)SCIP(

01/2016

MONTHLY SECURITY SUMMARY

Schwarzmarkt Darknet

Um den anonymen Teil des internet ranken sich viele Mythen. Wir haben das hinterfragt und das Darknet erforscht > 2

Moderne Überlebenskunst

OPSEC stammt aus dem Militär, ist aber im Informationszeitalter zu einem wichtigen Aspekt des Lebens geworden. > 6

Neues scip-Buch

Die Mitarbeiter der scip AG haben ihr jüngstes Buch veröffentlicht. Es ist ab sofort erhältlich. > 9

NEWS

Einschätzung des Linux Backspace-Bugs in watson

In vielen Linux-Distributionen ist es möglich, sämtliche Authentisierung mit dem Drücken der Backspace-Taste zu umgehen. Darüber berichtet der Journalist Daniel Schurter für die Schweizer Online-Zeitung watson. Im Artikel mit dem Titel «Merkwürdiger Linux-Bug: Während sechs Jahren konnte man Rechner mit der «Zurück»-Taste knacken» kommt Marc Ruef zu Wort, der die Pros und Kontras von Open-Source-Software einschätzt und nennt den Preis der Vulnerability auf dem Schwarzmarkt.

Ratschläge gegen den Microsoft-Scam

Im Kanton Obwalden gehen Betrüger auf Opfersuche. Am Telefon geben sich die Täter als Mitarbeitende Microsofts aus und erbeuten so Kreditkarten- und Bankdaten oder lassen ihre Opfer Schadsoftware auf dem heimischen PC installieren. Journalist Philipp Zurfluh geht dem im Artikel Falsche IT-Spezialisten zocken Leichtgläubige ab der Gratiszeitung 20 Minuten nach. Im Artikel kommt Stefan Friedli zu Wort, der die Auswirkungen eines solchen Angriffs erklärt und Einblick in die Update-Policy Microsofts gibt.

Darknet-Analyse im Online-Magazin Leodan

Das Online-Magazin der Privatbank Leodan hat einen Artikel über das Darknet veröffentlicht. In «Dunkel. Dunkler. Darknet», verfasst von Journalist Mark Baer, kommt Marc Ruef zu Wort, der in den vergangenen Monaten umfangreiche Forschungen im anonymen Netz betrieben hat. Die kompletten Forschungsergebnisse sind in seinem Labs-Artikel auf Seite 2 nachzulesen.

Interview zu WLAN-Passwörter in watson

Der Internetprovider UPC-Cablecom liefert WiFi-Router mit einem ableitbaren Initialpasswort aus. Marc Ruef äussert in einem Interview auf watson zur Problematik. Anhand der SSID (Name des WLAN) und des genutzten Frequenzbands können mögliche Passwortkombinationen abgeleitet werden. Dadurch kann ein Angreifer den Datenverkehr mitlesen, manipulieren oder stören. Wir empfehlen einen sofortigen Wechsel des Passworts.

Labs 7

EDITORIAL

Wen interessiert's?

Nutzer interessiert die Sicherheit nicht. Die Experten kämpfen auf verlorenem Posten. Ein Blick auf die Sicherheit, wie sie sein muss.

Dominik Bärlocher

Das Geschäft der Informationssicherheit boomt. Die Informationsgesellschaft ist Realität. Der Schutz der eigenen Informationen ist vom belustigenden Zeitvertrieb von Paranoiden zur alltäglichen Überlebensstrategie geworden, könnte man annehmen. Wo Unternehmen Tausende von Franken in benötigte Sicherheit und deren Tests investieren, sind die Endnutzer oft von einer fast schon an Dummheit grenzender Naivität beseelt.

Apps für Smartphones und Tablets werden heruntergeladen, ohne, dass die *Permissions* angesehen geschweige denn hinterfragt werden, die Telefonnummer wird auf Twitter veröffentlicht und die Facebook Privatsphäreneinstellungen bleiben in der Regel unangetastet. Clever und aufgeklärt geht anders. Es liegt aber nicht daran, dass die bösen App-Programmierer, die Fiesen von Facebook oder sonstwer sich keine Mühe geben, die Nutzer aufzuklären. Facebook selbst hat einen ausführlichen Artikel zum Thema Privatsphäre veröffentlicht. Andere Sites machen sich auch die Mühe und versuchen sich auch an Erklärungen.

Damit nicht genug. Etliche Artikel und Beiträge in sämtlichen Medien warnen davor, unbekannte Anwendungen zu installieren oder sonstigen Unsinn mit den eigenen Geräten anzustellen. Und dennoch: Tech Supporter erzählen haarsträubende Geschichten über Dinge, auf die Nutzer hereingefallen sind, von «Ich wollte ein *Desktop Picture Recovery Tool*» bis hin zur Geschichte, dass ein Kollege die Bilder auf einem an seinen Computer angeschlossenen Laptop einsehen kann und das ein Skandal sei. Eine Frage drängt sich auf: Worin liegt der Sinn, den Nutzern Sicherheit vermitteln zu wollen, wenn die Nutzer nicht an Sicherheit interessiert sind?

Eine Frage des Vertrauens

Für Unternehmen ist klar, warum sie auf Sicherheit setzen. Nicht nur, weil Betriebsgeheimnisse ihrem Namen folgend geheim bleiben sollen sondern auch, weil die Kunden, also sprich die Nutzer, das erwarten. Der Aufschrei der Nutzer und die Anfragen in unserem Büro von Medien wie auch Privatpersonen zeigt: Die Öffentlichkeit will die absolute Sicherheit und die Freiheit, sich abgrundtief dämlich verhalten zu können, out of the box. Und das steht im krassen Gegensatz zur obigen Frage, die Tech Supporter und andere IT-Experten zum Verzweifeln bringt.

Es liegt daher nicht an der Intelligenz oder dem Sicherheitsbewusstsein, sondern am Vertrauen.

Nutzer vertrauen Unternehmen viel an. Apps wird Zugriff auf Bilder und Kontaktdaten gegeben, im Vertrauen, dass diese weder angezapft noch weitergegeben werden. Den Betreibern von App Stores wird vertraut, dass sie nur gute und sichere Apps zum Vertrieb anbieten. Dating-Sites verknüpfen in einem Account eine Identität und intimste Vorlieben, im Vertrauen, dass diese sicher hinter einem Decknamen geschützt sind. Wenn dieses Vertrauen gebrochen wird, dann ist der Skandal nicht weit.

Daraus folgt auch der Schluss, dass Nutzer nicht dumm oder naiv sind. Es ist die Wahrnehmung der Experten, die andere für dumm oder naiv befindet. Und auch das ist eine natürliche Situation.

Wissen ist nicht Weisheit

Experten wissen viel über die Technologie. Nutzer wissen, dass die Experten das wissen. Darum legen sie auch ihr Vertrauen in die Expertise, die sie schlicht nicht haben. Und die sollten sie auch nicht brauchen, weil es die Experten sind, die für die Sicherheit verantwortlich sind.

Was den Nutzern fehlt, ist nicht Wissen, sondern Weisheit, neudeutsch wohl am ehesten mit *Awareness* übersetzt. Sie sind sich aller Warnungen zum Trotz nicht bewusst, wo die Gefahren im Internet lauern, was den nun heruntergeladen werden darf und was nicht und verlassen sich auf die Experten, diese zu mitigieren, bevor sie als Nutzer damit konfrontiert sind.

Die im Titel aufgeworfene Frage von wegen *wen interessiert's* ist also beantwortet. Es interessiert alle, wie sicher sie sind. Aber nur wenige haben das Zeug dazu, wirklich für Sicherheit zu sorgen. Denn es ist der Beruf von Menschen, die in der Information Security arbeiten, Sicherheit nicht nur zu schaffen, sondern sie auch endnutzergerecht zu vermarkten, auch wenn die Experten das nicht wollen und sich gerne mal etwas besser als das niedere Fussvolk fühlt. Jede und jeder will Sicherheit, aber nur wenige können sie herstellen und vermitteln.

BLOG DIGEST

Die besten Links des Monats Dezember

- 10 Reasons to Migrate from On-Premised Office to Office 365 (resources.infosecinstitute.com)
- Agreement on first EU wide cyber-security directive (enisa.europa.eu)
- Beware of state-sponsored hackers, Twitter warns dozens of users (arstechnica.com)
- Elite scientists really do hold back science (vox.com)
- FAA Announces Small UAS Registration Rule (faa.gov)
- Formula E announces the world's first driverless car racing series (theverge.com)
- Google, D-Wave, and the case of the factor-10^8 speedup for WHAT? (scottaaronson.com)
- Hacker Buba holds UAE bank to ransom (scmagazine.com)
- Internet Explorer End of Support (microsoft.com)
- Internet's root servers take hit in DDoS attack (theregister.co.uk)
- Kazakhstan will force its citizens to install internet backdoors (zdnet.com)
- Revealed: FBI can demand web history, phone location data without a warrant (zdnet.com)
- Stunning 'Reality Editor' Lets You Connect Everything (core77.com)
- TheRealDeal: This Long-Dead Market Was Just Relaunched! (deepdotweb.com)
- When children are breached - inside the massive VTech hack (troyhunt.com)
- When Your CEO Won't Take Security Awareness Training (resources.infosecinstitute.com)
- Why Application Security Testing Is a Growing Market (veracode.com)
- Yes, Google can remotely reset Android passcodes, but there's a catch (zdnet.com)

Impressum

Redaktion:
scip AG, Badenerstrasse 623, 8048 Zürich
Telefon: +41 44 404 13 13
Fax: +41 44 404 13 14
E-Mail: info@scip.ch

Redaktor: Dominik Bärlocher
Autoren: Andrea Covello, Stefan Friedli, Rocco Gagliardi, Flavio Gerbino, Veit Hailperin, Marc Ruef, Michael Schneider, Simon Zumstein

Das scip Monthly Security Summary erscheint monatlich.

Anmeldung: smss-subscribe@scip.ch
Abmeldung: smss-unsubscribe@scip.ch

LABS

Schwarzmarkt Darknet

Um das Darknet ranken sich unzählige Mythen und Legenden. Recherche zeigt, wie Drogendealer, Killer und Waffenschieber im Netz agieren.

Marc Ruef

Das *Darknet* ist ein *verborgener Bereich* des Internets. Er ist nur mit zusätzlicher Software und Vertrauensbeziehungen zugänglich. Im Rahmen einer aufwändigen Forschungsarbeit sind verschiedene Bereiche des Darknets untersucht worden. Ein Teil der Resultate wird in diesem Beitrag diskutiert.

