Medienimpulse
ISSN 2307-3187
Jg. 53, Nr. 3, 2015

Cyber Crime & Cyber War – "Part of the Game": Cyber Security, Quo Vadis?

Karl H. Stingeder

Welche Rolle spielt Cyber Crime gegenwärtig? Was unterscheidet Cyber Crime von Cyber War? Wie muss Cyber Security gestaltet sein, um effektiven Schutz nachhaltig zu gewährleisten? Cyber Crime-Aktivitäten kennzeichnen sich häufig durch eine einfache Zugänglichkeit von betrügerischem Know-How und technischen Hilfsmitteln. Bedingt durch eine schleppende und mangelhafte Umsetzung von koordinierten Gegenmaßnahmen, resultieren Cyber-Delikte in einem Low-Risk und High-Reward Szenario für Cyber-Kriminelle. Je organisierter und spezialisierter ein Cyber-Crime-Netzwerk gestaltet ist, desto größer wird das Schadenspotenzial. Cyber Crime ist der Überbegriff für betrügerische Aktivitäten über das Internet. Diese stützen sich auf das Vorbild von "traditionellen" Offline-Kriminalitätsverhaltensmustern, welche durch das technologische Spektrum des Internets einfach zugänglich sind. Nichtsdestoweniger ist es die

technische Ausführung der Delikte, die ein wesentliches Unterscheidungsmerkmal zwischen Online- und Offline-Betrug bildet. Auch steht die für organisierte, kriminelle Verbindungen, so auch für Regierungen oder Terrororganisationen geringere Hemmschwelle für eine militärische Instrumentalisierung des Internets im Brennpunkt von Cyber Security. Erfolgen Cyber Crime Aktivitäten unter dem Anspruch der Verfolgung politischer Ziele, sprechen wir von Cyber War. Nachhaltige, gegen Cyber Crime und Cyber War gerichtete Cyber Security-Maßnahmen finden in einem hochdynamischen Umfeld statt. Cyber-Kriminelle sind im Regelfall logistisch und finanziell gut ausgestattet. Viele werden von Regierungen unterstützt. Cyber Crime-Player verfügen über weitreichende technische Fähigkeiten, sodass sie maßgeschneiderte Schadprogramme (Malware) für ihre Ziele entwickeln können. Aktuell fehlt vielen Unternehmen und öffentlichen Institutionen das Bewusstsein für die Notwendigkeit von Abwehrsystemen. Ein Cyber Security-Fokus auf Präventivmaßnahmen ist weder ausreichend noch nachhaltig.

What roles does cyber crime play today? What differentiates cyber crime from cyber war? How must cyber security be organized in order to effectively ensure sustainable protection? Cyber crime activities are frequently characterized by the easy accessibility of fraudulent know-how and technical means. Due to the sluggish and inadequate implementation of coordinated countermeasures, cyber crimes are a low-risk and high-reward scenario for cyber criminals. The more organized and specialized a cyber crime network, the greater the potential for damage. In fact, cyber crime is the umbrella term for fraudulent activities via the World Wide Web. These rely on the model of "traditional" offline criminal behavior

patterns, which are easy to access thanks to the technological spectrum of the Internet. Nonetheless, it is the technical execution of the crime that represents a crucial distinguishing characteristic between online and offline fraud. Furthermore, from the point of view of organized crime, governments and terror groups, a lower inhibition threshold for a military exploitation of the Internet is a focal point of cyber security. As soon as cyber crime activity is the means by which to achieve political goals, it is called cyber war. Sustainable measures directed against cyber crime and cyber war take place in a highly dynamic environment. Cyber criminals are usually well-equipped in terms of logistics and financial resources. Many are supported by governments. Cyber criminals have wide-ranging technical expertise, which enables them to develop customized malware to accomplish their goals. At present, many companies and public sector entities do not fully realize how imperative defense systems are. Cyber security focus on purely preventive measures is therefore neither sufficient nor sustainable.

