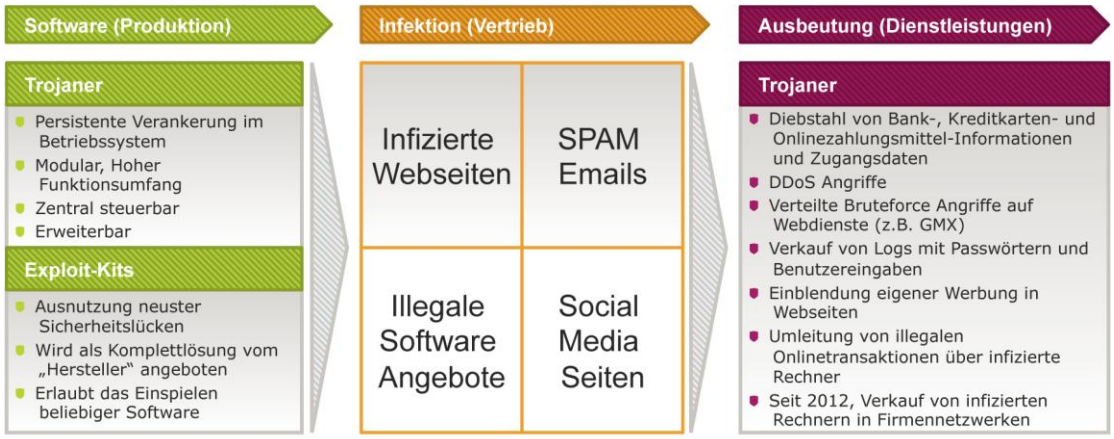

Bild 1 Die "Wertschöpfungskette" von Cybercrime und Botnetzen

3.1 Die Industrialisierung von Cybercrime, Malware und Botnetze

Botnetze, Onlinebetrug und der Diebstahl von Bankdaten haben 2012 eine besonders große Rolle gespielt. Besonders fällt die weiter steigende Professionalität der Akteure in diesem Bereich auf. Ähnlich der Industrialisierung, die sich zu Beginn in drei Sektoren Rohstoffgewinnung, Verarbeitung und Dienstleistung unterteilen ließ, zeichnet sich in der Onlinekriminalität eine ähnliche Arbeitsteilung ab.

Die Entwickler von Trojanern stellen die nötige Infrastruktur bereit um infizierte Rechner zu monetarisieren. Die von ihnen entwickelte Software muss jedoch erst einmal auf die Rechner potentieller Opfer gelangen und auch dazu gibt es weitere Entwickler die sogenannte Exploit-Kits entwickeln und vermarkten. Diese Softwarepakete umfassen mehrere Exploits für Sicherheitslücken und eine Schnittstelle mit Hilfe derer diese in Webseiten eingebunden werden können. Nach der Ausführung einer solchen Sicherheitslücke kann ein Trojaner auf den Rechner eines Opfers nachgeladen werden. Diese beiden Komponenten stellen die Grundlage für alle weiteren kriminellen Handlungen dar.

Der zweite Sektor befasst sich mit dem Verteilen der oben genannten Trojaner und setzt dabei vorwiegend auf illegal gehandelte Exploit-Kits. Als Botnetz bezeichnet man viele, mit einem Trojaner infizierte, Rechner die unter der Kontrolle einer einzelnen Person oder Gruppe stehen. Durch das hacken fremder Webseiten oder Phishing-Webseiten auf welche Opfer mittels SPAM-Emails, Social Media Seiten und Google Optimierung gelockt werden, versuchen diese Kriminellen möglichst viele Rechner zu infizieren.

Die Betreiber dieser Botnetze haben ein hohes Interesse daran ihr Netz möglichst gewinnbringend einzusetzen. Dies hat 2012 verstärkt dazu geführt, dass der Funktionsumfang von Schadsoftware stark zugenommen hat. Diese Funktionen bedienen den dritten Sektor, die Dienstleistungen. Mit einer Schadsoftware infizierte Computer wurden im vergangenen Jahr hauptsächlich für folgende Zwecke missbraucht:

- Diebstahl von Bank-, Kreditkarten- und Onlinezahlungsmittel-Informationen
- Ausspionieren der Zugangsdaten zu Onlineshops, Spielen und anderen Webseiten

