Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

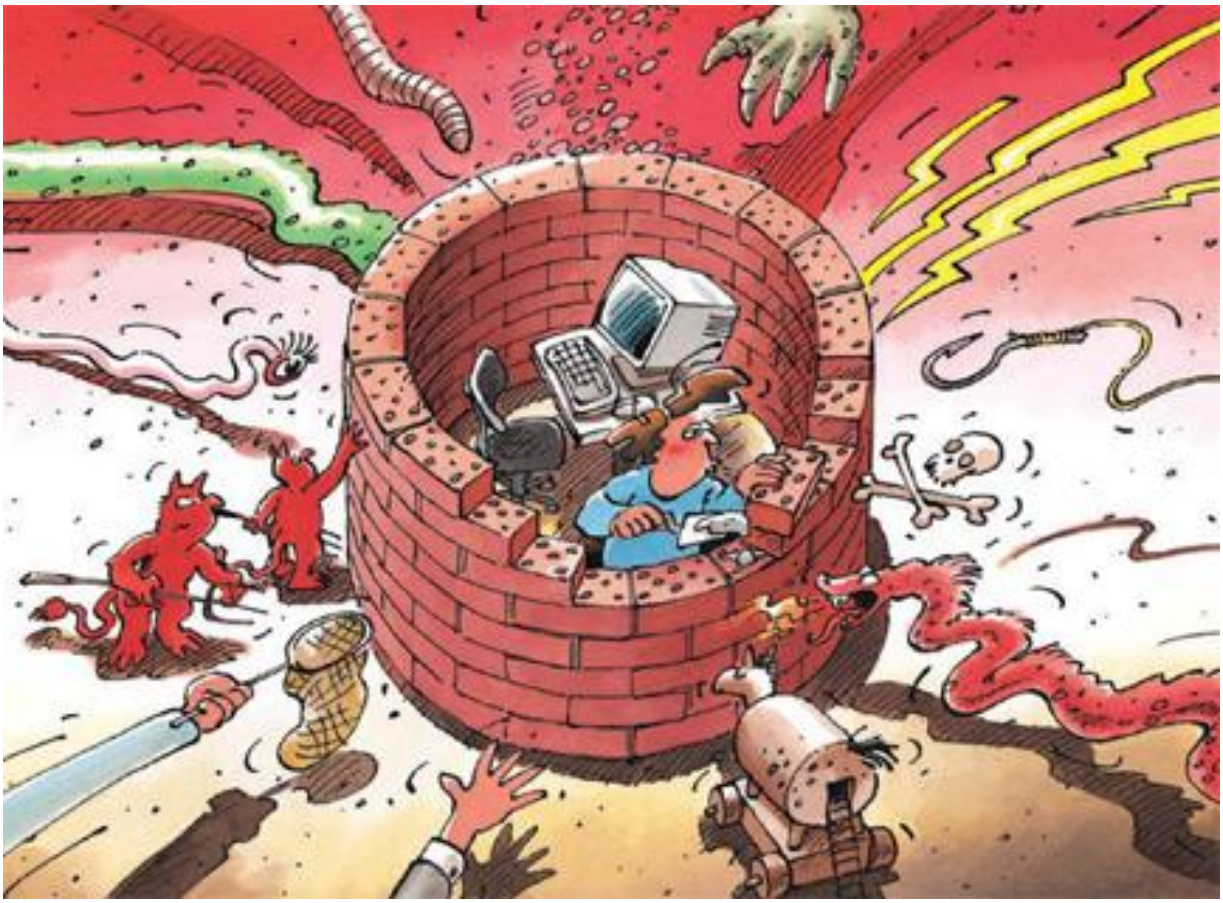
Informatiksteuerungsorgan des Bundes ISB
Nachrichtendienst des Bundes NDB

Melde- und Analysestelle Informationssicherung MELANI
www.melani.admin.ch

Informationssicherung

Lage in der Schweiz und international

Halbjahresbericht 2013/I (Januar – Juni)



Inhaltsverzeichnis

1 Schwerpunkte Ausgabe 2013/I

DDoS – massive Angriffe auch in der Schweiz
In der ersten Jahreshälfte 2013 ereignete sich die bisher grösste DDoS-Attacke in der Geschichte des Internets. Ziel war die in der Schweiz ansässige Non-Profit Organisation Spamhaus. Auch Schweizer DNS-Server wurden für DDoS-Angriffe missbraucht. Im Januar 2013 wurde die DNS-Infrastruktur der Stiftung SWITCH für eine Attacke auf Dritte missbräuchlich eingesetzt. MELANI zeigt Massnahmen auf, die getroffen werden können, um die eigene DNS-Infrastruktur vor Missbrauch bei DNS- Amplifikationsattacken zu schützen.
► **Aktuelle Lage Schweiz:** Kapitel 3.1

- **Kommunikationsüberwachung im Internet**
  Besonders ein Thema machte im letzten halben Jahr Schlagzeilen: Die mutmasslichen Abhörmethoden einzelner Nachrichtendienste, die durch den Informanten Edward Snowden publik gemacht wurden. Begonnen haben die Enthüllungen mit dem NSA-Abhörprogramm Prism, danach folgte die Veröffentlichung über die Möglichkeiten des Britischen Government Communications Headquarters (GCHQ), transatlantische Tiefseekabel zu überwachen und die Publikation einer Präsentation des Analyse-Programms XKeyscore.
  ► **Aktuelle Lage International:** Kapitel 4.1
  ► **Tendenzen/Ausblick:** Kapitel 5.1
- **Advanced Persistent Threats – zahlreiche Fälle veröffentlicht**
  Im ersten Halbjahr 2013 wurden zahlreiche gezielte und professionelle Angriffe auf Unternehmen oder staatliche Stellen bekannt. Da meist staatliche Akteure hinter den Angriffen vermutet wurden, hatten diese Attacken auch zahlreiche politische Stellungnahmen zur Folge.
  ► **Aktuelle Lage International:** Kapitel 4.2
- **Problemzone Content Management System**
  In den vergangenen Jahren ist die Anzahl von Webauftritten im Internet geradezu explodiert. Auch technisch nicht versierte Benutzer können dank einfachen Mitteln eine eigene Webseite ins Internet stellen. Dazu werden oftmals so genannte Content Management Systeme (kurz CMS) verwendet. Die zunehmende Verbreitung solcher Systeme macht diese auch für Cyberkriminelle interessant. Diese suchen vermehrt nach Schwachstellen in solchen Systemen und werden auch immer wieder fündig.
  ► **Tendenzen/Ausblick:** Kapitel 5.4
- **Smartphone-Trojaner auf dem Vormarsch**
  Der Trend von Schadsoftware auf Smartphones hat sich im letzten Halbjahr erneut fortgesetzt und hat in den letzten Monaten stark zugenommen. Im Fokus steht dabei vor allem das Betriebssystem Android.
  ► **Aktuelle Lage Schweiz:** Kapitel 3.3
  ► **Tendenzen/Ausblick:** Kapitel 5.6
  ► **Anhang:** Kapitel 7.1
- **SCADA-Systeme und Industriesteuerungen: Problembereiche, Sicherheitslücken, Angriffe und Schutz**
  Im Prinzip kann man bei jedem System, welches einen physischen Prozess regelt und/oder überwacht, von einem «Industriellen Kontrollsystem (ICS)» sprechen. Während bei klassischen Informatiksystemen nebst der Verfügbarkeit die Vertraulichkeit und die Integrität einen ebenso hohen Stellenwert geniessen, steht bei ICS die Verfügbarkeit stärker im Mittelpunkt.
  ► **Aktuelle Lage International:** Kapitel 4.5