So sieht das Darknet wirklich aus

Was ist das Darknet

Beim Begriff *Darknet* taucht ein Problem auf, das man im IT-Bereich öfter antrifft: Es ist ein Schlagwort, das oft genutzt aber wenig verstanden wird. Die Begründung dafür ist vielschichtig. Grundsätzlich haben bisher nur wenige Personen den Weg ins Darknet gefunden und sind bereit, über ihre Erfahrungen zu berichten. Journalisten schreiben lieber voneinander ab, ohne Aussagen zu verifizieren. Dadurch hat sich über die Jahre eine Masse an Fehlinformationen angesammelt, die zu entwirren sehr aufwendig ist.

Dazu beigetragen hat ebenfalls eine Infografik, die eigentlich Satire ist, aber durch Aussenstehende nicht so verstanden wird. Spätestens wenn berichtet wird, dass man in den tiefsten Bereichen des Darknets nur mit Quantencomputer agieren kann, weiss man, dass einmal mehr ein Journalist über etwas schreibt, das er nicht versteht. Artikel, die auf diesen Fehlinformationen fussen, werden monatlich veröffentlicht. Nachfolgende Illustration korrigiert dieses Bild.

Im Rahmen unserer Analyse teilen wir das Internet in Bereiche auf. Allgemein bezeichnen wir Bereiche als *Net* (also Darknet), wenn Dienste jeglicher Art gemeint sind. In vielen Publikationen wird der Suffix *Web* gebraucht (z.B. Darkweb), wobei damit ausschliesslich Darknet-Ressourcen gemeint sind, die durch einen Webserver angeboten und von einem Webbrowser genutzt werden. Das *Freenet* oder *Visible Net* (Visinet) ist das Internet, wie wir es kennen. In erster Linie frei zugängliche Webseiten, die durch Suchmaschinen indexiert werden.

Sobald Suchmaschinen keinen direkten Zugriff mehr auf Informationen erhalten, sprechen wir vom *Deepnet* oder *Invisible Net*. Dies ist zum Beispiel dann gegeben, wenn im *Deepweb* eine Webseite eine Authentisierung erfordert, sie auf einem unüblichen Port betrieben wird oder nur einer kleinen Gruppe bekannt ist. Oder wenn alternative Netzwerkprotokolle und Topologien eingesetzt werden, die eine Indexierung erschweren. Letzteres ist bei Peer-to-Peer-Netzen (P2P) der Fall, die den Download einer speziellen Software erfordern. Hier spricht man also zwangsweise nicht mehr vom *Deepweb*, da nicht mehr die im Web üblichen Mechanismen herangezogen werden.

Geht man noch einen Schritt weiter, dringen wir ins *Darknet* vor. Hier werden unter anderem spezielle P2P-Netze betrieben. Bei den Friend-to-Friend-Netzen (F2F) werden Daten nur noch dezentral unter ausgewählten Freunden ausgetauscht. Man muss sich also zuerst einen Bekanntenkreis aufbauen, bis man dort Daten tauschen kann. Des Weiteren gibt es auch private Foren, die man nur nach Einladung und Freigabe betreten kann. Solange man niemanden kennt, der für einen bürgt, wird der Zugriff verunmöglicht.

Schlussendlich gibt es noch temporäre Chat-Server, die kurzfristig aufgebaut und nach einer Transaktion wieder abgeschaltet werden. Diese werden für hochgradig illegale Aktivitäten, oftmals die Orchestrierung oder Abwicklung einer Transaktion, eingesetzt. Als Technologien kommen üblicherweise IRC und Jabber/XMPP zum Tragen. Die Kommunikation wird vollständig verschlüsselt und auf das Anlegen von Logs wird verzichtet.

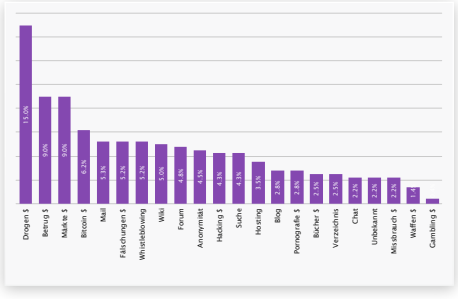
Die Komplexität und der Aufwand für das Bewegen in den tieferen Ebenen des Darknets steigen an. Dabei wird Komfort zu Gunsten der Sicherheit aufgegeben. Darum sind diese Bereiche für normale Aktivitäten unattraktiv und werden bevorzugt von dubiosen Akteuren herangezogen.

Struktur des Darknet

Ein Grossteil der Darknet-Aktivitäten spielen sich auf Webseiten ab, die nur über TOR erreichbar sind. Diese Darkweb-Seiten werden als *Hidden Services* bezeichnet, da sie den Suchmaschinen theoretisch verborgen bleiben. Es gibt jedoch ein paar Index-Suchmaschinen im Darknet. Effizienz, Qualität und Abdeckung der Suche ist aber nicht vergleichbar mit dem, was man von Google und seinen Konkurrenten gewohnt ist.

Es gibt verschiedene Auswertungen von Hidden Services. Die erste umfangreiche Auswertung wurde durch den Sicherheitsspezialisten Gareth Owen durchgeführt. Genaue zahlen nannte er aber in seinem Vortrag Tor: Hidden Services and Deanonymisation nicht. Dennoch wurde diese vage Datenlage als Grundlage für die Auswertung der viel zitierten Liste auf Wikipedia verwendet. Das Problem hierbei ist, dass die Summe der Prozentangaben die 100 Prozent übersteigt und damit die gesamte Liste unbrauchbar ist.

Deshalb haben wir eine erweiterte Auswertung der Hidden Services vorgenommen und sind zum unten gezeigten Resultat gekommen. Die Kategorisierung zeigte zugleich auf, dass fast die Hälfte der Hidden Services einen kommerziellen Hintergrund haben. Es werden also Daten, Informationen oder Produkte gegen Geld gehandelt, um Profit zu machen. Damit steht fest: Das Darknet wird hauptsächlich aus Profitgründen genutzt.



Aufteilung Hidden Services im Darknet

Marktanalysen

Unter Berücksichtigung der Gesetzeslage nehmen wir an ausgewählten Aktivitäten im Darknet teil, um die Struktur der Märkte und das Verhalten der Marktteilnehmer verstehen zu können.

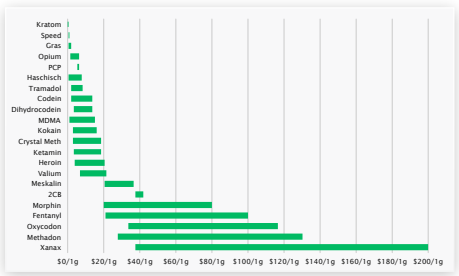
Im Folgenden werden die Hauptmärkte vorgestellt und die Erkenntnisse der Betrachtungen zusammengefasst. Dabei wird sich sowohl auf allgemeine Märkte (ähnlich eBay) als auch auf dedizierte Fachseiten konzentriert. Um Quellenschutz und die Identität unserer Analysten zu schützen, werden keine personenidentifizierenden Daten festgehalten.

Drogenhandel

Ein Grossteil der im Darknet gehandelten Waren sind Drogen und Medikamente. Der Global Drug Survey 2015 konnte durch systematische Befragung von Drogen-Händlern und -Konsumenten im Darknet viele spannende Erkenntnisse gewinnen. So ist der Hauptgrund, warum auf den Handel im Darknet ausgewichen wird, die Erhöhung der persönlichen Sicherheit. Das Umfeld um Ross Ulbricht alias Dread Pirate Roberts, der mit Silk Road einen der grössten Drogenumschlagsplätze im Darknet betrieben hat, führt an, dass damit ein Gewinn für alle Parteien erreicht werden kann. Dass die eigene Identität verborgen bleibt und der Drogenmissbrauch vor dem Umfeld versteckt werden kann, sind weitere Faktoren.

Grundsätzlich werden praktisch alle Drogen im Darknet gehandelt. Besonders populär sind dabei natürlich Cannabis (Weed und Haschisch), MDMA, Kokain, und Heroin.

Die Preisspanne der verschiedenen Drogen ist sehr unterschiedlich. So kosten ein Gramm Kratom zwischen 0.06 USD und 0.12 USD. Beim Opium ist eine bedeutend höhere Spannbreite von 1.30 USD bis 6.00 USD zu beobachten. Die grössten Abweichungen konnten wir bei Xanax beobachten, das zwischen 35.50 USD und 330.00 gehandelt wird. Preise für LSD fangen bei 3265.00 USD an.



Aktuelle Drogenpreise im Darknet

Diese enormen Abweichungen haben mehrere Gründe. Als Faustregel kann festgestellt werden, dass die meisten derzeit aktiven Händler Mengenrabatt gewähren. Will man nur ein *Sample*, also eine Probe, bestellen, sind die Kosten meist überproportional hoch. Kauft man Kokain im Kilogramm-Bereich, kann man weitaus günstiger ins Geschäft kommen.

Eine systematische Analyse zeigt, dass sich gewisse Händler bei der Definition des Mengenrabatts verrechnen. Ab und an kommt es vor, dass man beim Kauf von zwei Kilogramm Opium weniger pro Gramm bezahlt, als bei fünf Kilogramm. Automatisierte Auswertungen von Transaktionen lassen vermuten, dass Fehler dieser Art durch andere Händler nicht systematisch wahrgenommen und ausgenutzt werden (günstiger Ankauf, teurer Weiterverkauf).

Datentyp	Details	Preis in USD
E-Mail-Kontoinformationen	1000 Stück, zufällig, nicht verifiziert	0.50
E-Mail-Kontoinformationen	1 Stück, pro definierbarer Domain, verifiziert	5.00
Kreditkarte	nur Nummer, keine Personendaten, nicht verifiziert	0.60
Kreditkarte	nur Nummer, keine Personendaten, verifiziert	7.50
Kreditkarte	Plastik, inkl. PIN, verifiziert, garantierte Deckung	80.00
Pass	Frankreich, nur Scan	7.00
Pass	Schweiz, nur Scan	38.00
Pass	USA, vollumfängliche Fälschung	160.00
Ausweis	Generierung anhand von Templates	34.00
Ausweis	Australien, Führerschein, Scan	20.00
Ausweis	UK, Führerschein, modifizierte Kopie	10.00
Ausweis	Kanada, Ausweisdokumente, Scan	5.00
Ausweis	USA, Social Security Card, Scan	20.00

Preise im Darknet

Des Weiteren ist natürlich die Qualität des Produkts entscheidend. Möglichst reines Crystal Meth ist auf dem Markt mehr wert, als unsauberes. Manche Händler preisen ihre Produkte mit Reinheitsangaben an. Typischerweise sind diese geschönt, um hohe Verkaufspreise rechtfertigen zu können. Gerade dieser Faktor macht es sehr schwierig, vermeintlich gleiche Produkte miteinander zu vergleichen. Die meisten professionalisierten Märkte bieten Bewertungs- und Kommentarfunktionen für Käufer, anhand derer die Qualität abgeschätzt werden kann.