- Distributed-Denial-of-Service Attacken, um Webseiten lahm zu legen und deren Besitzer zu erpressen
- Verteilte "Bruteforce" Angriffe, bei denen die Passwörter von Onlineaccounts durch das Ausprobieren verschiedener Varianten geknackt werden sollen (z.B. Angriff auf über 3000 GMX E-Mail Accounts [5])
- Andere Passwörter werden häufig durch das Mitschreiben von Tastatureingaben ermittelt, da die Analyse dieser Dateien jedoch zeitaufwändig ist, werden diese häufig in 100 bis 1000 Rechner-Logs Bündeln weiterverkauft
- Die Werbeeinblendungen in Browsern von infizierten Rechnern werden häufig durch Werbung ersetzt, die dem Botbetreiber Geld bringen
- Um bei illegalen Aktivitäten im Internet schwerer zurückverfolgt werden zu können werden diese Aktivitäten häufig über infizierte Rechner "umgeleitet", so erscheint es, als würde der Akteur an diesem Rechner sitzen
- Besonders schockierend war ein Bericht von Brian Krebs [6], nach dem eine russische Webseite mit dem Namen "Dedicatexpress" gezielt infizierte Rechner aus Unternehmensnetzwerken für einstellige Dollarbeträge zum Kauf anbot

Der Vertrieb dieser aus Botnetzen hervorgehenden "Dienstleistungen" wird vorwiegend über russisch- und chinesischsprachige Internetforen organisiert. Die einzelnen Akteure handeln durchaus auch untereinander, so kaufen "neue" Botnetzbereiber Kapazitäten bestehender Botnetze ein um mehr SPAM verschicken zu können.

Ein Trend, der 2012 besonders zugenommen hat war die Vermietung ganzer Botnetze oder einzelner infizierter Computer. Die Tatsache, dass die Betreiber dieser Netze dieses Jahr begonnen haben gezielt Rechner in Firmennetzwerken an Dritte zu verkaufen ist für Unternehmen eine neue Bedrohung. Folgt man der Entwicklung im letzten Jahr, ist anzunehmen, dass diese Entwicklung kein isoliertes Phänomen darstellt, sondern den nächsten logischen Schritt in der Evolution von Botnetz-Organsiation: Der Vertrieb von infizierten Rechnern zur Industriespionage.

3.2 Malware auf Mobiltelefonen

Die zunehmende Verbreitung von Smartphones hat zu einer neuen Gattung von Malware geführt. Die Einführung von SMS-basierten Zwei-Faktor Authentifizierungen wie zum Beispiel mTAN machen die auf dem Smartphone befindlichen Daten besonders wertvoll. Es sind mindestens zwei Kampagnen bekannt, in denen im Jahr 2012 Kombinationen aus PC und Smartphone Malware eingesetzt wurden um die Kontodaten und die für Transaktionen nötigen mTANs [16] auszuspionieren.

3.3 Der Faktor Mensch spielt eine entscheidende Rolle bei der Verteilung von Schadsoftware

2012 hat einen Trend weiter hervorgehoben, dass Angriffe zunehmend technische Sicherheitsmaßnahmen umgehen indem sie gezielt auf den Nutzer zugehen. Dabei reichen die Strategien der Angreifer von ausgetüftelten Banking-Trojaner die falsche Kontostände anzeigen, Phishing-Emails mit persönlichen Daten aus sozialen Netzwerken über Anrufe mit Anleitung zur Installation von Remote-Access Software. Letztlich hat der Nutzer die Kontrolle über seine Daten und seinen PC, sodass ein

Angreifer die Suche, den Kauf oder die Entwicklung von teurer Schadsoftware umgehen kann indem er den Nutzer überzeugen kann diese selbst zu installieren.

Email Phishing wird weiterhin im Namen von bekannten Portalen wie Ebay, Paypal oder großen Banken durchgeführt. In qualitativ immer höherwertigeren E-Mails werden die Nutzer gebeten ihre Login-Daten anzugeben oder ihre Passwort einzugeben. Auch in sozialen Netzwerken nehmen die Fälle zu, bei denen präparierte Links Opfer auf gefälschte Seiten führen und private Daten oder Kreditkarteninformationen abfragen.