2 Einleitung

Der siebzehnte Halbjahresbericht (Januar – Juli 2013) der Melde- und Analysestelle Informationssicherung (MELANI) erläutert die wichtigsten Tendenzen rund um die Gefahren und Risiken, die mit den Informations- und Kommunikationstechnologien (IKT) einhergehen. Er gibt eine Übersicht über Ereignisse im In- und Ausland, beleuchtet Themen im Bereich der Prävention und fasst Aktivitäten staatlicher und privater Akteure zusammen. Erläuterungen zu Begriffen technischer oder fachlicher Art (Wörter in kursiv) sind in einem **Glossar (Kapitel 6)** am Ende dieses Berichts zu finden. Die Beurteilungen von MELANI sind jeweils farblich hervorgehoben.

Ausgewählte Themen dieses Halbjahresberichtes sind in **Kapitel 1** angerissen.

Kapitel 3 und 4 befassen sich mit Pannen und Ausfällen, Angriffen, Kriminalität und Terrorismus, die einen Zusammenhang mit IKT-Infrastrukturen aufweisen. Anhand ausgewählter Beispiele werden wichtige Ereignisse der ersten Hälfte des Jahres 2013 aufgezeigt. Kapitel 3 behandelt dabei nationale Themen, Kapitel 4 internationale Themen.

Kapitel 5 enthält Tendenzen und einen Ausblick auf zu erwartende Entwicklungen.

Kapitel 7 ist ein Anhang mit erweiterten Erläuterungen und Anleitungen zu ausgewählten Themen des Halbjahresberichtes.

3 Aktuelle Lage IKT-Infrastruktur national

3.1 DDos-Angriffe – zahlreicher und intensiver

In den vergangenen Monaten sind die so genannten *Distributed Denial Of Service (DDoS)* - Attacken im Fokus von Cyberkriminellen geblieben. Dabei lassen sich viele verschiedene Arten von DDoS-Angriffen unterscheiden. Einige behelfen sich dabei einem sogenannten *Botnetz*, welches aus infizierten Computern (Bots) oder gekaperten Servern im Internet besteht. Andere Arten von DDoS machen sich schlecht oder ungenügend gesicherte Systeme im Internet und/oder Schwächen in Internet-Protokollen zu Nutze. Solche DDoS-Angriffe sind nichts Neues, jedoch haben diese in den vergangenen Monaten sowohl in der Anzahl als auch an Intensität zugenommen. Während US-Banken weiterhin im Fokus von DDoS-Angriffen standen (siehe Abschnitt «Brobot weiterhin aktiv»), wurden auch einige Schweizer Unternehmen Ziel von DDoS-Angriffen. Mehr dazu in den kommenden Kapiteln.

Grösste DDoS-Attacke der Geschichte gegen Spamhaus

In der ersten Jahreshälfte 2013 ereignete sich die bisher grösste DDoS-Attacke in der Geschichte des Internets. Ziel war die in der Schweiz ansässige Non-Profit Organisation Spamhaus[1], welche sich mit der Bekämpfung von Spam und anderen Gefahren aus dem Cyberspace beschäftigt.

Im März 2013 startete eine unbekannte Täterschaft einen massiven DDoS-Angriff gegen die Website von Spamhaus. Dieser hielt mehrere Tage an und erreichte auf seinem Höhepunkt ein Datenvolumen von 300Gbp/s, was dem Dateninhalt von über 50 CDs entspricht – pro Sekunde. Spamhaus wandte sich daraufhin an den Cloud-Provider CloudFlare, welcher versuchte, den Angriff abzuwehren. Den Abwehrversuch von CloudFlare konterten die Angreifer mit einer Attacke auf den Internetknoten LINX in London (London Internet Exchange), worauf sämtlicher über diesen Internetknoten abgewickelter Datenverkehr kurzzeitig massiv beeinträchtigt wurde[2].

Bei dem DDoS-Angriff handelte es sich um eine sogenannte *DNS Amplifikationsattacke*. Dabei werden gefälschte *DNS*-Anfragen an offene DNS-Server im Internet (sogenannte *Open DNS resolvers*).[3] gesendet. Da die DNS-Anfragen gefälscht waren und die Quell-IP Adresse von Spamhaus enthielten, bewirkte dies, dass die offenen DNS-Server ihre Antworten an die IP-Adresse von Spamhaus sendeten und nicht an den tatsächlichen Absender des *Datenpakets*. Da eine Antwort auf eine DNS-Anfrage typischerweise um ein vielfaches grösser ist als die DNS-Anfrage selber, konnte so mit vergleichsweise wenig Bandbreite eine beachtliche Netzwerklast von bis zu 300Gbit/s generiert werden.

---

1 The Spamhaus Project: http://www.spamhaus.org/ (Stand: 31. August 2013).

2 The Verge - Spam war caused failure at critical internet exchange center: http://www.theverge.com/2013/3/28/4156570/Dutch-spamhaus-DDoS-took-down-london-internet-exchange (Stand: 31. August 2013).

3 Für Informationen über die Anzahl *Open DNS resolver* im Schweizer AS siehe: http://securityblog.switch.ch/2013/05/02/ddos-and-open-resolvers-the-swiss-view/ (Stand: 31. August 2013).