I Der Beitrag auf Deutsch

Nach sieben Jahren E-Commerce Berufserfahrung [1] und mehr als drei Jahren Erfahrung mit E-Commerce Betrugsprävention steht für mich fest: Cyber Crime, Cyber War und Cyber Security sind integrale Bestandteile des wirtschaftlichen und technologischen Ökosystems. Im Zuge regelmäßiger so genannter Anti-Money Laundering Schulungen – angesichts der an Zahlungsmittel-Dienstleistern gelegten Vorgabe mit den gesetzlichen Rahmenbedingungen des Zahlungsdienstegesetzes (ZaDiG) (vgl. Bundeskanzleramt 2015) und der Richtlinie der Zahlungsdienste bzw. Payment Service Directive (PSD) (vgl. Europäische Kommission 2015) der Europäischen Union konform zu gehen – konnte ich bereits zwischen 2008 und 2011 im Zuge von Schulungen bei paysafecard erstmals in die Welt der Cyber Security eintauchen. E-Commerce Betrugspräventions-

Mechanismen spielen im Zuge meiner Payment Service Provider Sales-Tätigkeit bei PayUnity – PayLife Bank GmbH/SIX Payment Services (Austria) GmbH – seit 2012 bis heute eine große Rolle: (Online-) Kreditkartenbetrug sowie Betrug im Zusammenhang mit Kunden- und Bezahldaten erhalten eine größer werdende, wirtschaftliche Tragweite, da das Online-Einkaufen in einem vom Internet durchdrungenen Alltag immer selbstverständlicher wird. Welche Rolle spielt Cyber Crime gegenwärtig? Was unterscheidet Cyber Crime von Cyber War? Und wie muss Cyber Security gestaltet sein, um effektiven Schutz vor Cyber-Bedrohungen nachhaltig zu gewährleisten?

Der Begriff Cyber Crime umfasst betrügerische Aktivitäten über das Internet. Diese stützen sich meiner Meinung nach auf "traditionelle" Verhaltensmuster bekannter "Offline-Betrugsdelikte", welche durch die technologischen Möglichkeiten des Internets ausgefeilt werden bzw. einfach zugänglich sind. Cyber Crime kann somit auch als technisches "Mittel zum Zweck" von illegalen Aktivitäten per se betrachtet werden. Somit ist tatsächlich die Ausführung des Kriminaldelikts ein wesentliches Unterscheidungsmerkmal zwischen Online- und Offline-Betrug. Werden Cyber Crime-Aktivitäten zu politischen Zwecken instrumentalisiert, z. B. wenn Hacker von Regierungen angeheuert werden, so sprechen wir von Cyber War. Generell kann die Hemmschwelle für organisierte, kriminelle Verbindungen, Regierungen oder Terror-Organisationen, das Internet militärisch zu instrumentalisieren, als gering eingestuft werden.

Die Relevanz und der Nutzen einer nachhaltigen und integrierten Antwort auf transnationale Cyber Crime- sowie Cyber War-Aufkommen sind (für mich) offenkundig. Cyber Crime-Aktivitäten kennzeichnen sich häufig durch eine einfache Zugänglichkeit von betrügerischem Know-How bzw. erleichterte Bezugsmöglichkeiten von Schadprogrammen (Malware). Bedingt durch eine schleppende und mangelhafte Umsetzung von koordinierten Gegenmaßnahmen, resultiert Cyberkriminalität in einem Low-Risk und High-Reward Szenario für Cyber Crime-Player. Fast jeder kann, eine gewisse kriminelle Energie und ein rudimentäres IT-Wissen vorausgesetzt, im sogenannten Darknet (vgl. Bleuth 2015) Malware

kaufen oder Botnetze mieten. (vgl. Stingeder 2015) Sensible Datenquellen können auch ohne Malware mittels Social Media-Plattformen oder einer simplen Google-Suche angezapft werden. "In this effort, online search tools and social networking have been a godsend to the attackers. [...] Just type the name into an Internet search engine and you can get everything from that executive's resume to the name of her daughter's pet iguana. As cybersecurity expert Gary McGraw wrote, >The most impressive tool in the attackers' arsenal is Google.<" (Singer/Friedmann 2014: 57)

Je organisierter und je spezialisierter ein Cyber Crime-Netzwerk desto höher das Schadenspotenzial. So wurde Ende Juni 2015 in Österreich ein Netzwerk aus Cyberkriminellen zerschlagen, das über mehrere Jahre hinweg mittels Malware TAN-Codes ausspionierte. 60 Beschuldigte sollen tausende Betrugshandlungen begangen haben. Der wirtschaftliche Schaden: mindestens zwei Millionen Euro. Alle österreichischen Großbanken seien von den Attacken betroffen. (vgl. derStandard.at 2015)