Verstärkt traten in diesem Jahr auch "Ransomware" Angriffe auf, bei denen Schadsoftware das Opfer aus dem eigenen PC aussperrt und eine Lösegeldsumme verlangt, damit der PC wieder freigeschaltet wird. Anonyme Bezahlsysteme wie uCash, Paysafe oder Western Union machen dies möglich. Beispiele hierfür sind Dorknet, Paysafe- und der BKA Trojaner [7].

4 Verlust von Betriebsgeheimnissen und Kundendaten

4.1 Der Preis verlorener Datensätze

Auch im vergangen Jahr fielen wieder eine Reihe von Unternehmen durch den Verlust von kundenbezogenen und geheimen Daten auf, nicht immer war dies auf Hackerangriffe zurückzuführen, in vielen Fällen waren die Unachtsamkeit der Mitarbeiter [17] oder schlecht entwickelte Software [18] der Auslöser.

Die Kosten für verlorene Datensätze setzen sich aus mehreren Faktoren zusammen. Zum Einen können enorme Kosten [19] durch Strafzahlungen bei Verstößen gegen Datenschutzauflagen entstehen, zum Anderen ist der Schaden der Dritten entsteht [18] schwer abzusehen. Neben möglichen Schadensersatzansprüchen müssen betroffene Unternehmen mit einem langfristigen Imageschaden [26] rechnen.

4.2 Industriespionage erreicht die Zulieferkette

Den medienwirksamen Fällen von Industriespionage im Jahre 2011 folgen 2012 viele Beispiele, bei denen es Angreifer auch auf kleinere Unternehmen abgesehen hatten. Dabei ging es unter Anderem um den Diebstahl von Technologieinformationen [20] oder Produktzeichnungen [21]. Nachdem sich große Unternehmen immer besser gegen Hacking und Industriespionage schützen, erreichen die Angriffe jüngst auch verstärkt deren Zulieferer [27]. Durch eng vernetzte IT- und Entwicklungsprozesse stellen Sicherheitsvorfälle bei Zulieferern eine unmittelbare Gefahr für deren Kunden dar. In Zulieferverträgen fehlt jedoch häufig eine Verpflichtung zur Gewährleistung der Informationssicherheit beider Parteien.

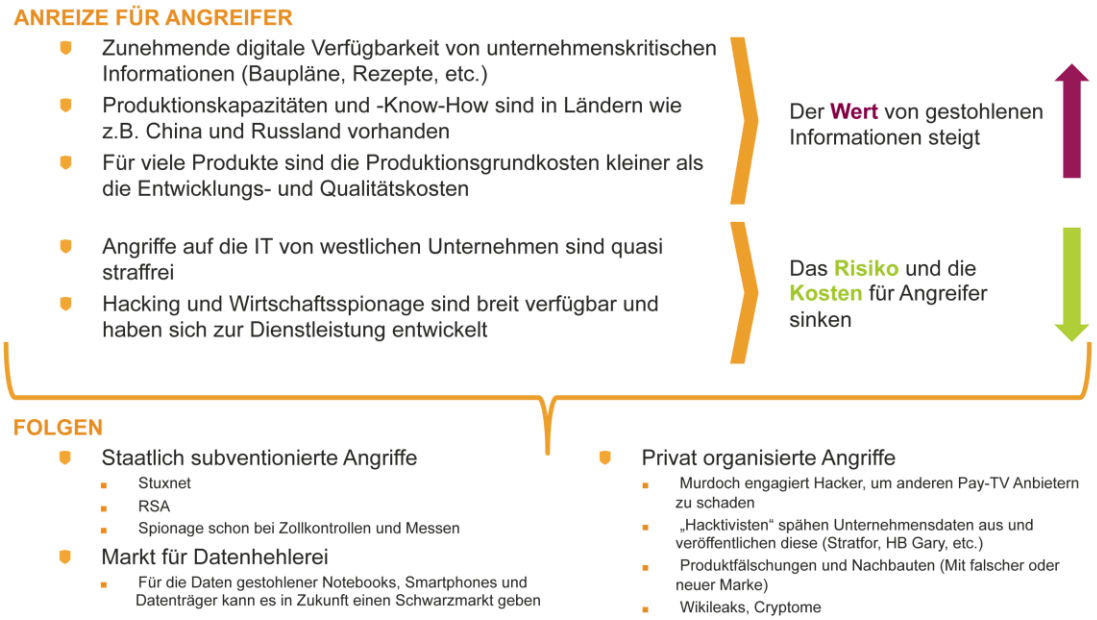

Bild 2 Industriespionage als Relation von Kosten und Nutzen für den Angreifer

4.3 Social Engineering als Angriffsvektor für Industriespionage

Social Engineering ist die gezielte Manipulation von Menschen mit Hilfe einer Reihe von Methoden, die das Opfer nicht merken lassen sollen, dass es manipuliert wurde. Social Engineering erfolgt per Email, am Telefon oder persönlich.