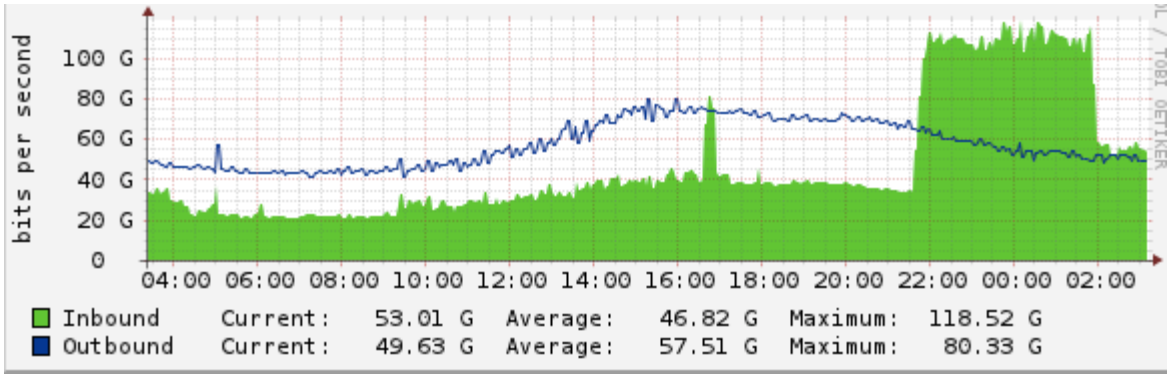


Abbildung 1: Netzwerkverkehr vor, während und nach dem DDoS Angriff (Quelle: CloudFlare)

Einige Quellen vermuteten, dass der Angriff so gross war, dass dieser kurzeitig das gesamte Internet beeinträchtigte. MELANI konnte diese Vermutungen jedoch nicht bestätigen und zumindest in der Schweiz keine Beeinträchtigung des Internets feststellen.

Folgende Massnahmen können getroffen werden, um die eigene DNS-Infrastruktur vor Missbrauch bei *DNS-Amplifikationssttacken* zu schützen:

Verhindern von IP address spoofing:

Es muss sichergestellt werden, dass Geräte im Internet keine Datenpakete mit einer beliebigen Absender IP-Adresse versenden können (*IP address spoofing*). Dazu wurde im Jahr 2000 eine Best Current Practice (BCP38) entwickelt, welche unter RFC2827 veröffentlicht wurde. Obwohl dieser Standard bereits über ein Jahrzehnt alt ist, hat ein Grossteil *der Internet Service Provider (ISP)* ihn erst teilweise oder noch gar nicht implementiert.

Um zu verhindern, bzw. die Möglichkeit zu minimieren, dass Schweizer IKT-Infrastruktur für diese Art von DDoS-Angriffen verwendet werden kann, empfiehlt MELANI allen Schweizer Internet Service Providern, den in RFC2827 beschriebenen Standard (BCP38) zur Verhinderung von IP address spoofing flächendeckend zu implementieren.

Absichern von DNS Servern:

Eine weitere Massnahme, um DNS Reflection Angriffe in Zukunft zu minimieren oder abzuschwächen, ist das Absichern von DNS-Servern. Viele (DNS-)Server, aber auch andere Netzwerk-Peripheriegeräte, werden mit einer Standardkonfiguration (meistens den Werkseinstellungen des Gerätes) an das Internet angeschlossen. Solche Standardkonfigurationen sind oftmals unsicher und zu wenig restriktiv. Konkret akzeptieren solche Geräte beispielsweise Anfragen aus dem ganzen Internet. Geräte, bzw. Software sollten so konfiguriert werden, dass diese nur Anfragen aus dem lokalen oder einem eingeschränkten IP-Adressbereich akzeptieren. Dadurch kann verhindert werden, dass sich die Geräte von Kriminellen für Angriffe auf Dritte im Internet missbrauchen lassen.

MELANI empfiehlt Betreibern von DNS-Servern oder Geräten, welche einen DNS-Dienst zur Verfügung stellen, folgende Standards und Best Practices einzuhalten bzw. umzusetzen:

1. RFC 5358 (BCP140) Preventing Use of Recursive Nameservers in Reflector Attacks: http://tools.ietf.org/html/bcp140

2. Windows 2003 Server – Securing DNS:
   http://technet.microsoft.com/en-us/library/cc785404%28v=ws.10%29.aspx
3. Secure BIND Configuration Template:
   http://www.cymru.com/Documents/secure-bind-template.html
4. Deaktivierung von DNS-Rekursion (wenn diese nicht benötigt wird):
   http://www.team-cymru.org/Services/Resolvers/instructions.html
5. Implementierung von Response Rate Limiting:
   http://www.redbarn.org/dns/ratelimits

Schweizer DNS-Server für DDoS-Angriff missbraucht

Auch Schweizer DNS-Server werden für DDoS-Angriffe missbraucht. Im Januar 2013 wurde die DNS Infrastruktur der Stiftung SWITCH, welche die Top Level Domains (TLDs) «.ch» und «.li» betreibt, für eine *DNS-Amplifikationsattacke* auf Dritte missbraucht[4]. Dabei konnten die Angreifer mit wenig Bandbreite ihrerseits eine hohe Last auf der DNS-Infrastruktur erzeugen, welche das Ziel des Angriffes mit bis zu 500Mbit/s überflutete.

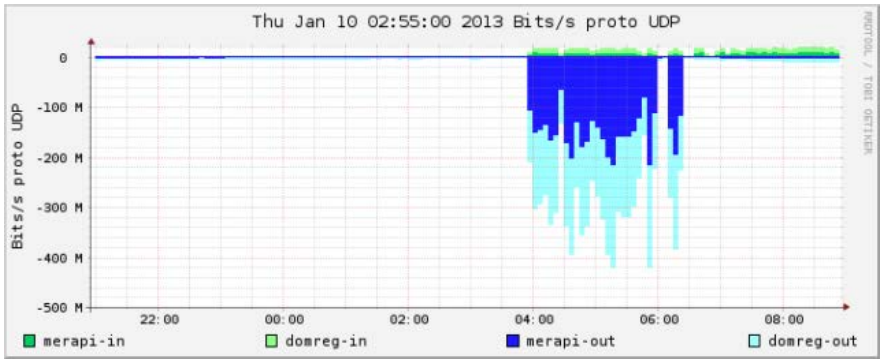


Abbildung 2: Netzwerkverkehr vor, während und nach dem DDoS-Angriff (Quelle: SWITCH Security Blog)

Da die DNS-Infrastruktur von SWITCH für grossen Datenverkehr ausgelegt ist, hatte der Missbrauch der Infrastruktur keinen Einfluss auf die Top Level Domains «.ch» und «.li». Gemäss SWITCH war es bei diesem DNS-Amplifikationsangriff möglich, mit einer Bandbreite von nur 3 MB/s Antworten mit bis zu 225MB/s zu erzeugen. Um einen solchen Angriff durchzuführen ist also (zusammen mit dem nötigen Know-How) nur ein Standard-DSL- oder Kabel-Anschluss nötig. Das Beispiel zeigt, mit wie wenig Aufwand heutzutage ein DDoS-Angriff schon möglich ist. Durch die gute Reaktion von SWITCH konnte der Missbrauch innert kürzester Zeit gestoppt werden.