Ein weiterer ins Auge stechender Wesenszug von Cyberkriminalität ist die an Fahrt aufnehmende Größe und Frequenz von Cyber Crime-Aufkommen und des daraus resultierenden, wirtschaftlichen Schadens. Laut der 2015 veröffentlichten Global State of Information Security Survey ist die sogenannte Compound Annual Growth Rate (CAGR) der anerkannten Sicherheitsvorfälle seit 2009 um 66 % angestiegen. Die in der Studie befragten Teilnehmer gaben in der Erhebung für das Jahr 2014 in Summe 42,8 Millionen erkannte Sicherheitsvorfälle an, was eine Steigerung von 48 % im Vergleich zu den 2013 identifizierten Vorfällen entspricht. (vgl. PwC 2015) "Einer der größten Händler Nordamerikas wurde ausgerechnet in der Einkaufszeit vor Weihnachten im Jahr 2013 Opfer eines Datendiebstahls im großen Stil. Cyber-Diebe manipulierten Point-of-Sale-Systeme (POS-Systeme) und gelangten so an die Daten von 40 Millionen Kunden sowie an die persönlichen Daten von weiteren 70 Millionen Kunden. (vgl. Krebs 2014) Was die Menge an sensiblen Daten betrifft, die in Zusammenhang mit diesem Vorfall gestohlen wurden, handelt es sich um einen der größten Datendiebstähle der Geschichte." (Peterson 2015a)

Eine, durch meinen Blickwinkel betrachtet, entweder fehlende oder nur mangelhaft umgesetzte Cyber Security-Strategie erleichtert einzelnen Playern und organisierten Gruppen die profitträchtige Umsetzung von Cyber Crime. Das Ziel ist der illegale Erhalt von monetärem Kapital, sensiblen Daten oder – hier wieder aus meinem Blickwinkel des Berufsalltags eines E-Commerce-Spezialisten – das betrügerische Erschleichen von leicht wiederverkäuflichen Sachgütern (z. B. der Wiederverkauf von betrügerisch erlangten und hochpreisigen Elektronikprodukten wie Tablets oder Smartphones über Ebay) mittels gestohlener Bezahldaten. Abgesehen von auf Privatpersonen fokussierten Betrugsaktivitäten während des Online-Einkaufs, zielen organisierte Cyberkriminalität-Aktivitäten auch auf die Infiltration von Smartphones, Notebooks und PCs sowie auf Infiltrierung sensibler Überwachungs- und Steuerungssysteme ab, wie z. B. die bereits erwähnte Penetration von POS-Systemen der US-Kette Target im Jahr 2013.

Dabei sind Schlüsselstellen in der Privatwirtschaft sowie auch verwundbare Punkte bei staatlichen Institutionen und im Bankensektor stets im Fadenkreuz von Cyberkriminellen. (vgl. ebd.)

Ich bin der Überzeugung, dass eine effektive Bekämpfung von Cyber Crime und Cyber War einer koordinierten und Instanzen übergreifenden Zusammenarbeit bedarf. Aus heutiger Sicht wären folgende zwei Maßnahmen hilfreich:

1. Auf Basis eines breit gestreuten Maßnahmenkatalogs muss ein nachhaltiges Bewusstsein für Datensensibilität und vorhandene Risikopotenziale geschaffen werden.
2. Wichtiger Schlüssel bei der Bekämpfung von Cyber Crime und Cyber War ist eine multidimensionale Zusammenarbeit zwischen nationalstaatlichen Institutionen, intra- und supranationalen Instanzen z. B. das 2013 in Den Haag gegründete Europäische Zentrum der Cyberkriminalität, (vgl. Europäische Kommission 2013) Interpol und der Privatwirtschaft.

Hier wurden in den letzten Jahren erste Schritte in die richtige Richtung gesetzt, aber es bleibt viel Luft nach oben. Statische Patentrezepte sind wenig praxistauglich. Nachhaltige, gegen Cyber Crime und Cyber War gerichtete Cyber Security-Maßnahmen finden stets in einem hochdynamischen Umfeld statt. "Cyber-Kriminelle sind sehr gut

organisiert und mit ausreichend finanziellen Mitteln ausgestattet. Viele von ihnen werden bekanntermaßen von Regierungen unterstützt. Sie verfügen über weitreichende technische Fähigkeiten, sodass sie maßgeschneiderte Malware für bestimmte Ziele entwickeln können. Außerdem sind sie in der Verfolgung ihrer Ziele gnadenlos." (Petersen 2015b)