Schlussendlich sind die Versandgegebenheiten mitentscheidend für den Preis eines Produkts. Je nach Herkunft und Destination einer Bestellung können unterschiedliche Risiken anfallen, die ihrerseits einen direkten Einfluss auf den Preis eines Produkts haben werden. Ein Effekt, der auch beim Waffenhandel zu beobachten ist.

Auftragsmorde

Ein ganz spezieller Markt sind *Auftragsmorde*. Traditionell können *Assassins*, *Killer* oder *Guns for Hire* beauftragt werden, eine oder mehrere Personen gegen ein Entgelt umzubringen. Die Bezahlung erfolgt dabei meist entweder ganz im Vorfeld oder als Teilzahlung vor und nach Abschluss des Auftrags.

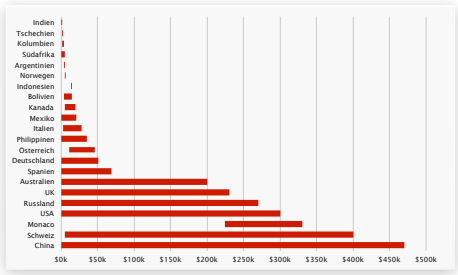
Eine spezielle Form von Auftragsmorden wird durch ein Bidding-Verfahren angeboten. Dabei können Nutzer nach ihrem Belieben eine Zielperson auf eine Liste setzen lassen. Personen haben dann die Möglichkeit, Bitcoins auf diesen Mordauftrag einzuzahlen. Derjenige Killer, der die Person umbringt, erhält das angehäufte Geld. Auf dieser Liste finden sich hauptsächlich bekannte Personen wie Barack Obama.

In den Assassin-Netzwerken bieten die Auftragsmörder ihre Dienste in einem Profil an. Dort werden typischerweise die folgenden Modalitäten festgehalten:

- Region/Land für Auftrag
- Minimales Alter von Zielpersonen
- Herangehensweise
- Preis

Unsere Recherche lässt vermuten, dass viele der angebotenen Dienstleistungen nicht echt sind. Die Profile und Preisstrukturen widersprechen teilweise dem, wie in solchen Kreisen operiert wird. Hier geht es wohl oftmals um Provokation und Trolling. Wir haben mehrere Quellen verglichen, um unter anderem die Preisspanne für Auftragsmorde pro Land zu ermitteln. Hierbei haben wir in einem ersten Schritt ausschliesslich verifizierte Preise berücksichtigt. Ein Preis gilt als verifiziert, wenn nachweislich ein Geldtransfer stattgefunden hat oder Auftraggeber oder Mörder nach einer Festnahme die Preisstruktur kommuniziert haben. Zudem wurden lediglich *professionelle* Mörder berücksichtigt. Gelegenheitstäter, die aus einer Situation heraus und einmalig agiert haben, wurden ausgelassen.

David Wilson, Professor an der Birmingham City University, hat die Morde in den Jahren 1974 bis 2014 in Grossbritannien analysiert, um statistische Merkmale zu identifizieren. Dabei konnte er ebenfalls Preisstrukturen und Auftragsverhältnisse von Auftragsmorden bestimmen. Die von uns zusammengetragenen Daten wurden dementsprechend mit den Angeboten im Darknet verglichen, um Authentizität und Preisbereiche erkennen zu können.



Preise für Auftragsmorde

Wie nicht anders zu erwarten war, fangen Eintrittspreise bei Entwicklungs- und Schwellenländern deutlich tiefer an als in Industriestaaten. Ebenso werden in letztgenannten viel höhere Maximalpreise bezahlt. Dies hat zwei Gründe:

1. Das Lohnniveau der Täter
2. Der kommerzielle Wert (Net Worth) des Opfers

Diese und ähnliche Informationen werden von uns benutzt, um Risikoprofile für hochkarätige Mitarbeiter unserer Kunden zu erstellen. Dadurch kann von bestimmten Aktivitäten oder Reisen abgeraten oder bei Bedarf das Sicherheitsdispositiv vor Ort erhöht werden.

Waffenhandel

Der Waffenhandel im Internet, allem voran im Darknet, befindet sich im

Wachstum. Es gibt verschiedene Quellen, aus denen diese Waffen stammen. Oftmals sind es private Sammler und Händler, die Waffen und Munition verkaufen oder tauschen wollen. Die Szene in Deutschland und Österreich zeigt sich da auffällig motiviert.

In diesen Kreisen finden sich in erster Linie alte und modifizierte Schusswaffen. Oftmals sind es Enthusiasten, die einfach nur Freude an den Geräten haben. Eine Kontaktaufnahme mit Händlern zeigt, dass sie leichtfertig mit dem Thema umgehen. Eine Waffe wird als Sportgerät oder Werkzeug angesehen. Dass damit Menschen getötet werden können, wird entweder ausgeblendet oder die Verantwortung hierfür vollumfänglich auf den Käufer übertragen.

Die Terroranschläge vom 13. November 2015 in Paris haben dennoch zu unmittelbaren Effekten im Darknet geführt. Die beiden populären Märkte *Agora* und *Nukleus* haben im Zuge dessen den ungehinderten Verkauf von Waffen eingestellt. Es erstaunt, dass auf diesen Plattformen doch ein gewisser moralischer Kompass vorhanden ist.

Grosse Kaliber und Sprengstoff, die zum Kauf oder Tausch angeboten werden stammen vorwiegend aus Krisengebieten und Bürgerkriegen. Hier können sowohl sehr alte Waffen aber auch neue Versionen - und dies jeweils in grossen Mengen - bezogen werden.

Viele Händler liefern bevorzugt innerhalb des Ziellands. Im europäischen Raum werden in den Inseraten oftmals Hinweise untergebracht, dass nicht ausserhalb dieses Gebiets geliefert wird. Dadurch möchte man die kostspielige und gefährliche Zollabfertigung verhindern. Ein Verhalten, das auch im Drogenmarkt - wenn nicht so extrem - beobachtet werden kann.

Datenhandel

Im Informationszeitalter spielt der Datenhandel eine zunehmend wichtige Rolle. Es gibt eine Vielzahl an Informationen, die gehandelt werden. Für Unternehmen und Behörden führen wir tagesaktuelle Preislisten, um Bewegungen im Markt erkennen zu können. Zum Beispiel, wenn sich Preise für Kreditkarteninformationen im grossen Stil ändern, wird voraussichtlich irgendwo ein grösseres Datenleck ausgenutzt worden sein. Dadurch kann quasi eine seismographische Beobachtung des Markts stattfinden. Die auf Seite 3 abgedruckte Tabelle zeigt einige Richtwerte für Daten.

Kreditkarten werden seit eh und je im Untergrund gehandelt. Dies hat in den letzten Jahren nur marginal zugenommen. Auffällig dabei ist jedoch, dass beim Kreditkartenhandel eine Professionalisierung stattgefunden hat: Die Anbieter bereiten die Daten besser auf. Marktführer in Bezug auf Einfachheit, Komfort und Angebot ist zur Zeit der *CC Autoshop* von *AlphaBay*: Hier kann mit Filtern nach spezifischen Karten gesucht werden (Ablaufdatum, Herkunft, Geburtsdatum).

Ausgewählte Preisbeispiele für Exploits

Gesundheitsdaten rücken immer mehr in den Fokus. Social Security Numbers (SSN) sind in den USA ein wichtiges Element, um sich auszuweisen und Leistungen zu beziehen. Grundlegende Informationen zu einer Person sowie die dazugehörige SSN machen es sehr einfach, eine Identität zu stehlen. Dementsprechend erfreut sich der Handel mit SSN grosser Beliebtheit. Diese werden manchmal mit zusätzlichen Dokumenten (Ausweisen, Krankenakten) als Pakete angeboten.

Im europäischen Raum ist etwas Vergleichbares nicht vorzufinden. Zwar werden auch hier Ausweisdokumente getauscht und verkauft. Oftmals sind es aber nur Kopien von Dokumenten. Oder es werden Templates angeboten, mit denen sich ein gefälschter Ausweis selber zusammenklicken lässt. Ausdrucken muss man ihn dann aber noch immer selber. Ein Grenzübertritt wird mit diesen nicht ohne weiteres möglich sein. Viele Online-Dienste, gerade im Finanzumfeld, setzen aber mittlerweile das Einschicken des Fotos eines Ausweisdokuments voraus. Mit entsprechenden Kopien können solche Dienste unter falschem Namen genutzt werden. Geldwäsche in kleinerem Stil wird damit unter anderem möglich.

Auffällig ist, dass immer mehr und konkreter Daten von Unternehmen angeboten werden. Dazu gehören Kundeninformationen, interne Dokumente und Patente. Diese werden zwar sehr selten auf den grossen Märkten feilgeboten. Im kleineren Kreis werden diese jedoch ausgetauscht. Ebenso hört man immer wieder davon, dass sich dadurch ebenfalls Zugänge zu kompromittierten Systemen kaufen lassen. Mittlerweile sind es nicht nur externe Angreifer, die ihre Erfolge so zu Geld machen - Stattdessen werden die Zugangsdaten auch von Administratoren der betroffenen Systeme in den Markt gebracht. Für Angreifer, die in eine Firma eindringen wollen, ist dies ein gut geeigneter Startpunkt. Und oftmals bedeutend günstiger, als sich mit eigenen Kräften einen Zugang zu verschaffen. Professionelle Hacker und qualitativ hochwertige Exploits können da bedeutend teurer sein.

Exploit-Handel

Ein Exploit ist eine Software, die das Ausnutzen einer Schwachstelle teilweise oder ganz automatisiert. Exploits werden beispielsweise von uns angewendet, um die Existenz und Tragweite einer Schwachstelle im Rahmen einer Sicherheitsüberprüfung bestimmen zu können. Der Kunde erhält dadurch ein konkretes Bild davon, wie und was von dieser Ausnutzung erwartet werden kann.