Gezielte Angriffe auf Unternehmen griffen ausnahmslos auf diese Strategien zurück, um bestehende Sicherheitsmechanismen zu umgehen und Zugang zu Firmendaten, Netzwerken oder Bankdaten von Unternehmen zu erlangen. Die Methoden variieren und werden meist in Koordination mit technischen Angriffen eingesetzt, doch an einer kritischen Stelle ist es der Mensch, der unwissend oder fahrlässig die Tür zu weiteren Daten oder Zugängen ermöglicht.

Manipulierte USB-Sticks [22], präparierte Links in Emails oder sozialen Netzwerken und manipulierte Dateianhänge werden dem Opfer untergejubelt, indem geschickte Lügen den Nutzer überzeugen, die Schadsoftware auszuführen:

- Unbekannte haben auf einem Parkplatz des niederländischen Chemiekonzerns DSM [22] mehrere USB-Sticks mit Schadsoftware platziert
- Auch Stuxnet [23] setzte für die Erstinfektion offenbar auf USB-Sticks
- Ein Spionagefall bei der indischen Marine [24] ist auf verseuchte USB-Sticks zurückzuführen
- Im Iran und angrenzenden Ländern [25] hat Symantec einen Wurm entdeckt, der gezielt SQL-Datenbanken manipuliert und sich über USB-Sticks weiter verbreitet

5 Medienaufmerksamkeit für Hacktivismus und Politik

5.1 Hacktivismus und Cybercrime in den Medien

2012 stieg das öffentliche Interesse an Cybercrime, Hacktivismus und den Verlust von Daten weiter. Der andauernde Prozess um Wikileaks-Gründer Julian Assange [9] war, die angedrohte Veröffentlichung von Steuerdaten des amerikanischen

Präsidentschaftskandidaten Mitt Romney [10] durch Anonymous, und die politisch motivierten Angriffe auf amerikanische Banken durch die islamische Gruppe Izz ad-din Al qassam [11], wurden von der gesamten Presse und nicht nur dem Ressort Technik verfolgt. Auch Skandale um Datenlecks und Sicherheitslücken in weit verbreiteter Software schaffen es verstärkt in Tageszeitungen und Abendnachrichten, das Thema gewinnt an gesellschaftlicher Relevanz.

5.2 Medien als Opfer von Angriffen

Die Online-Auftritte von Reuters [12] und Al-Jazeera [13] wurden nach Hackerangriffen dazu missbraucht, um politische Meinungen zu verbreiten. Die Aktivisten setzten dabei nicht mehr auf medienwirksame Angriffe und Ziele, sondern nutzen die Webseiten der Medien direkt um auf ihre Anliegen hinzuweisen. Innerhalb von kurzer Zeit waren die Veränderungen rückgängig gemacht, die öffentliche Wirkung hielt jedoch noch länger an.

6 Cyberwar im Wandel

2012 hat ein neues Zeitalter des Cyberkrieg eingeläutet, nachdem die USA aufgrund eines New York Times Berichtes zugaben, die Hersteller der Stuxnet Malware [14] zu sein. Neben Stuxnet wurden in 2011 und 2012 weitere Malware-Programme entdeckt, die aufgrund ihrer Bauweise staatlichen Geheimdiensten zugeordnet werden konnten. Hinter den Namen "Duqu", "miniFlame", "Gauss [33]" und "Flame [34]" stecken eine Reihe von Trojanern, Datensammlern und Spionagetools, die anhand ihrer Dateinamen benannt sind und dank aufwändigen Bauweise nur mit hohem finanziellen Aufwand hergestellt worden sein können. Gefunden und analysiert werden diese Tools von Antivirus Herstellern wie Kaspersky oder F-Secure, meist auf Rechnern in Nahen Osten, beispielsweise dem Iran [35].