[4] SWITCH Security Blog - CH-Zone Opfer eines DNS-Amplifikations-Angriffes: http://securityblog.switch.ch/2013/01/10/ch-zone-dns-angriff/ (Stand: 31. August 2013).

DDoS mit Brobot auch in der Schweiz

Im letzten MELANI Halbjahresbericht berichteten wir über DDoS-Angriffe auf US-Banken[5]. Dabei wurden die Websites mehrerer US-Banken durch DDoS-Angriffe mit Datenvolumen von bis zu 60Gbit/s beeinträchtigt und zeitweise sogar lahmgelegt. Es wird vermutet, dass der Iran hinter den Angriffen steht.

Die Angriffe werden mit Hilfe von kompromittierten Webservern durchgeführt. Dazu durchsuchen die Angreifer das Internet nach verwundbaren Joomla![6]-Installationen. Stossen die Angreifer auf ein solches, wird eine bekannte Sicherheitslücke in Joomla! ausgenutzt, um *Schadsoftware* auf dem Webauftritt des Opfers zu platzieren. Bei der Schadsoftware handelt es sich um ein bösartiges *PHP-Script* namens Brobot[7], welches eine Hintertür zum System öffnet und eine DDoS-Funktionalität besitzt. Aus Sicht der Angreifer bieten gehackte Webserver einen grossen Vorteil: Webservern steht oftmals eine grössere Bandbreite zur Verfügung als normalen Internet-Anschlüssen, weshalb sich bereits mit einer geringen Anzahl an Bots effektive DDoS-Angriffe realisieren lassen.

Auch Schweizer Websites sind von Brobot betroffen. MELANI hat in der ersten Jahreshälfte 2013 dutzende Betreiber von mit Brobot infizierten Websites informiert:

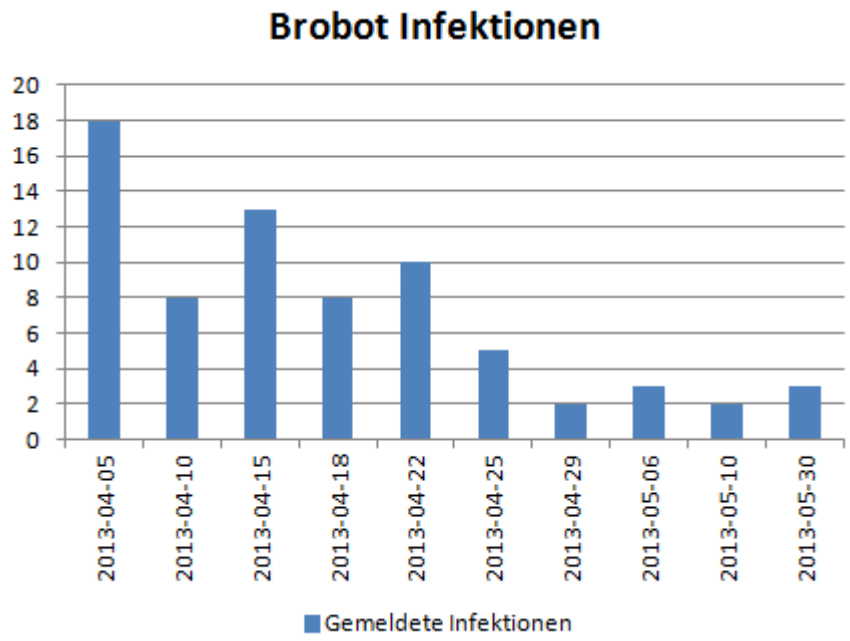


Abbildung 3: Durch MELANI gemeldete Brobot-Infektionen

---

[5] MELANI Halbjahresbericht 2012/2, Kapitel 4.2.1: http://www.melani.admin.ch/dokumentation/00123/00124/01535/index.html?lang=de (Stand: 31. August 2013).

[6] Joomla! Ist ein weit verbreitetes *Content Management System*.

[7] Symantec - PHP.Brobot: http://www.symantec.com/security_response/writeup.jsp?docid=2013-011012-0840-99&tabid=2 (Stand: 31. August 2013).

Die betroffenen Inhaber der Websites sowie die Web Hosting Provider wurden von MELANI über die Infektionen informiert. Allerdings reagierten nicht alle Betreiber – einige Webauftritte blieben über mehrere Monate hinweg infiziert und wurden regelmässig für DDoS-Angriffe gegen US-Banken missbraucht.

3.2 Phishing-Trends

Auch im ersten Halbjahr 2013 sind wiederum zahlreiche Phishing-Versuche beobachtet worden. Der Trend, dass auch E-Banking Kunden von kleineren Banken ins Visier der Angreifer geraten, hat sich fortgesetzt. Anscheinend lohnt es sich für die Betrüger, die Systeme extra für diese Ziele zu konfigurieren und anzupassen, auch wenn sie statistisch gesehen nur mit einem oder zwei potenziellen Opfern bei dem betroffenen Finanzinstitut rechnen können.

Erschweren der Deaktivierung

Verschiedene Techniken, womit die Kriminellen den Administratoren das Deaktivieren der Phishing-Seiten erschweren können, sind bereits in einem früheren Halbjahresbericht diskutiert worden.[8] In der aktuellen Berichtsperiode wurde eine neue Technik beobachtet. In diesem Fall hing das Anzeigen der Phishing-Seite von der im Browser eingestellten Zeitzone ab. Bei mitteleuropäischer Zeit wurde gephisht - in jeder anderen Zeitzone erschien eine Fehlermeldung. Dies hatte natürlich zum Zweck, dem (z. B. amerikanischen) Provider vorzugaukeln, dass die Seite bereits entfernt worden ist und keine weiteren Aktionen mehr nötig sind. Eine betrügerische Seite bleibt entsprechend länger online und fängt damit auch potenziell mehr Opfer.

Phishing-Seite gegen Schweizer Finanzinstitut erstmals in Flash

Im Normalfall kopieren die Betrüger beim Erstellen der Phishing-Seiten die Originalseite der Bank, machen ein paar kleine Änderungen und speichern diese danach auf einen Server, der für diesen Betrug präpariert ist. Dieser Vorgang ist relativ simpel und verlangt auch keine grossen IKT-Kenntnisse. Erstaunlich ist, dass nun erstmals eine Phishing-Seite in *Flash* entdeckt wurde, welche gegen ein Schweizer Finanzinstitut gerichtet war. Über den Grund, weshalb Betrüger auf diese eher komplizierte Programmierungsart zurückgreifen, kann nur spekuliert werden. Daten, die sich jeweils im Verzeichnis der Phishing-Seite befunden haben, lassen darauf schliessen, dass die Betrüger einen einfachen Kit zur Erstellung von Webseitenformularen benutzt haben, das Flash-Versionen generiert. Ein anderer möglicher Grund könnte sein, dass der Text in diesen Flash-Programmen nicht durchsuchbar ist. Antiphishing-Programme haben weniger Möglichkeiten, anhand von Schlüsselwörtern eine Phishing-Seite zu erkennen und den Computernutzer zu warnen.