Technische Entwicklungen, die Cyber Crime-Gefahrenpotenziale bereithalten – man denke hier an das aktuell in aller Munde und häufig zitierte "Internet der Dinge" – sowie auch innovative Cyber Crime-Taktiken- und Cyber War-Strategien müssen adäquat identifiziert und analysiert werden. Nach vorgenommener Risikobewertung sollen Gegenmaßnahmen entwickelt und an die Schlüsselinstanzen ausgegeben werden, welche transparent in vorhandene Kommunikationskanäle eingespielt und durch Exekutivinstanzen umzusetzen sind. An dieser Stelle sollte ein wechselseitig befruchtender "Cyber Security"-Kreislauf ins Rollen gelangen: auf Basis der praktischen Erfahrung der Exekutivorgane sowie in Folge von transparenten Feedback-Rückkopplungs-Mechanismen (somit sind die Urheber der Maßnahmenkataloge über die Auswirkungen der Strategie mit der operativen Umsetzung im Bilde) besteht das ultimative Ziel darin, maßgeschneiderte Abwehrmaßnahmen zu entwickeln, die über die bloßen Präventionstaktiken des Cyber Security-Status Quo hinaus gehen. Nur mit Hilfe einer mehrdimensionalen, multilateralen und gut abgestimmten Zusammenarbeit wird es möglich sein, Cyber Crime und Cyber War Playern auf gleicher Augenhöhe zu begegnen.

Auf Basis vieler Gespräche mit Geschäftspartnern und Webshop-BetreiberInnen – im Zuge meiner E-Commerce Berufserfahrung der letzten Jahre – hat sich ein starkes Interesse an Cyber Crime, Cyber War und Cyber Security entwickelt. Wesentlicher Bestandteil meines operativen Tagesgeschäfts ist die Bewusstseinsbildung bei UnternehmerInnen (in deren Rolle als WebshopbetreiberInnen). Hier gilt es, die Augen für die vorhandenen Gefahren- und wirtschaftliche Schadenspotenziale von Cyber Crime zu öffnen. Häufig münden meine

Beratungsgespräche mit Kunden in einem Erwachen aus dem "Cyber Security Dornröschenschlaf". Wichtige Fragen vieler Kunden für die Erörterung der Gefahrenpotenziale sind in diesem Kontext: Welche erprobten Werkzeuge gibt es (weit über E-Commerce Fraud-Prävention hinaus), um das "Sicherheitsnetz" gesamtheitlich engmaschiger zu knüpfen? Welche Anti-Cyber Crime Strategien und Maßnahmen gegen Internet-Wirtschaftskriminalität bestehen aktuell?

Gegenwärtig liegt der Fokus der meisten Unternehmen und öffentlichen Institutionen bei der Implementierung von IT-Sicherheit im Rahmen von Präventivmaßnahmen. Allerdings fehlt das Bewusstsein für die Notwendigkeit einer Strategie für den Fall, dass Sicherheitsnetze durchdrungen werden. Häufig liegt es schlichtweg am nicht vorhandenen Wissen ob der dringlichen Notwendigkeit und den Konsequenzen von inexistenten Abwehrsystemen. P.W. Singer und Allan Friedman bringen eine der möglichen Wurzeln dieses fehlenden Verständnisses in ihrem Buch "Cybersecurity and Cyberwar" gut auf den Punkt: "But the world is still mostly led by 'digital immigrants', older generations for whom computers and all the issues the Internet age presents remain unnatural and often confusing." (Singer/Friedmann 2014: 4-5). Egal ob alt oder jung, wir alle sollten uns vor Augen führen, dass IT-Umgebungen heute deutlich angreifbarer sind als noch vor wenigen Jahren. Wir erinnern uns: In einer Zeit als Begriffe wie "Cloud-Computing", das "Internet der Dinge" oder "Big Data" noch nicht existierten bzw. noch nicht Teil des Laien-Sprachgebrauchs waren und UnternehmerInnen sich nach Installation von Firewall und Virenscanner durch deren IT-Abteilungen sicher wähnten. Neil MacDonald, Vizepräsident der Gartner Inc., empfiehlt: "Investieren Sie in Ihre Ressourcen zur Reaktion auf Angriffe, entwickeln Sie einen Prozess, mit dem Sie schnell die Tragweite und die Auswirkung eines erkannten Eindringens erkennen können, und sorgen Sie für die entsprechende personelle Ausstattung." (Peterson 2015a)