Das Entwickeln von Exploits ist mit sehr viel Aufwand verbunden. Einerseits ist ein hohes Mass an Verständnis für die zugrundeliegende Schwachstelle erforderlich. Dies macht es unmöglich, einen Exploit von einem Entwickler, der sich nicht in erster Linie im Bereich der IT-Sicherheit bewegt, schreiben zu lassen. Zudem müssen Eigenheiten des Zielobjekts sowie Gegenmassnahmen, die das Ausnutzen der Schwachstelle behindern oder verhindern können, berücksichtigt werden. Dies sind in erster Linie Eingabeüberprüfungen und Encodierungen in der Ziel-Anwendung. Es kann sich aber auch um zusätzliche Sicherheitsmechanismen, wie Antiviren-Software und Firewalling handeln.

Aus diesem Grund hat sich ein aktiver und lukrativer Exploit-Markt entwickelt. Darin bewegen sich Akteure mit unterschiedlichen Hintergründen aber ähnlichen Zielen:

- **Security Researcher**: Privatpersonen oder Unternehmen, die im Bereich der IT-Security arbeiten und sich mit Schwachstellen auseinandersetzen. Hierzu zählen auch Unternehmen wie wir, die Sicherheitsüberprüfungen durchführen.
- **Exploit Developer**: Programmierer, die auf das Schreiben von Exploits spezialisiert sind. Diese entwickeln Exploits meist als Auftrag für eine andere Partei.
- **Vulnerability Broker**: Unternehmen, die sich auf den Handel mit Schwachstellen und Exploit spezialisiert haben. Diese entwickeln Exploits selbst oder kaufen diese ein, um sie dann an andere Organisationen weiterzuverkaufen.
- **Nachrichtendienste**: Traditionellerweise sind auch Geheimdienste um das Ausnutzen von Schwachstellen in Computersystemen bemüht. Mittlerweile sehr aktiv und mit einem nicht zu unterschätzenden Budget werden entsprechende Informationen eingekauft.
- **Hacker und Cracker**: Personen mit teilweise zwielichtigem Hintergrund bemühen sich um das Finden und Ausnutzen von Schwachstellen. Diese *Black und Gray Hats* sind eher selten Käufer. Sie entwickeln die Exploits selber oder tauschen sie unter Gleichgesinnten.
- **Organisierte Kriminalität**: Das Interesse der organisierten Kriminalität an illegalen Aktivitäten im virtuellen Raum hat in den letzten 20 Jahren rasant zugenommen. Die Möglichkeiten von Exploits werden langsam aber sicher für Erpressung und Diebstahldelikte entdeckt.

Exploits werden teilweise auf den üblichen Märkten im Darknet getauscht. Zudem gibt es spezialisierte Märkte, die sich aber aus nicht näher erkennbaren Gründen nicht über einen längeren Zeitraum etablieren konnten. Dazu gehört der Markt namens The Real Deal (TRD). Dieser ist nach nur wenigen Monaten Präsenz plötzlich spurlos verschwunden, bis er einige Monate später wieder aufgetaucht ist. Über die Gründe kann nur spekuliert werden. Die Fachpresse und Vertreter der Industrie werden den Machern vor, einen sogenannten Exit Scam vollzogen und mit dem Geld noch nicht vollzogener Transaktionen geflohen zu sein.

Die Vulnerability Broker oder der direkte Handel auf der Basis etablierter Vertrauensbeziehungen macht schlussendlich nach wie vor einen Grossteil dieses Marktes aus.

Der Preis eines Exploits orientiert sich an sechs grundlegenden Merkmalen:

- Popularität
- Exklusivität
- Qualität
- Zuverlässigkeit
- Durchschlagskraft
- Möglichkeiten

Aufgrund langjähriger Marktbeobachtungen konnten wir ein Modell entwickeln, um die Preise für Exploits vorauszusagen. Wir gehen dabei von einem Zeroday-Exploit aus, dessen Schwachstelle und Existenz nicht bekannt ist. Er wird exklusiv und einmalig verkauft, bis die Schwachstelle publik ist oder ein alternativer Exploit herausgegeben wird. Sobald diese Exklusivität verloren geht, wird ein tagesaktueller Preis erzeugt. Dieser ist von Ereignissen (Bekanntwerden der Schwachstelle, alternativer Exploit verfügbar, Gegenmassnahme veröffentlicht) und der zeitlichen Entwicklung abhängig. Nachfolgend werden einige Preisbereiche für bekannte Software-Komponenten dargestellt.

Die Abwicklung einer Zahlung erfolgt in der Regel gestaffelt:

1. Der Käufer erhält einen Grossteil oder einen grösstenteils funktionierenden Auszug des Exploits. Dadurch kann seine Legitimität und Qualität geprüft werden.
2. Der Käufer gibt bei Gefallen dem Verkäufer eine Anzahlung, die bevorzugt in Bitcoins geleistet wird. Falls beispielsweise ein Exploit den Gesamtpreis von 50'000 USD hat, wird die Anzahlung 20'000 USD betragen.
3. Danach erfolgen jeweils im Abstand von meist 30 Tagen eine weitere Teilzahlung von je 10'000 USD. Durch diese Staffelung können zwei unliebsame Effekte aus Sicht des Käufers flankiert werden:

1. Falls der Exploit anderswo auftaucht und damit die ausgehandelte Exklusivität verliert, kann die Zahlung eingestellt werden.
2. Falls der Hersteller die Schwachstelle frühzeitig patcht, kann die Zahlung ebenfalls ausgesetzt werden. Viele professionelle Exploit-Anbieter reichen aber in diesem Fall einen alternativen oder aktualisierten Exploit als Kompensation nach.

Der Markt für Exploits befindet sich in explosionsartigem Wachstum. Dies betrifft einerseits die Anzahl der zur Verfügung stehenden Exploits. Andererseits aber auch die Preise, die mittlerweile für Exploits hoher Qualität gezahlt werden. Es ist davon auszugehen, dass in den kommenden Jahren die Marke von 1.5 Millionen USD für einen einzelnen Exploit gesprengt werden wird. Das theoretische Marktvolumen für Zeroday-Exploits für Schwachstellen in 2015 schätzen wir auf 155 Millionen USD. Dies entspricht einem Wachstum von 67 Prozent gegenüber 2014.

Echte und unechte Inhalte

Im Darknet tummeln sich sehr dubiose und kuriose Gestalten. Im Rahmen unserer Recherchen stossen wir immer wieder auf sehr verstörende Individuen und Aktivitäten. Manche Situationen sind manchmal gar so übertrieben, dass man an deren Echtheit zu zweifeln beginnt.

Im Laufe der Zeit haben unsere Analysten ein Gespür dafür entwickelt, welche Inhalte echt sein können und welche nicht. Viele Seiten oder Inhalte werden nur veröffentlicht, um zu provozieren. Dies fällt besonders im Bereich der Auftragsmorde auf. Es gibt Seiten, deren Struktur und Inhalte fernab von echten Märkten dieser Art auftreten. Sie sind meist so gestaltet, dass sie spannend wirken und deshalb bevorzugt von Journalisten zitiert oder abgebildet werden. Wir haben es hier also mit einer ganz speziellen Form des *Trolling* zu tun.

Generell gibt es um das Darknet eine sehr grosse Legendenbildung, sogenannte *Creepypasta*. Hierbei werden fiktive oder übertriebene Geschichten verbreitet, die bei jeder neuen Iteration noch mehr zur Folklore beitragen. Zum Teil sind es unendlich brutale Erzählungen, die ein zartes Gemüt durchaus zu erschüttern in der Lage sind. Vor allem, weil sie manchmal halt doch etwas Wahres in sich tragen könnten - Oder in einigen Fällen gar irgendwann tatsächlich von der Realität eingeholt werden.

Ein typisches Beispiel für diese Art von Mythenbildung sind die sogenannten *Red. Rooms*. Hierbei handelt es sich um spezielle Chat-Rooms, in die man sich einloggen kann. Durch das Übertragen eines Live-Streams kann gesehen werden, wie eine Person misshandelt, verletzt oder gar getötet wird. Die Teilnehmer dieses Snuff-Chats können Einfluss darauf nehmen, wie sich das Vorgehen genau gestalten soll. Es gibt verschiedene Personen, die von solchen Szenerien berichten. Diese Geschichten, die an den Film Hostel erinnern, lassen sich jedoch bisher nicht bestätigen.

Viele kommerzielle Angebote haben einen betrügerischen Hintergrund. Zum Beispiel werden viele der angebotenen Uhren-Replikas nach gewährter Vorauszahlung nie ausgeliefert. Ein typischer Scam, der nicht nur im Darknet anzutreffen ist.

Die wohl populärste und ertragreichste Art des Betrugs im Darknet sind *Exit Scams*. Bei diesen wird ein Markt plötzlich geschlossen und mit ihm verschwinden die von Kunden einbezahlten und verwalteten Geldbeträge. Viele Märkte bieten einen Escrow-Service an. Sie agieren dabei als Broker und vermitteln bei Uneinigkeiten zwischen Käufer und Verkäufer. Der Käufer muss zwar eine Vorauszahlung an den Markt leisten. Dieser überweist den Geldbetrag aber erst an den Verkäufer, sobald der Käufer den Erhalt und die Qualität der Bestellung bestätigt hat. Grosse Märkte verwalten also stets eine hohe Geldsummen, die im Rahmen eines *Exit Scams* mitgenommen werden könnten. Der grosse Vorteil dieser Betrugsform ist, dass die betroffenen Personen meist gar nicht bei der Polizei vorstellig werden wollen oder können. Oft sind sie selbst in zwielichtige Geschäfte verstrickt, so dass man von einer Anzeige absieht.

Dabei ist es aber oft nicht einfach zwischen einem *Exit Scam* und einer Beschlagnahmung durch die Behörden zu unterscheiden. Der wahrnehmbare Effekt für Aussenstehende ist der Gleiche. Plötzlich tauchen Märkte dann wieder auf, manchmal gar betrieben durch die gleichen Leute. Ob es sich dann einfach um eine Fortsetzung des *Exit Scams* oder um einen Honeypot der Behörden handelt, kann nicht gesagt werden.

Wenn eine Bitcoin-Adresse veröffentlicht wird, kann durch Online-Tools wie BitRef die Balance, der auf diesen Wallets bestehende Betrag, identifiziert werden. Dadurch können Marktteilnehmer oder Märkte auf ihre Echtheit hin, wenigstens in Bezug auf den Cash Flow, überprüft werden. Viele Bereiche im Darknet lassen sich so als *Fakes* entlarven.