Auch E-Banking-Kunden von kleineren Banken betroffen

Es wird vermehrt beobachtet, dass neben den zahlreichen Phishing-Versuchen gegen Kreditkartenfirmen und Grossbanken in der letzten Zeit auch kleinere Banken von Phishing be-

[8] MELANI Halbjahresbericht 2011/2, Kapitel 3.4: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=de (Stand: 31. August 2013).

troffen sind. Ein Grund dürfte sein, dass die Betrüger auf diese Finanzinstitute ausweichen in der Hoffnung, dass hier die Sicherheitsmassnahmen noch nicht so hoch sind, respektive die Kunden noch nicht oft mit diesem Phänomen konfrontiert worden sind.

Rein statistisch würde ein Angriff auf kleinere Banken nur Sinn machen, wenn eine exzellente Datenlage existiert und gezielt Kunden ausschliesslich dieser Bank angeschrieben werden. Dieses gezielte Vorgehen bei kleineren Banken konnte bis heute nicht festgestellt werden – die Verbreitung respektive der Versand der Phishing-Mails scheint nach wie vor eher nach dem Prinzip Zufall zu funktionieren.

3.3 E-Banking-Schadsoftware auf Smartphones im Umlauf

Die Melde- und Analysestelle Informationssicherung MELANI hat im ersten Halbjahr 2013 vor einer neuen Angriffswelle auf Schweizer E-Banking-Geschäfte mit SMS-Transaktionssignierung gewarnt. Bei dieser Angriffsart wird eine Schadsoftware auf dem Computer installiert. Loggt sich ein Kunde in sein E-Banking-Konto ein, erscheint eine Meldung, wonach ein neues E-Security-Zertifikat installiert werden müsse. Der Kunde wird aufgefordert, den Typ seines Smartphones sowie die mobile Telefonnummer anzugeben. Danach wird der Kunde per SMS aufgefordert, das neue Zertifikat auf dem Smartphone zu installieren. Tatsächlich wird auf dem Gerät jedoch eine Schadsoftware installiert, die es den Angreifern erlaubt, die für die Transaktionssignierung notwendige SMS abzufangen und missbräuchliche Zahlungen vorzunehmen.

Abbildung 4: Fenster, das während dem Login-Vorgang eingeblendet wird und den E-Banking Kunden auffordert, eine Zertifikat auf dem Smartphone zu installieren.

Schweizer Banken fordern ihre Kunden niemals durch Bildschirmeinblendungen oder per SMS dazu auf, neue Sicherheitselemente auf Geräten zu installieren. MELANI empfiehlt allen E-Banking-Kunden, die während der E-Banking Sitzung aufgefordert werden, ein Zertifikat (siehe Bild) oder etwas Ähnliches auf dem Smartphone zu installieren, den E-Banking-Vorgang abzubrechen, die Verbindung zum E-Banking zu schliessen (Logout-Button) und unverzüglich mit der Bank in Kontakt zu treten. Eine ausführliche Beschreibung des Angriffs finden Sie im Anhang 7.1.

3.4 Gezielte Social Engineering-Angriffe gegen Schweizer Firmen

Bei gezielten Betrugsversuchen werden verschiedene Social Engineering-Methoden eingesetzt. Dabei richten sich diese Angriffe immer öfter gegen kleinere und mittlere Unternehmen (KMU).

Zwei Fälle gegen Schweizer Firmen, die MELANI gemeldet worden sind, sollen hier thematisiert werden. Im ersten Fall, der im März 2013 stattfand, erhielt der Finanzchef einer international tätigen KMU eine E-Mail, welche angeblich vom CEO an ihn gesendet worden war. Die E-Mail sah den im Unternehmen üblicherweise verwendeten E-Mails täuschend ähnlich und forderte den Finanzchef auf, für eine angebliche Akquisition in China eine grosse Summe auf das Konto eines Anwalts zu überweisen. Das Vorhaben war natürlich erfunden und das Ganze bloss eine Masche, um an eine Überweisung zu kommen.

An diesem Fall besonders interessant ist der relativ grosse Rechercheaufwand, den die Täter im Vorfeld betreiben mussten. So mussten sich die Betrüger, um überhaupt ein solch unternehmensbezogenes Szenario erstellen zu können, mit der Organisationsstruktur der Firma befassen und diese analysieren.

Im Juni 2013 wurde MELANI ein weiterer Angriff auf ein Schweizer KMU gemeldet. Dabei versuchte eine unbekannte Täterschaft, in das Unternehmensnetzwerk dieser Firma im Kanton Zürich einzudringen. Der Angreifer rief dazu eine Mitarbeiterin des Unternehmens an und verlangte, mit der Buchhaltung über eine offene Rechnung zu sprechen. Da die Mitarbeiterin der Buchhaltung die Rechnung im System nicht finden konnte, bot der Angreifer an, welcher sich in Französisch verständigte, die Rechnung einzuscannen und via E-Mail zu senden. Die Mitarbeiterin gab dem Anrufer ihre E-Mail-Adresse bekannt und erhielt wenige Minuten später, wie telefonisch abgemacht, eine E-Mail mit einem *Hyperlink*. Durch das Anklicken des Hyperlinks erhielt sie jedoch anstelle der erwarteten Rechnung eine ausführbare Windows-Datei mit der Dateiendung «.exe». Durch das Ausführen der Datei installierte sich dabei unbemerkt ein sogenanntes *Remote Administration Tool (RAT)* auf ihrem Computer. Dieses Tool erlaubte es den Angreifern, den Computer unbemerkt über das Internet fernzusteuern.

Glücklicherweise hat die betroffene Mitarbeiterin Verdacht geschöpft und dem firmeninternen IKT-Support die verdächtige E-Mail gemeldet. Dieser konnte die Infektion des Gerätes bestätigen und unschädlich machen. Das betroffene Unternehmen hat daraufhin Strafanzeige gegen unbekannt eingereicht. MELANI geht auch in diesem Fall davon aus, dass die Angreifer finanzielle Absichten hatten.