Fazit: Quo vadis, Cyber Crime, Cyber War und vor allem: Quo vadis, Cyber Security? Dass es hoch an der Zeit für EntscheiderInnen – aus allen Bereichen – wäre, Verantwortung für die IT-Sicherheit "in den eigenen vier

Wänden" zum Wohle der Gemeinschaft zu übernehmen, steht für mich fest. Die Notwendigkeit einer nachhaltigen Umsetzung von Cyber Security-Abwehrmaßnahmen zeigt sich dadurch dass immer häufiger Zahlungssysteme, Kundendaten sowie sensible Überwachungs- und Steuerungssystemen das Ziel von Cyber-Kriminellen werden, die immer intelligenter vorgehen. Einerseits wird sich die Öffentlichkeit der Cyber-Kriminalität und der Cyber-Risiken mit jedem großen und erfolgreichen Cyber-Angriff mehr und mehr bewusst (vgl. ebd.), anderseits fehlt es bei vielen EntscheiderInnen an Schlüssel-Instanzen vielerorts weiterhin das benötigte Cyber Security-Problembewusstsein: Wir können jederzeit Ziel eines Cyber-Angriffs oder einer Bedrohung werden.

II Der Beitrag auf Englisch

After seven years of working in e-commerce and more than three years working in e-commerce fraud prevention, it is clear to me that cyber crime, cyber war and cyber security are integral components of the economic and technological ecosystem. Between 2008 and 2011 at paysafecard, over the course of regular training courses on Anti-Money Laundering – within the framework of the Payment Services Providers Act (ZaDiG) (cf. Bundeskanzleramt 2015) in Austria and the EU's Payment Service Directive (PSD) (cf. European Commission 2015) – I was able to delve into the world of cyber security. As part of my role in payment service provider (PSP) sales at PayUnity since 2012 (the PSP of PayLife Bank GmbH/SIX Payment Services (Austria) GmbH), e-commerce fraud prevention has played an important role: (online) credit card fraud and fraud relating to customers and payment data is gaining increasing economic scope. This is because online shopping is becoming more and more customary in everyday life. What role does cyber crime play today? What differentiates cyber crime from cyber war? How must cyber security be organized in order to effectively ensure sustainable protection?

The term cyber crime encompasses fraudulent activities via the Internet. In my opinion, these are based on "traditional" offline criminal behavior patterns and are easy to access/becoming more sophisticated thanks to

the technological possibilities of the Internet. Cyber crime could therefore be viewed as the technical "means to an end" of illegal activities per se. For this reason, it is the technical execution of the crime that represents a crucial distinguishing characteristic between online and offline fraud. As soon as cyber crime activity becomes the means by which to achieve political goals, it is termed cyber war. In general, from the point of view of organized crime, governments and terror groups, the inhibition threshold for a military exploitation of the Internet can be regarded as low.

The impact and benefits of a sustainable, integrated response to transnational cyber crime and cyber war are apparent (to me). Cyber crime activities are often characterized by the easy accessibility of fraudulent know-how and malware. Due to the sluggish and inadequate implementation of coordinated countermeasures, cyber crime is a low-risk and high-reward scenario for cyber criminals. Virtually everyone these days can purchase malware or rent botnets (cf. Stingeder 2015) on the so-called Darknet, assuming they have a certain criminal energy and rudimentary knowledge of IT. (cf. Bleuth 2015) What's more, sensitive data sources can even be tapped without malware – through social media platforms or by using a simple Google search. "In this effort, online search tools and social networking have been a godsend to the attackers. [...] Just type the name into an Internet search engine and you can get everything from that executive's resume to the name of her daughter's pet iguana. As cybersecurity expert Gary McGraw wrote, "The most impressive tool in the attackers' arsenal is Google." (Singer/Friedmann 2014: 57)

The more organized and specialized a cyber crime network, the greater the potential for damage. For instance, a network of cyber criminals was destroyed in Austria in late June 2015. Over a number of years, the group had been spying out TAN codes by means of malware. 60 defendants have supposedly committed thousands of defraudations resulting in a financial loss of two million Euros. All the big Austrian banking houses were affected. (cf. derStandard.at 2015)