Mit der steigenden Komplexität und höheren Ausgaben wurde eine Art "Kalter Krieg" der Rüstungsmächte über Cyberwaffen losgetreten, viele Veröffentlichung dienen in erster Linie der Abschreckung anderer Parteien. Auch andere Staaten machen großflächig von Spionagesoftware Gebrauch um Dissidenten und andere "Straftäter" aufzuspüren, beispielsweise die FinFisher Software [15] in Ägypten oder Bahrain. In Deutschland sind seit den Veröffentlichungen des Chaos Computer Club zum "Staatstrojaner" in 2011 keine neuen Informationen bekannt geworden.

International, in der EU als auch auf Landesebene werden Richtlinien für den Umgang mit Cyberangriffen [28] eingeführt. Auch für Rüstungsunternehmen wird Cyberkrieg ein sehr lukratives Geschäftsfeld, da inzwischen große Aufträge in den USA und anderen Ländern vergeben werden. Beispielsweise hat Lockheed Martin, die auch schon Opfer eines Cyberangriffs wurden, einen Auftrag in Höhe von $454 Millionen [29] vom US Department of Defence erhalten haben. Auch die deutsche Bundeswehr [30] bereitet sich auf einen Krieg im Netz vor, eine Truppe ist bereits seit 2006 im Aufbau.

Eine Diskussion über Konsequenzen von Cyberangriffen wurde im August losgetreten, als Harald Koh vom State Department darstellte, dass es sich bei Cyber-Angriffen um kriegerische Akte handelt, die einen Vergeltungsschlag [31] rechtfertigen. Da Cyberangriffe jedoch Staaten nicht eindeutig zuzuordnen sind, und Angriffe von Privatpersonen auf Unternehmen, beispielsweise zur Industriespionage,

ähnliche Software und Sicherheitslücken nutzen und Staatsgrenzen überschreiten, ist dies eine unklare und gefährliche Aussage.

Dennoch können Sicherheitslücken in kritischer Infrastruktur, beispielsweise den Steuerungseinheiten von Kraftwerken [32], dazu führen, dass staatliche Angreifer einem Land schweren Schaden zufügen können. Bisher ist ein solcher Angriff in der westlichen Welt nicht vorgekommen und Vorfälle konnten als Missverständnisse ausgeräumt werden. Dennoch ist ein Fokus auf die Verbesserung der Sicherheitsmaßnahmen in diesen Systemen zu begrüßen: Da Updates in diesem Umfeld dort sehr aufwändig und kostenintensiv sind, führen viele Betreiber diese ohne externen Druck nicht durch.

7 Herausforderungen für Unternehmen im Jahre 2013

Digital abgelegte Informationen gewinnen weiter an Bedeutung, fast sämtliches Know-How in modernen Unternehmen ist elektronisch verfügbar. Phänomene wie Cloud-Dienste beschleunigen Kommunikation und Kollaboration, führen aber auch zu einer Externalisierung von Informationen und den damit verbundenen Risiken. Genügten vor wenigen Jahren noch Sicherungskopien lokaler Server, wächst heute die Notwendigkeit einer Dateninventur, um den Überblick verteilter Daten und Prozesse zu wahren.

Komplexe Schnittstellen zwischen Prozessen und Unternehmen schaffen neue Risiken für Datenlecks und Hackerangriffe. Die Kompetenz von IT Abteilungen wird sich in Zukunft stärker daran messen lassen, wie sie das Spagat zwischen Bedienbarkeit, Sicherheit und Nachhaltigkeit meistert. Die Kommunikation dieses Dilemmas und transparente Entscheidungsprozesse sind essenziell um Mitarbeiter für diese Themen zu sensibilisieren und die Einhaltung von Regeln und Richtlinien sicher zu stellen.

7.1 Informationssicherheit als Teil des Risikomanagements

Bild 3 Informationssicherheit als Teil des unternehmerischen Risikos

Informationssicherheit und die daran eng angegliederte Sicherheit der IT-Infrastruktur sind in vielen Unternehmen allein die Aufgabe der IT-Abteilung. Dieser Zustand ist jedoch nicht zukunftsfähig: Entscheidungen über die Vernetzung des Unternehmensnetzes mit Zulieferern und Kunden werden nicht von der IT entschieden, sondern entstehen aus dem Geschäftsalltag heraus. Die dabei entstehenden Risiken können durch die IT Abteilung identifiziert, bewertet und den zur Abstellung entstehenden Kosten gegenübergestellt werden. Die Entscheidung welche Risiken tragbar sind und welche nicht muss jedoch die Unternehmensführung im Rahmen des Risikomanagements treffen.