In den vergangenen Jahren haben solche gezielten Angriffe gegen Schweizer Unternehmen zugenommen. Das Beispiel zeigt, dass nicht nur Grossunternehmen von diesen Angriffen betroffen sind, sondern auch kleine und mittelgrosse Betriebe. Dabei verfolgen die Angreifer unterschiedliche Ziele. Oftmals handeln sie aber aus finanziellen Absichten (z. B. E-Banking-Betrug) oder aus geschäftlichem Interesse (Beschaffen von Informationen über die Konkurrenz, Informationen über den Kundenstamm, Industriespionage).

Solche Angriffe werden oftmals mit Hilfe eines *Remote Administration Tools (RAT)* realisiert. Dabei handelt es sich um Schadsoftware, welche im Internet für ein paar hundert Dollar erworben werden kann und eine breite Auswahl an Funktionalitäten bietet (Aufzeichnen von Tastatureingaben bis hin zur kompletten Fernsteuerung des Computers). Solche RATs sind in der Regel, verglichen mit E-Banking-Trojanern und anderen Schäd-

lingen, technisch nicht allzu ausgeklügelt. Dennoch erkennen viele Antivirenprogramme solche Schadsoftware nicht oder erst, wenn es zu spät ist.

3.5 E-Mails mit Link auf infizierte Seiten im Umlauf

E-Mails, welche den Empfänger dazu verleiten möchten, auf irgendetwas zu klicken, sind weit verbreitet. So hat MELANI bereits im letzten Halbjahresbericht[9] auf E-Mails mit fiktiven Rechnungen oder Transaktionen hingewiesen, die jeweils den Empfänger verleiten sollen, auf den Anhang zu klicken. Im Anhang befindet sich jeweils eine Schadsoftware, meist verpackt in eine *zip-Datei*, die beim Öffnen den Computer infiziert. Ein etwas anderer Versuch wurde am 22. Januar 2013 beobachtet. Eine E-Mail in holländischer Sprache gab an, von einer öffentlichen Stelle des Kantons Aargau zu stammen. Beim Anklicken des Links wurde im Hintergrund versucht, Schwachstellen auf dem Computer zu finden, um eine Schadsoftware zu installieren. Der Kanton Aargau war nicht Opfer eines Hackerangriffs – es wurden lediglich gefälschte E-Mail-Adressen der Domäne „ag.ch“ als Absender benutzt. Es wird oft beobachtet, dass bekannte Firmen oder Stellen als Absender missbraucht werden.


Betreff: Informatie met betrekking tot uw NAT3799 belastingformulier

Houd er rekening mee dat je hebt fouten gemaakt bij het invullen van de laatste NAT3799 aangifte (ID:).
Zie aanbevelingen en tips van onze fiscalisten Door hier te klikken
(Wacht 3 minuten tot rapport zal laden)

Alsjeblieft tot wijziging van de fouten en verzenden de herziene aangifte aan uw lokale belastingkantoor zo snel mogelijk.

Kanton Aargau

Abbildung 5: E-Mail mit Link zu Drive-By-Infektion

Wieso die E-Mail in holländischer Sprache verfasst worden ist, ist unklar. Es ist aber davon auszugehen, dass es sich um einen Fehler der Angreifer gehandelt hat, da dieser Umstand die Erfolgschancen doch erheblich vermindert hat. Ebenso unklar ist, wieso als Absender eine öffentliche Stelle des Kantons Aargau verwendet wurde. Trotzdem muss einmal mehr darauf hingewiesen werden, dass gerade auch bei unerwarteten E-Mails von bekannten Firmen und Behörden immer grösste Vorsicht geboten ist, da die Absender E-Mail-Adressen einfach gefälscht werden können. Die Tatsache, dass im aktuellen Falle bei der Infektion der Computer eine Sicherheitslücke ausgenutzt wurde, zeigt, wie wichtig es ist, neben dem Betriebssystem auch alle Applikationen auf dem neuesten Stand zu halten.

[9] MELANI Halbjahresbericht 2012/2, Kapitel 3.2: http://www.melani.admin.ch/dokumentation/00123/00124/01535/index.html?lang=de (Stand: 31. August 2013).

3.6 VoIP: Missbrauch in der Schweiz

VoIP (Voice-over-IP) ist die Bezeichnung für die Technologie, mit der über IP-Netze telefoniert werden kann, entweder auf einem privaten, kontrollierten Netz oder dem öffentlichen Internet. In den letzten Jahren hat die VoIP-Telefonie und insbesondere diejenige über das öffentliche Internet bei Privatpersonen und Unternehmen stark zugenommen. Einer der Hauptgründe für die zunehmende Beliebtheit ist der günstige Preis vor allem bei internationalen Gesprächen. Doch mit der steigenden Verbreitung dieser Technologie, gibt es auf der anderen Seite auch eine Zunahme an Missbräuchen.

Im ersten Halbjahr 2013 wurde die Melde- und Analysestelle Informationssicherung MELANI über einen Betrug im grossen Stil informiert, bei dem die Infrastruktur eines Schweizer Unternehmens, oder genauer gesagt ein virtueller Server dieser Firma, für einen Betrug bestehend aus Anrufen auf zahlungspflichtige Mehrwertnummer missbraucht wurde (Premiumnummern, *VoIP Toll Fraud*). Der Hacker erhält, als Gegenleistung für dieses sehr einträgliche Geschäft, vom Anbieter der Premiumnummern eine Kommission.

In diesem Fall wurde der virtuelle Server gehackt und für die Durchführung des Betrugs missbraucht. Mit grosser Wahrscheinlichkeit wurden auch die Konten gehackt, die sich auf dem Server befunden haben, und die Kosten für die Anrufe auf diese Mehrwertnummern am Ende dem tatsächlichen Inhaber des jeweiligen Telefonkontos, einer Privatperson oder einem Unternehmen, belastet.

Betrug, der ganz oder teilweise via Telefon erfolgt, benutzt heute weitgehend die VoIP-Technologie. Dies betrifft insbesondere Voice-Phishing, bei dem die Opfer angerufen werden, um ihnen Zugangsdaten zum E-Banking zu entlocken. Auch die Anrufer, die sich als Supporter von Microsoft ausgeben und versuchen, wegen eines angeblichen Sicherheitsproblems Zugang zum PC zu erhalten, machen sich diese Technologie zu Nutze. Somit steht auch die Sicherheit dieser Technologie vermehrt im Fokus. Für die Täter hat die Verwendung einer gehackten Infrastruktur verschiedene Vorteile: In erster Linie können sie damit auf Kosten anderer telefonieren, aber auch ihre Identität besser verschleiern. Neben diesen Betrügereien werden in Kapitel 5.7 noch weitere mögliche Missbräuche von VoIP aufgeführt.