Another striking trait of cyber criminality can be seen in the increasing magnitude and rate of cyber crime incidence and the resulting economic

loss. According to the Global State of Information Security Survey published in 2015, the Compound Annual Growth Rate (CAGR) of recognized security incidents have increased about 66 % since 2009. Interviewed participants gave a total sum of 42.8 million recognized security incidents for the year 2014, which is an increase of 48 % in comparison to incidents identified in 2013. (cf. PwC 2015). One of the biggest retailers in North America fell victim to large-scale data theft in 2013 – just in the run-up to Christmas. Cyber criminals manipulated point-of-sale (POS) systems and obtained data from around 40 million customers as well as personal data from 70 million customers. (cf. Krebs 2014) As to the quantity of sensitive data stolen during this incident, it is one of the largest data thefts in history. (cf. Peterson 2015a)

In my opinion, either a complete lack of cyber security strategy or inadequately implemented strategy facilitates a profitable execution of cyber crime for individuals or organized groups. The goal is to illegally obtain monetary funds, sensitive data or – again, from my perspective as an e-commerce specialist – easily resaleable material goods (e.g. high-priced electronic consumer products such as tablets or smartphones via Ebay) via stolen payment data. Apart from fraudulent activities that target consumers in online shopping, organized cyber crime activities focus on infiltrating smartphones, notebooks and PCs, as well as on penetrating sensitive surveillance and monitoring systems e.g. the aforementioned infiltration of POS systems of US retail giant Target in 2013.

Furthermore, key points in the private sector as well as vulnerabilities at governmental institutions are constantly in cyber criminals' sights (cf. ibid.)

It is my belief that an effective control of cyber crime and cyber war requires coordinated cooperation across instances. From our present position, the following two measures would be helpful:

1. Based on a widespread package of measures, a sustainable awareness for careful data management and existing risk potentials must be developed.
2. An important key to countering cyber crime and cyber war is multidimensional collaboration between governmental institutions, as well as with intra- and supranational entities, e.g. the

European Cybercrime Centre founded in 2013 in The Hague – (cf. European Commission 2013), Interpol, and players from the private sector.

Over the last few years, there have been a few initial steps in the right direction, but there is still plenty of room for improvement. Static panaceas are hardly practical, while sustainable countermeasures combating cyber crime and cyber war take place in a highly dynamic environment.

Cyber criminals are well-organized and usually well-equipped in terms of logistics and financial resources. Many are supported by governments. Cyber criminals have wide-ranging technical expertise, which enables them to develop customized malware to accomplish their goals. They are also merciless in pursuing their objectives. (cf. Petersen 2015b) Technical developments that are at risk of cyber crime – speaking here of the oft-cited "Internet of Things", as well as innovative cyber crime tactics and cyber war strategies - must be adequately identified and analyzed. A timely development and deployment of countermeasures must follow directly after risk assessment. Such measures must be transparently integrated into existing communication channels and properly executed. Ultimately, a mutually beneficial "cyber security" cycle should start rolling at this stage: based on field experience from executive players and as a result of transparent feedback mechanisms (so that the creators of package measures are kept informed about the results of their operative strategy), the ultimate goal is to develop and deploy tailor-made defensive measures. Measures that will go far beyond the mere prevention tactics of present-day cyber security. Only with the aid of a multidimensional, multilateral and well-aligned cooperation will it be possible to meet cyber crime and cyber war on a level playing field.

Over the course of many conversations with business partners and customers throughout my work in e-commerce over the past few years, I have developed a strong interest in cyber crime, cyber war and cyber security. An essential part of my day-to-day business is raising awareness for my customers (in their role as webshop operators). It is a case of opening people's eyes to the existing dangers of cyber crime and the

potential economic loss that results. My consultations often lead to an "awakening" in the field of cyber security. Many clients ask the following important questions: which field-tested tools are available (often far beyond e-commerce fraud prevention) to spin the "security net" more tightly overall? Which anti-cyber crime strategies and measures can currently be obtained?

At present, most companies and public sector entities are still focusing merely on preventive cyber security measures. However, many entities often do not recognize the necessity of deploying countermeasures to safeguard their systems in case of a security network breach. There is frequently a lack of knowledge about the need for countermeasures and the potential consequences of their non-existence. P.W. Singer and Allan Friedman put in a nutshell one of the possible roots of this lack of awareness in their book "Cybersecurity and Cyberwar": "But the world is still mostly led by 'digital immigrants', older generations for whom computers and all the issues the Internet age presents remain unnatural and often confusing." (Singer/Friedmann 2014: 4-5) Regardless of how young or how old one might be, we must all realize that IT environments today are far more vulnerable compared to as recently as a few years ago. Let’s take a look back: in a time when terms like "cloud computing", the "Internet of Things" or "Big Data" were either not yet coined or not part of the layman’s language. In a time when entrepreneurs and corporate executives thought themselves safe as soon as firewall and virus scanners were installed by their IT departments. Neil MacDonald, Vice President of Gartner Inc., recommends a significant investment in resources to counter cyber threats. He also urges developing a process by which to swiftly identify the scope and ramifications of cyber intrusions. (cf. Peterson 2015a)