Strafverfolgung

Die Strafverfolgung im Darknet gestaltet sich nicht einfach. Als erstes ist da die technische Hürde: Es muss eine Infrastruktur für Überwachung und Analyse bestehen, um illegale Aktivitäten erkennen und verstehen zu können. Zudem muss ein Verständnis für die eingesetzten Mechanismen vorhanden sein. Dazu gehören unter anderem:

- Proxy-Technologien (Tor, Onion-Routing)
- Kryptowährungen (Bitcoin, Litecoin)
- Verschlüsselungssysteme (SSL/TLS, VPN)
- Chatsysteme (IRC, Jabber)

Diese Aspekte lassen sich unter Kontrolle bringen. Schwieriger wird die Strafverfolgung, da man nicht ohne weiteres mit den Zielpersonen interagieren kann. Immer dort, wo wirklich illegale Aktivitäten stattfinden, verhalten sich die Beteiligten sehr zurückhaltend und diskret. Man kommt nicht ohne weiteres mit diesen Leuten ins Gespräch.

Man muss sich zuerst eine Reputation in der Szene schaffen, um dann eine Vertrauensbeziehung zu einzelnen Leuten etablieren zu können. Dies kostet sehr viel Zeit und Aufwand. Zudem muss man sich mit den Gepflogenheiten des Milieus auskennen, die richtige Sprache sprechen. Dies fällt uns natürlich besonders im Exploit-Bereich leicht, da wir tagtäglich mit dem Thema zu tun haben und die technischen Hintergründe verstehen. In anderen Bereichen gestaltet sich das dann aber bedeutend aufwendiger.

Oftmals baut man sich dann eine Legende auf, eine fiktive Person mit einem erfundenen Leben. In nachrichtendienstlichen Kreisen empfiehlt man jeweils, in der Legende möglichst wenig Abweichungen vom eigenen Leben einzubringen. Das ständige Aufrechterhalten eines komplexen Lügengebildes ist zu anstrengend und fehleranfällig. Deshalb versucht man die Legenden möglichst simpel und authentisch zu halten. Dabei läuft man natürlich Gefahr, dass man zu viel von seiner eigenen Person preisgibt. Es ist also immer eine Gratwanderung. Und je nach dem in welchen Kreisen man sich bewegt, können Fehler verheerende Folgen haben.

Die grösste Hürde für die Strafverfolgung ist jedoch die Gesetzeslage an sich. Ermittlungen mit falschen Identitäten sind entweder gar nicht erlaubt oder bewegen sich in einer juristisch und gesellschaftlich umstrittenen Grauzone. In vielen Bereichen wird von Käufern erwartet, dass sie ihre eigene Authentizität beweisen. Beim Ankauf grosser Mengen Kreditkarten wird es dann erforderlich, dass man selbst ein paar gestohlene Kreditkarten vorzeigen kann. Die Verkäufer wissen, dass den Behörden eine Verteilung gestohlener Kreditkarten untersagt ist. Wird eine solche aber provoziert, können sie davon ausgehen, dass der Käufer legitim ist. In den Bereichen des Drogenhandels und der Kinderpornographie haben sich ähnliche Mechanismen etabliert.

Wenn dann doch Beweise gesichert werden konnten, muss man sich mit internationalen Rechtshilfebegehren auseinandersetzen. Diese sind zeitaufwendig und werden oft von den angefragten Behörden gar nicht erst richtig weiterverfolgt. Gerade in Krisenländern wird Internetkriminalität eine sehr geringe Priorität beigemessen. Ermittlungen verlaufen deshalb oft im Sand.

Fazit

Beim Darknet handelt es sich um einen dedizierten und oft speziell abgeschotteten Bereich des Internets. Dort werden Plattformen und Dienste angeboten, die zu grossen Teilen eine kuriose oder gar dubiose Beschaffenheit aufweisen.

Anhand der Beispiele der Märkte für Drogenhandel, Auftragsmorde, Waffenhandel, Datenhandel und Exploithandel wurde illustriert, welche Eigenarten in diesen Milieus anzutreffen sind.

Um sich in diesen richtig bewegen zu können, muss man sich den Gepflogenheiten bewusst sein. Nur so kann sich in einer Szene etabliert und eine Vertrauensbeziehung zu den Akteuren aufgebaut werden. Dies ist jeweils mit sehr viel Zeit und Aufwand verbunden.

Dieser Effekt und die Tatsache, dass ein technologisches Verständnis vorhanden sein und die Möglichkeiten der Gesetzeslage ausgereizt werden muss, macht die Strafverfolgung im Darknet sehr schwierig. Deshalb ist es nicht von der Hand zu weisen, dass auch in Zukunft ein Grossteil der illegalen Aktivitäten im Internet in diesen Bereich verlagert wird. Behörden müssen zwangsweise aufrüsten, um dieser wachsenden Schattenwirtschaft entgegnen zu können.

LABS

OPSEC - Geschichte und Grundlagen

Vom Geheimnis zur militärischen Strategie zur digitalen Überlebenstaktik - Operations Security wird immer zentraler. Die Strategie, wie Informationen geschützt werden, will gut geplant sein.

Dominik Bärlocher

Sogar Eichhörnchen haben Geheimnisse, die sie schützen.

Geheimnisse. Jeder hat sie. Betriebe erzählen keinem, wer ihre Kunden sind. Armeen sagen keinem, wohin sie ihre Truppen verschieben. Menschen wollen nicht, dass jeder weiss, was sie zu bestimmten Zeiten getan haben. Geheimnisse sind in unserer Gesellschaft in jeder Schicht vorhanden. Sogar Tiere haben Geheimnisse. Eichhörnchen, zum Beispiel, verstecken Nüsse so, dass andere Eichhörnchen sie nicht finden können und andere Tiere stellen sicher, dass ihre Nester vor Jägern versteckt sind.

Geheimnisse zu haben, ist einfach. Diese geheim zu halten stellt sich mit dem Fortschritt der Technologie als immer schwieriger heraus. Damit Geheimnisse geheim bleiben, müssen die Aktionen, oder Operationen, rund um das Geheimnis abgesichert sein. Das ist ein Prozess, der Operations Security - kurz OPSEC - genannt wird. Der Begriff wurde vom Militär im frühen 20. Jahrhundert geprägt, doch das Konzept dahinter ist so alt wie es Geheimnisse sind.

Von der Antike bis heute

Geheimnisse bringen immer Macht mit sich. Wenn eine Armee weiss, wohin ihr Feind seine Truppen verschiebt, dann kann sie einen Hinterhalt vorbereiten und sich so einen Vorteil verschaffen. Wenn ein Erpresser ein Geheimnis einer Person kennt, dann kann er Geld oder andere Dienste verlangen, damit er im Gegenzug das Geheimnis geheim hält.

Zum ersten Mal werden Geheimnisse als Konzept wohl bei den alten Griechen erwähnt. Die Griechen assoziieren Geheimnisse mit der Rose. Denn der Legende nach gab die Göttin Aphrodite ihrem Sohn Eros einer Rose, der sie an Harpokrates - dem Gott des Schweigens - weitergab, damit dieser sicherstellt, dass Aphrodites Indiskretionen geheim blieben. Einige Versionen der Legende sprechen auch von den Indiskretionen aller Götter, die Harpokrates geheim halten sollte. So wurde die Rose zum Symbol des Geheimnisses.

Das Christentum kennt Gespräche *sub rosa*, also unter der Rose, was heisst, dass geheime Informationen ausgetauscht werden und dass alle im Gespräch Involvierten zu einem engen Kreis der Vertrauten gehören. Beichten sind auch *sub rosa*, weshalb manch ein Beichtstuhl mit Rosen- oder Blumenbildnissen verziert ist.

Unter den ersten Menschen der jüngeren Zeit, die sich dem abstrakten Konstrukt eines Geheimnisses annahmen, war der deutsche Soziologe, Philosoph und Kritiker Georg Simmel. In seinen Propositionen beschreibt er den Aufbau eines Geheimnisses und was es mit den Vertrauten anstellt. Er schliesst, dass, je mehr Geheimnisse organisiert und geteilt werden, eine zentrale Befehlsstruktur sich etablieren kann oder etabliert wird.

Weil der Bedarf einer Kontrollinstanz gegeben ist, sind Geheimnisse und ihre Wahrung für die Militärs aus aller Welt von enormer Wichtigkeit und grossem Vorteil. Dies wird in der Regel mit dem *Need-to-Know-Prinzip*, der Denkweise, dass nur die über Wissen verfügen, die es wirklich brauchen. Es ist selten, dass alle Mitglieder einer Einheit alle Informationen zu einer Mission haben. Sie vertrauen ihren Oberen, die mehr Informationen haben, dass sie das Privileg des Geheimnisses nicht missbrauchen.

Hier kommt die strategische Operations Security, das was im frühen 21. Jahrhundert als OPSEC bekannt ist, ins Spiel.

Schäm dich, Schwätzer

OPSEC, obwohl zweifelsohne schon früher betrieben, wurde im zweiten Weltkrieg zum Element des öffentlichen Bewusstseins. Es gibt aus dieser Zeit eine Unzahl Poster, Pamphlete und Geschichten, die alle zum Ziel haben, dass Menschen still sind weil sie nicht sicher sein konnten, ob der Feind zuhört. Das wohl berühmteste Poster trägt den Titel *Loose Lips Sink Ships* - lockere Lippen versenken Schiffe - und soll Menschen daran erinnern, dass sie unter Umständen in der Lage hätten sein können, dem Feind Flottenpositionen und -bewegungen mitteilen zu können. Das Poster stammt von den Amerikanern.

Aber sie sind nicht die einzigen, die OPSEC-Poster veröffentlicht haben.

Das Ausspionieren des Feindes und von Menschen im Alltag erreichte während des kalten Krieges seinen Höhepunkt, aber der Bedarf an OPSEC ging verloren. Das Zeitalter des Internets begann in den frühen 1990er-Jahren nur kurz nach dem Ende des kalten Krieges. Spätestens dann wurde OPSEC von etwas, das die Interessen eines Staates schützen sollte, zu einer wichtigen Überlebensfähigkeit im Alltag.