8 Verweise

[1] http://insidersknowledge.com
[2] http://ids.cs.columbia.edu/sites/default/files/CuiPrintMeIfYouDare.pdf
[3] http://www.heise.de/newsticker/meldung/Scan-in-Mobilfunknetzen-foerdert-tausende-ungeschuetzte-Geraete-zu-Tage-1653619.html
[4] http://www.youtube.com/watch?v=f3zUOZcewtA
[5] http://seclists.org/fulldisclosure/2012/Apr/277
[5] http://www.heise.de/newsticker/meldung/Spam-Versand-ueber-gehackte-GMX-Konten-1635150.html
[6] http://krebsonsecurity.com/2012/10/service-sells-access-to-fortune-500-firms/
[7] http://www.heise.de/newsticker/meldung/BKA-Trojaner-zapft-Webcam-an-1636582.html
[8] http://www.isssource.com/stuxnet-loaded-by-iran-double-agents/
[9] http://www.wired.com/threatlevel/2012/06/assange-seeks-asylum/
[10] http://blog.eset.com/2012/09/06/low-tech-romney-tax-return-hack-could-be-lesson-in-physical-security
[11] http://www.informationweek.com/security/attacks/bank-of-america-website-slows-after-isla/240007581
[12] http://www.heise.de/newsticker/meldung/Falsche-Syrien-Berichte-im-Reuters-Blog-1660299.html
[13] http://www.guardian.co.uk/media/2012/sep/04/al-jazeera-website-hacked?newsfeed=true
[14] http://www.itworld.com/security/279652/us-admits-cyberattacks-iran-others
[15] http://www.heise.de/newsticker/meldung/Trojaner-made-in-Germany-spioniert-in-Bahrain-1652460.html
[16] https://threatpost.com/en_us/blogs/new-fraud-ring-operation-high-roller-targets-rich-062612
[17] http://www.welt.de/wirtschaft/article109795382/Patientendaten-offenbar-bei-Raucherpause-verschlampt.html
[18] http://www.heise.de/newsticker/meldung/Unister-Fall-Moeglicherweise-Kreditkartendaten-mangelhaft-gesichert-1772677.html
[19] https://threatpost.com/en_us/blogs/massachusetts-hospital-agrees-pay-15m-after-stolen-laptop-hipaa-violation-091912
[20] http://www.welt.de/wirtschaft/article106217762/Mit-Geheimwaffen-gegen-die-Produktpiraten.html
[21] http://blog.eset.com/?p=13194
[22] http://www.heise.de/newsticker/meldung/USB-Spionagekoeder-Niederlaendische-Firma-beisst-nicht-an-1641190.html
[23] http://www.isssource.com/stuxnet-loaded-by-iran-double-agents/
[24] http://www.heise.de/security/meldung/Indische-Marine-bestaetigt-Sicherheitsleck-1632142.html
[25] http://www.heise.de/newsticker/meldung/Wurm-manipuliert-Datenbanken-im-Iran-1753143.html
[26] http://www.heise.de/newsticker/meldung/LinkedIn-wegen-Passwort-Leck-verklagt-1622142.html
[27] http://www.bbc.co.uk/news/technology-20310342
[28] http://www.heise.de/newsticker/meldung/EU-plant-Meldepflicht-fuer-Cyber-Attacken-1756475.html
[29] http://www.lockheedmartin.com/us/news/press-releases/2012/may/isgs-DC3-EITS-0503.html
[30] http://www.spiegel.de/netzwelt/netzpolitik/cyberwar-die-bundeswehr-kann-nun-auch-cyberkrieg-a-836991.html
[31] http://www.washingtonpost.com/world/national-security/us-official-says-cyberattacks-can-trigger-self-defense-rule/2012/09/18/c2246c1a-0202-11e2-b260-32f4a8db9b7e_story.html
[32] http://arstechnica.com/security/2012/10/backdoor-in-computer-controls-opens-critical-infrastructure-to-hackers/
[33] https://www.securelist.com/en/blog/208193767/Gauss_Nation_state_cyber_surveillance_meets_banking_Trojan
[34] http://www.heise.de/security/meldung/Windows-Update-kompromittiert-1605393.html
[35] http://www.f-secure.com/weblog/archives/00002403.html