Bottom Line: Quo vadis, cyber crime, cyber war and particularly: Quo vadis, cyber security? It is beyond dispute that it is high time for decision makers across the board to accept responsibility for IT security within their "own four walls" for the good of all. The urgent need for a sustainable implementation of cyber security countermeasures is

illustrated by a growing number of sophisticated cyber threats targeting payment systems, payment and user data as well as sensitive surveillance and monitoring systems. On one hand, public awareness is growing with every major cyber attack (cf. ibid), but many decision makers holding key positions still lack the necessary awareness of the cyber security problem: that we could become the target of a cyber attack or a threat at any time.

Anmerkung

[1] Anm.: bei paysafecard Wertkarten Vertriebs GmbH, einem führenden Prepaid-Online-Zahlungsmittel, und PayLife Bank GmbH/SIX Payment Services (Austria) GmbH, eine der größten MasterCard und Visa Akzeptanzbanken in Europa/n.b.: at paysafecard.com Wertkarten GmbH (acquired by Skrill Group in 2012, Skrill Group was acquired by Optimal Payments in August 2015), a leading prepaid online payment-method, and PayLife Bank GmbH/SIX Payment Services (Austria) GmbH, one of Europe's largest MasterCard and Visa acquiring banks

---

Quellen/Sources

Bleuth, Patrick (2015): Darknet: Ein Schwarzmarkt für Sicherheitslücken, online unter: http://www.zeit.de/digital/internet/2015-04/darknet-the-real-deal-schwarzmarkt-exploits (letzter Zugriff: 05.09.2015).

Bundeskanzleramt (2015): Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Zahlungsdienstegesetz, Fassung vom 01.08.2015, online unter: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20006355 (letzter Zugriff: 05.09.2015).

derStandard.at (2015): Cybercrime-Netzwerk zerschlagen: Tausende Straftaten, 60 Beschuldigte, online unter: http://derstandard.at/2000018007386/Cybercrime-Netzwerk-zerschlagen-Tausende-Straftaten-60-Beschuldigte (letzter Zugriff: 05.09.2015).

Europäische Kommission/European Commission (2015): Richtlinie über Zahlungsdienste (PSD)/Directive on Payment Services (PSD), online unter:

http://ec.europa.eu/finance/payments/framework/index_de.htm (letzter Zugriff: 05.09.2015).

Europäische Kommission (2013)/European Commission (2013): Europäisches Zentrum zur Bekämpfung der Cyberkriminalität: Eröffnung am 11. January/European Cybercrime Centre (EC3) opens on 11 January, online unter: http://europa.eu/rapid/press-release_IP-13-13_de.htm (last viewed: 02.08.2015).

Krebs, Brian (2014): The Target breach, by the numbers, online unter: http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/ (letzter Zugriff: 05.09.2015).

Petersen, Christopher (2015a): Die Risiken von Cyber-Bedrohungen – ein Leitfaden für CEOs und Vorstände, online unter: http://files.vogel.de/vogelonline/vogelonline/companyfiles/9090.pdf (letzter Zugriff: 05.09.2015).

Petersen, Christopher (2015b): Mit Security Intelligente kritische Cyber-Bedrohungen aufdecken, online unter: http://files.vogel.de/vogelonline/vogelonline/companyfiles/9091.pdf (letzter Zugriff: 05.09.2015).

PwC (2015): The Global State of Information Security Survey 2015, online unter: http://www.pwc.com/gsiss2015 (letzter Zugriff: 05.09.2015).

Singer, P.W./Friedmann, Allan (2014): Cybersecurity and Cyberwar. USA: Oxford University Press, 57.

Stingeder, Karl H. (2015): Rezension: World Wide War: Angriff aus dem Internet/Cyber War: The Next Threat to National Security and What to Do About It, online unter: http://www.medienimpulse.at/articles/view/759/webpapers (letzter Zugriff: 05.09.2015).