Schäm dich, Twitterer

Im frühen 21. Jahrhundert ist die Gesellschaft an einem Punkt, an dem Geheimnisse zum Fall von Unternehmen oder zu öffentlicher Blamage einer Person führen können. Selbst wenn die Folgen eines OPSEC-Fehlers nicht katastrophal sind, können sie doch sehr lästig sein und zu Imageverlust oder Belästigung führen.

Ein junges Beispiel hierfür sind die *Snowden Cat Facts*. Ein anonymer Hacker hat einen Bot programmiert, der öffentliche Twitter-Nachrichten nach Telefonnummern durchsucht. Wenn er eine Telefonnummer findet, dann schickt er ihr unnütze Fakten über Katzen per SMS. Es gibt nur einen Weg, die Katzenfakten wieder abzustellen: Ein Tweet an NSA-Whistleblower Edward Snowden mit folgendem Inhalt:

@Snowden Meow, I <3 catfacts

Edward Snowden selbst hat anscheinend nichts mit den Katzenfakten per SMS zu tun. Fakten wie *Etwa 40000 Menschen in den USA werden pro Jahr von Katzen gebissen* sind zwischen amüsant und nervtötend anzusiedeln, zeigen aber auf, dass viele moderne Menschen an OPSEC scheitern, da sie ihre Telefonnummer für jeden zugänglich öffentlich gemacht haben.

Bevor das soziale Netzwerk Facebook die Nennung des echten, vollen Namens akzeptabel und zum Standard gemacht hat, war die Angabe des eigenen Namens eine Verletzung von OPSEC. War es einst höchst unge-

wöhnlich, dass jemand im Chat oder in einem Forum seinen echten Namen und sein echtes Foto verwendet hat - Nicknames und Avatare waren in den frühen Tagen des Netzes ein grosses Thema -, so ist es heute gang und gäbe, auch übelste Inhalte wie rassistische Äusserungen oder sexistische Kommentare mit Klarnamen und echtem Foto zu posten. Menschen haben keine Bedenken mehr, sich unter ihrem echten Namen und mit Bild im Internet zu zeigen. Diese entspannte Haltung gegenüber Privatsphäre schlägt sich nicht nur in Unternehmen nieder, wo Geheimhaltung Pflicht ist, sondern ist auch zum Problem im Alltag geworden. Im Leben von Privaten werden Fragen zur *informationellen Selbstbestimmung*, der Hoheit über die Veröffentlichung der eigenen persönlichen Daten, laut, da Freunde auf Facebook und anderen sozialen Medien gerne eigene und fremde Daten preisgeben und Marketingfirmen untereinander Datensätze austauschen und damit handeln.

Die Fragen der OPSEC

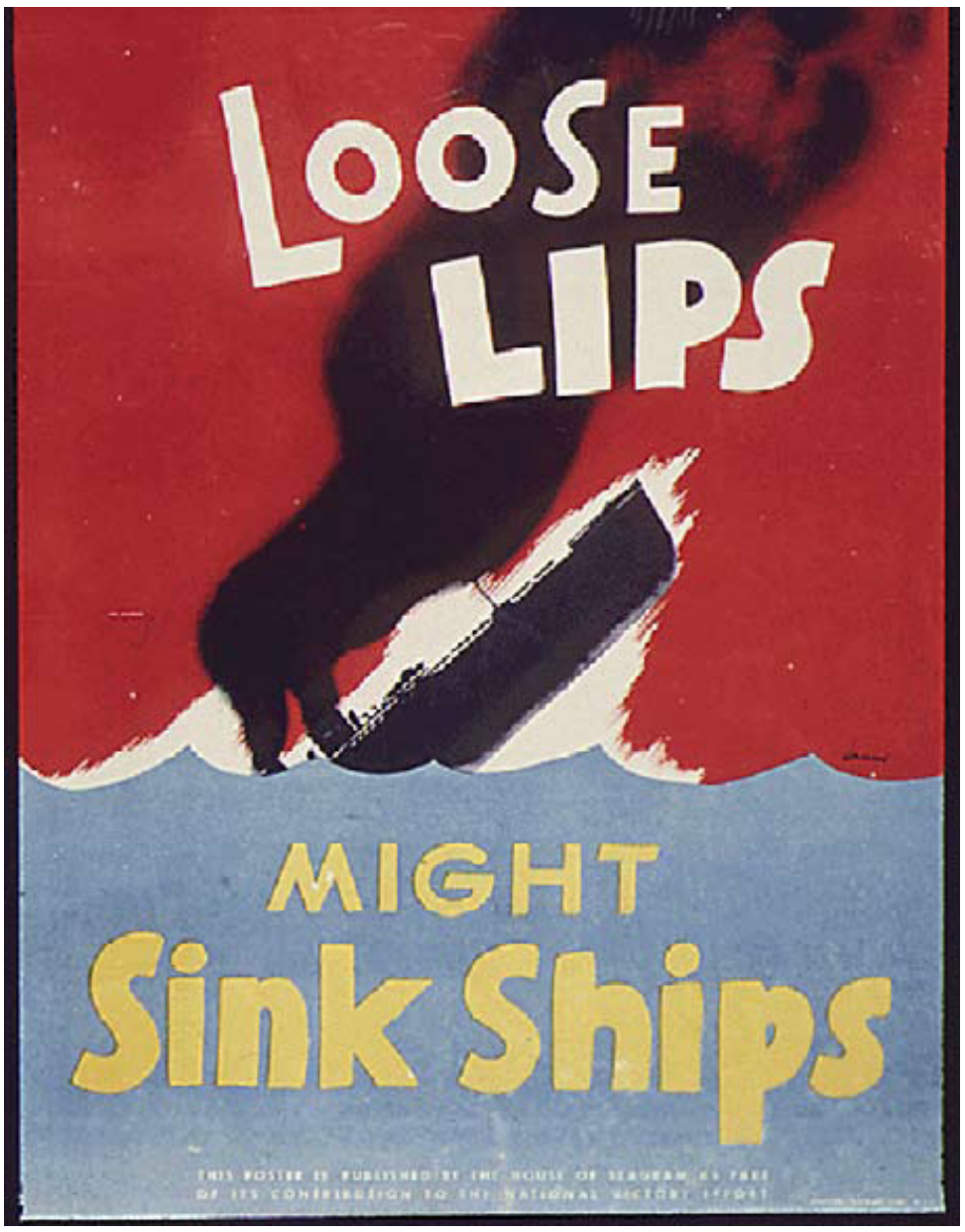
Naturgemäss sind OPSEC-Prozesse und -methoden ebenfalls geheim. Denn wenn ein Angreifer die OPSEC-Massnahmen seines Ziels kennt, dann kann er oder sie diese umgehen und dennoch zu geheimem Wissen kommen. Zum Beispiel: Wenn ein Unternehmen Codenamen verwendet, um Klienten zu benennen, kann ein Angreifer herausfinden, wer die Klienten sind, wenn er das System der Namensgebung kennt.

Daher beschäftigen sich viele Unternehmen mit OPSEC-Prozessen, trainieren ihre Angestellten , sich daran zu halten und überarbeiten die Prozesse immer und immer wieder. Denn OPSEC ist ein Prozess und kein Status. Damit eine solide Basis für OPSEC entstehen kann, bedarf es einem Framework. Um dieses zu erarbeiten können Fragen aus dem Journalismus hinzugezogen werden um festzustellen, was wann wo wie und weshalb vor wem geschützt werden muss.

- Was muss geschützt werden?
- Warum muss es geschützt werden?
- Vor wem muss es geschützt werden?
- Wann muss es geschützt werden?
- Wo muss es geschützt werden?
- Wie ist es am besten geschützt?

Das sind recht generische Fragen, aber sie haben sich als funktional herausgestellt und liefern die wichtigsten Antworten. Aus ihnen kann abgelesen werden, was wirklich wichtig ist. Sie liefern aber nicht die Antworten auf alles und führen nicht unmittelbar zu OPSEC-Massnahmen. Die Beantwortung der Fragen ist vielmehr nur der Anfang des Prozesses. Nach diesen grundlegenden Fragen können die konkreten Massnahmen angegangen werden.

Der Grund liegt nicht darin, dass die Fragen ungenügend sind, sondern sie sollen nur der Faktenfindung dienen.



OPSEC-Poster aus dem zweiten Weltkrieg.

Denn die Antworten geben eine Richtung vor oder zeigen einen Hinweis auf eine Richtung, nicht aber den Weg dahin.

Die drei Richtungen der OPSEC

Es gibt drei Stossrichtungen oder Herangehensweisen an OPSEC, jede mit ihren eigenen Vor-und Nachteilen. Der Hauptunterschied dieser Herangehensweisen liegt im Ausgangspunkt des zu Massnahmen führenden Denkprozesses, selbst wenn die endlich eingeführten Massnahmen dieselben sind, wie wenn eine andere Herangehensweise gewählt wurde.

Jede dieser Herangehensweisen wird nach der abstrakten Erklärung mit einem theoretischen Business Use Case illustriert. Im Beispiel wird ein Automobilhersteller verwendet, der ein revolutionäres Auto vor der Markteinführung geheim halten will.

Der Feind zuerst

Die Herangehensweise *Der Feind zuerst* basiert auf realistischer und fundierter Einschätzung des Feindes. Die wichtigste Frage, die absolut beantwortet und klar beantwortet werden muss, ist *Wer möchte an meine Daten?* Sollte diese Frage nicht fundiert und klar beantwortet werden, dann sollte diese Herangehensweise wohl nicht gewählt werden. Die Frage nach dem *Wer* setzt intimes oder zumindest fundiertes Wissen über den Gegner und seine Fähigkeiten voraus.

- Wer ist der Gegner?
- Was kann er?
- Welche Mittel zur Verteidigung gegen diesen Gegner gibt es?

Bei der sachlichen Einschätzung von Gegnern scheint es zunächst sinnvoll, alles und jeden einzuschliessen, darunter die chinesische Regierung, Betrüger aus Nigeria, die NSA, Konkurrenzfirmen und die Nachbarn. Aber diese Denkweise, wenn auch auf den ersten Blick sinnvoll, wird die Kosten für die Verteidigung ins Astronomische steigen lassen. Daher zahlt es sich aus realistisch zu bleiben. Vielleicht ist weder die chinesische Regierung noch die NSA am Unternehmen interessiert. Vielleicht kann der Nachbar nicht einmal einen Computer jenseits von Internet Explorer verwenden. Die Nigerianer sind dafür bekannt, einfache Ziele auszunehmen und werten meist Quantität höher als Qualität, weshalb sie auch wegfallen.