3.7 SMS-Welle mit Vorschussbetrug

Bei E-Mails hat man sich an *Spam* längst gewöhnt. Hier versuchen die Provider, die unerwünschten Nachrichten so gut wie möglich zu filtern und zu entfernen. Dass diese Angriffsart früher oder später auch über den Kanal *SMS* eingesetzt wird, ist nur die logische Konsequenz. Bislang war der SMS-Versand im Vergleich mit dem E-Mail-Versand für die Spammer jedoch zu aufwändig. Dies scheint sich nun zu ändern, wie ein Fall im ersten Halbjahr 2013 gezeigt hat.

Im April 2013 erfasste eine SMS-Spam-Welle auch die Schweiz. Über 500‘000 Swisscom Kunden, aber auch zahlreiche Orange und Sunrise Kunden, waren von dieser Welle betroffen. Die Nachricht wurde anscheinend nach dem Zufallsprinzip an bekannte Nummernbereiche gesendet. Bei der SMS, die im aktuellen Fall versendet worden war, handelte es sich um einen typischen Vorschussbetrug. Die in einer solchen Nachricht gemachten Angebote und Versprechungen - in diesem Fall ein Lotteriegewinn - sind jeweils frei erfunden und sollen lediglich eine mehr oder weniger glaubhafte Kulisse bilden, vor welcher dann der Betrug abgewickelt werden kann. Wird auf eine Nachricht geantwortet, wird unter irgendwelchen Vor-

wänden eine Vorauszahlung verlangt. Das versprochene Geld wird jedoch nie überwiesen. Gleichzeitig können auch bekannt gegebene persönliche Daten (Passnummer, Fotos usw.) als falsche Identität für weitere Betrügereien missbraucht werden.

Abbildung 6: Versendete SMS mit Vorschussbetrug

Die SMS wurden über die britischen Telefonprovider T-Mobile UK und Orange UK versendet, was die Swisscom zu der kurzfristigen Massnahme bewogen hat, SMS von diesen beiden Providern solange nicht mehr durchzuleiten, bis sie diese SMS in ihrem eigenen Netz stoppen, respektive blockieren konnten.

SMS-Spam-Nachrichten sind weniger verbreitet als E-Mail-Spam, welcher je nach Quelle mehr als 70%[10] bis 85%[11] des gesamten E-Mail-Aufkommens ausmacht. Bei SMS-Spam gibt es zudem grosse regionale Unterschiede. In den USA wird die SMS-Technologie wenig genutzt. Deshalb liegt hier die SMS-Spam-Rate unter einem Prozent. In Asien beträgt die Spam-Rate bis zu 30%.[12] SMS-Spam ist im Vergleich zu E-Mail Spam aufwändiger und deshalb für die Spamer noch nicht wirklich interessant. Allerdings wird die Zunahme von Smartphones in Verbindung mit den diesbezüglichen Möglichkeiten, diese Telefone zu hacken, auch die Anzahl des versendeten SMS-Spam beeinflussen.

Die Möglichkeit SMS-Spam zu filtern, ist jedoch noch nicht weit fortgeschritten und funktioniert meist auf Basis von «Schwarzen Listen» im Gegensatz zum Filtern von E-Mails mittels *Spam Score*.

3.8 Fremd gesteuerte Werbemonitore

Eine spezielle Aktion fand im Juni 2013 statt. Bei einer Postfachstelle in Zürich haben sich Jugendliche an einem Werbemonitor zu schaffen gemacht. Die Post vermietet hier einer externen Werbefirma entsprechende Fläche zum Aufstellen von Werbemonitoren. Der Betrieb und Support wird durch die Mieterin (in dem Fall die Werbefirma) wahrgenommen.

Durch Demontage der physischen Sicherheitselemente und neu starten des am Monitor montierten Computers, loggte sich ein 17-jähriger kurzerhand in das System ein. Dort installierte er ein Tool, welches es ihm ermöglichte, von einem anderen Standort aus pornografi-

[10] http://www.spamfighter.com/News-18508-Spam-Increases-to-707-of-Total-E-mail-Traffic.htm (Stand: 31. August 2013).
[11] http://senderbase.org/static/spam#tab=1 (Stand: 31. August 2013).
[12] http://en.wikipedia.org/wiki/Mobile_phone_spam (Stand: 31.August 2013).

sche Inhalte auf den Werbemonitor aufzuschalten. Der 17-jährige wollte mit seiner ungewöhnlichen Aktion auf diese Sicherheitslücke aufmerksam machen. Mit seinem Auftritt in Presse und Fernsehen bewirkte diese Aktion nationale Beachtung.

Neben den rechtlichen Fragen im konkreten Fall, dass das zugänglich machen pornografischen Materials für Minderjährige strafbar ist, wirft dieser Vorfall stellvertretend die Frage auf, was die beste Vorgehensweise ist, wenn man eine Sicherheitslücke findet. Dabei gilt es abzuwägen, inwieweit eine solche Aktion wirklich der Sensibilisierung oder nur der persönlichen Genugtuung dient und ob es in solchen Fällen nicht effizienter wäre, die betroffene Stelle direkt zu informieren.

Immer öfter spielen beim Finden von Sicherheitslücken auch finanzielle Überlegungen eine Rolle. Der Markt im Security Business ist hart umkämpft. So gibt es Firmen, die sich darauf spezialisiert haben, Sicherheitslücken zu suchen und diese auch an die Herstellerfirmen zu verkaufen. Das Finden und Publizieren von Sicherheitslücken wird jedoch auch als Werbegelegenheit genutzt, um auf die Professionalität der eigenen Firma hinzuweisen.

3.9 Swiss Cyber Storm und die Cyber-Talente von morgen

Am 13. Juni 2013 fand im KKL Luzern die Konferenz «Swiss Cyber Storm 4» statt. Ein breites Feld von internationalen Referenten mit hervorragendem Fachwissen richtete sich bei ihren Ausführungen primär an Entscheidungsträger der Schweizer Wirtschaft.

Daneben galt es jedoch auch, die besten Schweizer Cyber Talente zu suchen. In den Wochen vor dem ganztägigen Kongress hatten Studierende und Schüler die Gelegenheit, online an so genannten «Challenges» teilzunehmen. Dabei galt es, Cyber-Rätsel oder -Knacknüsse zu lösen. Gesucht waren aber nicht etwa Hacker, sondern Talente, die weiter und globaler denken als Hacker. Konkret hiess das: Es reichte nicht aus, verschlüsselte zip-Files knacken zu können. Vielmehr mussten die Kandidatinnen und Kandidaten auch aufzeigen, aufgrund welchen Fehlers in der Verschlüsselung sie die Files knackten - und wie sie diesen Fehler beheben würden. Hierbei ging es also nicht nur um das Angreifen, sondern es galt ebenfalls aufzuzeigen, wie die eigenen Systeme geschützt werden sollten.