Es bleiben nur noch die Konkurrenten übrig. Die Konkurrenz ist natürlich daran interessiert, Geheimnisse zu erfahren, aber das sollen sie nicht, weil das den für den Wettbewerb notwendigen Vorteil eliminieren würde. Doch mit dem Wissen, dass die Konkurrenz der Feind ist, können Massnahmen ergriffen werden. Es ist aber schwierig, etwas auf unbestätigten oder veralteten Fakten zu basieren, da auch die Konkurrenz kein Interesse daran hat, dass jemand ihre Geheimnisse kennt. Wenn das Assessment der Konkurrenz dennoch auf solidem Wissen und nüchterner Einschätzung basieren, können die daraus erarbeiteten Verteidigungsmassnahmen sehr effektiv sein.

Beispiel: Das neue Auto muss vor Industriespionen geschützt werden. Das sind in erster Linie chinesische Grossindustrielle, die hinter den Bauplänen her sind. Sollten diese oder ein fertiges Auto ihnen in die Hände fallen, so würde die Marktposition des Autos gefährdet. Daher ist es wenig ratsam, das neue Auto in China oder einem chinafreundlichen Land herzustellen.

Das Projekt zuerst

Die Herangehensweise *Projekt zuerst* entscheidet über OPSEC-Massnahmen basierend auf den Eigenschaften des geheimen Projekts. Sie ist wohl die umfangreichste und am schwierigsten einzuhaltende Herangehensweise, da die Herangehensweise nicht das gesamte Spektrum der vom Betrieb ausgeführten Aktivitäten abdeckt, sondern granulär auf einzelne Teilprojekte angewendet wird. Aber im Gegenzug liefert sie, wenn gut durchdacht und umgesetzt, ein hohes Mass an Sicherheit, da jede Operation und jedes Projekt in einem Unternehmen oder im Privatleben massgeschneiderte Sicherheit erhält. Die Herangehensweise kann auch zu einer soliden aber bewusst vage definierten Grundlage für Sicherheitsvorkehrungen führen und somit einen Massnahmenkatalog, zumindest im Abstrakten, definieren, der künftige Projekte vereinfacht.

Projekt zuerst analysiert jedes Projekt als eigenständiges Konstrukt und stellt echte und potentielle OPSEC-Lücken fest, zeigt auf, wo Informationen abfliessen könnten und - im schlimmsten Falle - zum kompletten Scheitern des Projekts führen können. Wenn diese Herangehensweise gewählt wird, zahlt es sich aus, auf der Seite der Vorsicht zu schreiten und scheinbar harmlose OPSEC-Lücken überzubewerten.

Ein Projekt unter *Projekt zuerst* kann alles sein, von einer Business-Operation zu einer gefälschten Identität, die ohne Kompromittierung existieren soll. Das kann sogar ein IT Security Audit in einer Firma sein, in der externe Auditoren undercover agieren müssen, damit Angestellte nichts von den stetig stärker werdenden Angriffswellen mitbekommen.

Die journalistischen Fragen können dabei helfen eine Liste von Wörtern und Begriffen zu finden, die Tabu sind. Sie sollen nicht ausgesprochen werden. Personal, die in die Operation eingebunden sind, sind nicht beim Namen zu nennen, die Assets des Projekts sind unter Codenamen zu nennen, Ort und Zeit des Projekts könnten dazu führen, dass ein Angreifer die Art des Projekts ermitteln kann.

Unter *Projekt zuerst* ist es von grosser Wichtigkeit, dass die über die aktuelle Sicherheit Entscheidenden nicht nur Vertraute sind sondern auch bewusst objektiv bis kritisch an die Definition der Massnahmen herangehen. Auch ist es notwendig, dass C-Level und andere den Definierenden Vorstehen-

den in der Lage sind, Dinge zu hören, die ihnen nicht gefallen werden, wenn es um Sicherheitslücken geht. In den frühen Phasen des Projektes sehr kritisch zu sein und auf gegenseitiges Schulterklopfen und Schmeicheln zu verzichten, zahlt sich mittel- bis langfristig aus, wenn das Projekt in die operative Phase übergeht.

Beispiel: Die Markteinführung des neuen Autos steht an. Damit diese möglichst geheim bleibt und nur Fachpresse, aber nicht den Industriespionen zugänglich ist, werden Einladungen gezielt verschickt und die Halle, in der das Auto vorgestellt wird unter falschem Namen gemietet. Catering und anderen Diensten wird erzählt, dass es sich um ein Investorentreffen handelt. Zudem werden alle Anwesenden mit einem Non-Disclosure Agreement belegt. Die Fenster der Halle werden abgedeckt.

Assets zuerst

Die dritte Herangehensweise, *Assets zuerst*, ist die defensivste Herangehensweise und diejenige, die sich am engsten an Fakten und bestätigtes Wissen hält. Es handelt sich hierbei um die Inversion von *Feind zuerst*. Sollte diese Herangehensweise gewählt werden, werden Daten, Personal und alles Schützenswerte detailliert analysiert und die Hochrisiko-Assets definiert. Diese sind die kritischen Assets, die, wenn sie in die falschen Hände fallen, zu grossem Schaden oder dem totalen Scheitern der Operation führt.

Verteidigungsmassnahmen für diese Hochrisiko-Assets können Zugriffsrestriktion, Codenamen, Aufteilung von Wissen und die Nutzung von Non-Disclosure Agreements (NDA) sein. In der Implementationsphase dieser Massnahmen ist es wichtig, den in der Operation involvierten die Wichtigkeit ihrer Aufgaben bewusst zu machen. NDAs sind zwar effektiv aber nicht der Weisheit letzter Schluss. Ferner sollte das Wissen vermittelt werden, dass OPSEC nur einmal scheitern muss bevor grosser Schaden entstehen kann.

Beispiel: Das grösste Asset des Autoherstellers ist das neue Modell. Daher muss das Auto vor der Markteinführung um jeden Preis geschützt werden. Nicht einmal der CEO der Firma kennt alle Geheimnisse des Fahrzeugs. Ausserhalb der Firma wird nicht über das neue Auto gesprochen und auch in-house wird nur mit einem Codenamen über das neue Auto gesprochen. Sogar der Motor und die neue Auspufftechnologie werden mit Codenamen versehen. Externe Berater und Fachkräfte sind mit NDA belegt und haben keinen externen Zugriff auf Mails oder Kalenderdaten.

Die richtige Wahl

Die richtige Wahl über die Herangehensweise zu treffen ist, genau wie die Wahl der endlich implementierten Massnahmen, ein Diskussionsthema zwischen Entscheidungsträgern und Experten im Unternehmen oder im Kern des Geheimnisses. Die journalistischen Fragen, die in diesem Artikel gestellt worden sind, zu beantworten kann auf eine Tendenz hinweisen, die eine Herangehensweise anbietet, aber auch diese Tendenz sollte hinterfragt werden.

Es lohnt sich, dass zumindest eine der im Geheimnis involvierten Parteien die stetige Rolle des Angreifers einnimmt, Löcher in Argumente, Pläne und Ideen bohrt. In diesem Prozess könnte es auch lohnenswert sein, externe Experten hinzuzuziehen, abhängig davon, wie gross und umfangreich die geheime Operation ausfällt. Denn solange die fiktiven Angreifer auf der Seite des Geheimnisses stehen und Sicherheitslücken feststellen bevor sie ausgenutzt werden, dann können diese vor der operativen Phase behoben werden und ein echter Angreifer seine Arbeit beginnen kann.

Zusammenfassung

Geheimnisse sind so alt wie das Leben. Geheimnisse zu wahren ist schwieriger denn je. Daher hat sich das militärische Konzept der OPSEC an die Existenz moderner Privatpersonen und Unternehmen angepasst und betrifft nun alle Aspekte des Lebens. Es gibt eine Vielzahl der Herangehensweisen, damit die Operational Security verbessert werden kann. Nur wenige davon sind technologischer Natur. Die Massnahmen sind bewusst low-tech und verlassen sich auf theoretische Konzepte, da die praktischen Aspekte einem längeren Überlegungsprozess folgen, der keine technologischen Aspekte hat.

Es ist wichtig, zu wissen, dass OPSEC nur einmal scheitern muss bevor der Schaden permanent entstanden ist. Mit diesem Wissen im Hinterkopf zahlt es sich aus, jede vorgeschlagene Sicherheitsmassnahme und jeden Aspekt der geheimen Operation mehrfach zu hinterfragen. Ebenso wichtig ist das Wissen, dass alle Personen im Zentrum des Geheimnisses zum vertrauten Zirkel gehören und das selbe Ziel verfolgen - die Sicherheit der Operation und deren Implementation. Ihre Kritik ist kein persönlicher Angriff, sondern eine Massnahme zur Erreichung des selben Ziels.

SERVICE

Security Assessment

Auch ein gut funktionierendes Sicherheitskonzept kann Lücken haben. Auditoren mit einem Auge für Schwachsstellen können da Abhilfe schaffen.

Security Assessments, auch Security Audits genannt, sind fast schon Klassiker im Security-Bereich: Sie gehören zu den am längsten etablierten und auch zu den wirkungsvollsten Prozessen im Sicherheitsbereich. Während eines Assessments werden Objekte auf ihren aktuellen Stand der Sicherheit hin untersucht. Meist werden diese Untersuchungen von automatisierten Vulnerability Scannern übernommen. Das führt in der Regel zu eineem schnellen Überblick, braucht wenig Zeit und erhöht so die Wirtschaftlichkeit eines Assessments enorm.

Die Interpretation der Daten hängt dann aber vom Fachwissen und der Fachsicherheit von Menschen ab. Die Erkenneung von Falschmeldungen oder die Einteilung von Risiken in vordefinierte Klassen kann nur von erfahrenen und gut ausgebildeten Auditoren zuverlässig erledigt werden. Dieser geschulte Blick und die in die Untersuchung eingeflossene Erfahrung sichern dann die Genauigkeit der Datenprüfung.

Exploiting auf sicherer Seite

Mit der automatischen und manuellen Datenprüfung alleine ist das Assessment aber noch nicht abgeschlossen. Damit die Grösse der Sicherheitslücken und der mögliche Schaden, der durch ihre Ausnutzung entstehen kann, zweifelsfrei festgestellt werden kann, werden diese Lücken von den Auditoren ausgenutzt.Im Zuge dieses Schritts werden fast schon als Nebeneffekt alle *false positives* aus der automatischen Schwachstellenerkennungsphase erkannt. Dennoch werfen die Auditoren einen Blick auf die scheinbaren Fehlalarme, um zu garantieren, dass da nichts ist, dass Ihnen Schaden zufügen könnte.

Wie ein Angreifer

Das Vorgehen während eines Security Assessments unterscheidet sich nur wenig von dem eines echten Angreifers, der Ihrem Unternehmen oder Ihrem Netzwerk Schaden zufügen will. Die Auditoren der scip AG versuchen zuerst, so viel Wissen über die Zielumgebung - also Ihr Unternehmen und Ihr Netzwerk - wie möglich zu finden. Dessen Auswertung zeigt ihnen dann den erfolgversprechendsten Punkt für ihren Angriff.

Das Ziel eines Audits ist nicht, in ein System einzubrechen. Es geht darum, die Angriffsfläche und damit alle potentiellen Schwachstellen festzustellen. Längerfristig soll die Sicherheit in allen Bereichen gewahrt oder gar erhöht werden können.

Haben wir Ihr Interesse geweckt? Zögern Sie nicht und kontaktieren Sie uns unter der Telefonnummer +41 44 404 13 13 oder schicken Sie eine Mail an info@scip.ch.

JETZT ERHÄLTLICH

scip Labs 7 - Das neue Jahrbuch

Die spannendsten Fachbeiträge des vergangenen Jahrs sind auf fast 400 Seiten gesammelt und überarbeitet worden. Das Buch ist ein Deutsch und Englisch per Klick auf das Cover erhältlich.

Das verflixte siebente Jahr merkt man Labs, der regelmässigen Publikation der scip AG nicht an: Mit der Verlässlichkeit eines Uhrwerkes erscheinen die Artikel der Mitarbeiter aus allen Geschäftsbereichen der scip AG allwöchentlich und erreichen mittlerweile eine Leserschaft, die zu den grössten im deutschsprachigen Bereich gehört.

Weniger vorhersehbar sind die Themen, mit denen sich Labs beschäftigt: Der Bereich der Informationssicherheit ist so vielschichtig und schnelllebig, nicht selten finden tagesaktuelle Themen noch binnen Wochenfrist ihren Weg zur Veröffentlichung.

Es überrascht daher wenig, dass der dritte Sammelband, Labs 7, eine Selektion mit interessanter Bandbreite zusammenfasst: Von Wearables über Drohnen bis hin zu klassischen Themen wie Datenverschlüsselung oder Compliance bietet dieses Buch einen gleichermassen abwechslungsreichen und aktuellen Ausflug durch alle Bereiche der Informationssicherheit.

Mit einem Vorwort von Pascal Adam, Chief Information Security Officer der Schweizer Parlamentsdienste und Dozent an der Telematikschule Bern.

VULDB

Die Top 5 Schwachstellen des Monats

Die Top 5 Liste zeigt die interessantesten und schwerwiegendsten Schwachstellen des laufenden Monats. Alle Schwachstellen und Statistiken gibt es tagesaktuell in der scip VulDB.

1 Microsoft Windows DirectShow Heap-based Pufferüberlauf

Datum	12.01.2016
Risiko	kritisch
Link	http://www.scip.ch/?vuldb.80220

Es wurde eine Schwachstelle in Microsoft Windows bis Server 2012 R2, ein Betriebssystem, gefunden. Sie wurde als kritisch eingestuft. Es betrifft eine unbekannte Funktion der Komponente DirectShow. Die Schwachstelle lässt sich durch das Einspielen des Patches MS16-007 beheben. Dieser kann von technet.microsoft.com bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Microsoft hat sofort reagiert.

2 Microsoft Windows win32k.sys Pufferüberlauf

Datum	12.01.2016
Risiko	kritisch
Link	http://www.scip.ch/?vuldb.80215

In Microsoft Windows bis Server 2008 R2 SP1, ein Betriebssystem, wurde eine kritische Schwachstelle ausgemacht. Es geht um eine unbekannte Funktion der Bibliothek win32k.sys. Die Schwachstelle lässt sich durch das Einspielen des Patches MS16-005 lösen. Dieser kann von technet.microsoft.com bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Microsoft hat damit sofort gehandelt.

3 Microsoft Internet Explorer VBScript/JScript Pufferüberlauf

Datum	12.01.2016
Risiko	kritisch
Link	http://www.scip.ch/?vuldb.80209

In Microsoft Internet Explorer 8/9/10/11, ein Webbrowser, wurde eine kritische Schwachstelle entdeckt. Hierbei betrifft es eine unbekannte Funktion der Komponente VBScript/JScript. Die Schwachstelle lässt sich durch das Einspielen des Patches MS16-003 lösen. Dieser kann von technet.microsoft.com bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Microsoft hat demnach sofort gehandelt.

4 Google Chrome MIDI Subsystem midi_manager.cc Pufferüberlauf

Datum	24.12.2015
Risiko	kritisch
Link	http://www.scip.ch/?vuldb.79884

Es wurde eine kritische Schwachstelle in Google Chrome bis 47 entdeckt. Betroffen hiervon ist eine unbekannte Funktion der Datei midi_manager.cc der Komponente MIDI Subsystem. Ein Upgrade auf die Version 47.0.2526.106 vermag dieses Problem zu beheben. Eine neue Version kann von chrome.google.com bezogen werden.

5 Microsoft Office Office Document Handler Pufferüberlauf

Datum	12.01.2016
Risiko	kritisch
Link	http://www.scip.ch/?vuldb.80216

Eine kritische Schwachstelle wurde in Microsoft Office bis 2016 ausgemacht. Es geht hierbei um eine unbekannte Funktion der Komponente Office Document Handler. Die Schwachstelle lässt sich durch das Einspielen des Patches MS16-004 beheben. Dieser kann von technet.microsoft.com bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Microsoft hat hiermit sofort reagiert.

Auswertungsdatum: 18.01.2016

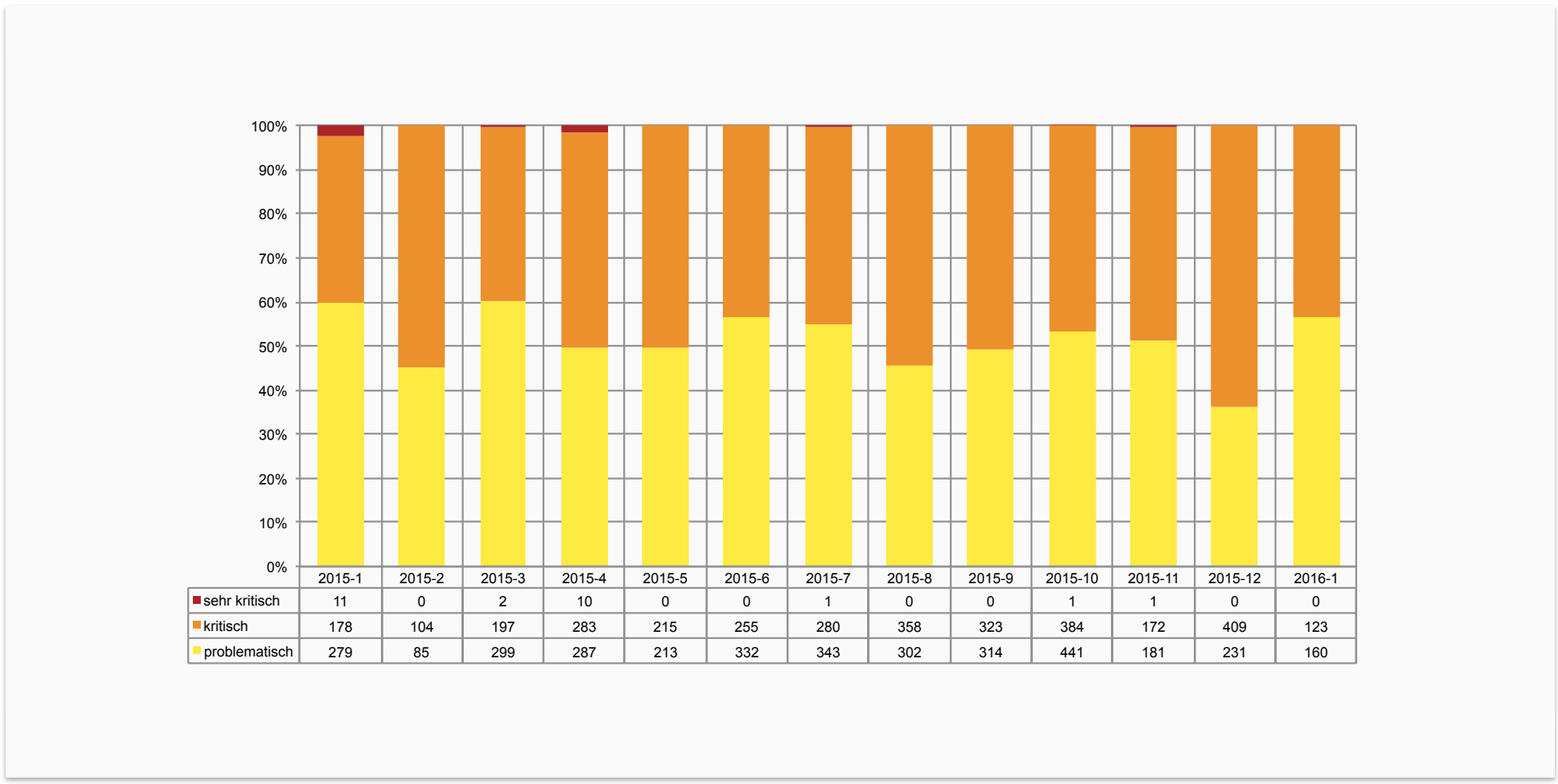
VULDB

Statistiken aus der VulDB

Die Welt der Information Security wandelt sich stets. Um einen Überblick über den Verlauf und die Entwicklungen der Schwachstellen zu erhalten, analysieren wir die scip VulDB einmal im Monat.

MEISTBETROFFENE PRODUKTE IM VERGANGENEN MONAT

VERLAUF DER SCHWACHSTELLEN DER VERGANGENEN 12 MONATE



	2015-1	2015-2	2015-3	2015-4	2015-5	2015-6	2015-7	2015-8	2015-9	2015-10	2015-11	2015-12	2016-1
sehr kritisch	11	0	2	10	0	0	1	0	0	1	1	0	0
kritisch	178	104	197	283	215	255	280	358	323	384	172	409	123
problematisch	279	85	299	287	213	332	343	302	314	441	181	231	160

Auswertungsdatum: 18.01.2016