Die Anforderungen an die Teilnehmenden waren sehr vielfältig. Nebst der technischen Herausforderung galt es beispielsweise auch, diese in einer gesetzten Frist zu lösen, was den Druck auf die Teilnehmenden nochmals erhöhte. Gefragt war somit die Fähigkeit, nicht nur in den vorgegebenen Pfaden zu denken, sondern flexibel zu reagieren und lösungs- und teamorientiert zu arbeiten

Für sämtliche Teilnehmenden war der Swiss Cyber Storm ein Gewinn: Sie konnten ihr Wissen erweitern und wichtige Kontakte zur Privatwirtschaft knüpfen. So hat beispielsweise einer der Teilnehmenden bereits ein Jobangebot erhalten.

Was folgt nach dem Swiss Cyber Storm?

Die Gewinnergruppe kann sich nicht auf den Lorbeeren ausruhen. Sie wurden von den Organisatoren der Swiss Cyber Strom eingeladen, im November 2013 gegen das Siegerteam der österreichischen Schwesterkonferenz in Linz den Finalwettkampf zu bestreiten.[13]

MELANI hat zusammen mit Swiss Police ICT - einem privaten Verein, der mit dem Schweizer Polizei Informatik Kongress seit Jahren die Brücke zwischen Informatik und Strafverfolgung schlägt – das Patronat des Swiss Cyber Storm übernommen. Das gemeinsame Ziel ist, auch in Zukunft neue Schweizer Cyber Talente zu finden.

4 Aktuelle Lage IKT-Infrastruktur international

4.1 Kommunikationsüberwachung im Internet

Besonders ein Thema machte im letzten halben Jahr Schlagzeilen: Die mutmasslichen Abhörmethoden einzelner Nachrichtendienste, die durch den Informanten Edward Snowden publik gemacht wurden. Begonnen haben die Enthüllungen mit dem NSA-Abhörprogramm Prism. Danach folgte die Veröffentlichung über die Möglichkeiten des Britischen Government Communications Headquarters (GCHQ), transatlantische Tiefseekabel zu überwachen und anschliessend die Publikation einer Präsentation des Analyse-Programms XKeyscore. Snowden war bei der CIA angestellt, bevor er zum privaten Sicherheitsdienstleister Booz Allen Hamilton wechselte, der unter anderem auch für die NSA Aufträge erfüllt.[14] Im Zuge dieser Enthüllungen wurden auch in diversen anderen Ländern Überwachungsprogramme thematisiert.

Prism

Prism heisst ein angebliches Abhörprogramm der NSA, welches durch Edward Snowden publik gemacht worden ist. Der Name kommt daher, dass Signale in Glasfaserkabeln mittels einem Prisma aufgetrennt und ausgeleitet werden können. Es ist allerdings fraglich, ob die Daten wirklich auf diese Weise erhoben werden. Vielmehr dürfte es sich bei diesem Abhörprogramm um ein Projekt handeln, durch welches die NSA Zugang zu den Servern von verschiedenen US-Firmen wie beispielsweise Microsoft, Google oder Yahoo erhalten.

Die Tatsache, dass staatliche Stellen Zugriff auf die inländische Telekommunikationsinfrastruktur haben, ist nichts Aussergewöhnliches. Allerdings sind solche Zugriffe in der Regel strikt reglementiert: Um an solche Daten zu gelangen, bedarf es typischerweise eines Strafverfahrens und eines richterlichen Beschlusses oder besonderer Gründe, welche spezialgesetzlich vorgesehen sind. Neu an den veröffentlichten Informationen ist, dass die US-Nachrichtendienste nicht nur punktuellen Zugriff, sondern anscheinend systematisch und flächendeckend Zugang zu diese Daten haben sollen. Sämtliche betroffenen Firmen haben

[13] http://www.verbotengut.at/ (Stand: 31.August 2013).

[14] Dieser Bericht umfasst die Berichtsperiode Januar-Juni 2013. Die weiteren Informationen, die durch den Informanten Edward Snowden publik gemacht wurden, werden im nächsten Halbjahresbericht thematisiert.

eine solche umfassende Zusammenarbeit bestritten und darauf hingewiesen, dass Daten nur nach Gerichtsbeschlüssen zu spezifischen Konten herausgegeben werden.

Von staatlicher Stelle wurde stets bekräftigt, dass alle getroffenen Abhörmassnahmen gesetzlich legitimiert und von den drei Staatsgewalten der USA genehmigt seien. Der 1978 erlassene «Foreign Intelligence Surveillance Act (FISA)» regelt die Überwachung im Ausland, von ausländischen Personen auf US-Territorium sowie von US-Bürgern. Das Foreign Intelligence Surveillance Court (FISC) genehmigt als richterliche Behörde entsprechende Überwachungsmassnahmen. Änderungen am FISA durch Erlasse mit Namen wie «Patriot Act» (2001) oder «Protect America Act» (2007) räumten den Behörden weitgehende Kompetenzen bei der Kommunikationsüberwachung ein, welche auf die veränderte Bedrohungslage - insbesondere Terrorismus - und die technischen Entwicklungen wie das Internet als Medium und die Verlagerung der internationalen Kommunikation von Satellit auf Glasfaserkabel, angepasst sind.

Tempora

Ein weiterer Bericht, der von Snowden der Britischen Zeitung «The Guardian» zugespielt worden ist, handelt von einem Abhörprogramm mit dem Namen Tempora, welches durch den britischen Nachrichtendienst betrieben werden soll. Im Rahmen dieses Programms soll das Britische Government Communications Headquarter (GCHQ) Zugang zu transatlantischen Datenverbindungen haben und dadurch die gewünschten Daten ausleiten und so kopieren. Im Fokus der Berichterstattung stand dabei die Leitung TAT-14, die von Deutschland, Dänemark, den Niederlanden und Frankreich via Grossbritannien nach New Jersey führt. In der Hafenstadt Bude, dem Durchleitungspunkt dieses Kabels in Grossbritannien, soll das GCHQ Zugriff auf diese Leitung haben. Zu den abgegriffenen Daten sollen E-Mails, Facebook-Einträge aber auch Telefongespräche gehören. Der GCHQ soll dabei über 200 Glasfaserverbindungen anzapfen und für die Analyse 500 Mitarbeitenden einsetzen.[15]

Der transatlantische Internetverkehr hat sich in den letzten Jahren immer stärker auf Tiefseeglasfaserkabel verlagert. Während 1986 bis zu 80% des transatlantischen Datenverkehrs via Satellit abgewickelt worden ist, geht heute sowohl kontinental als auch interkontinental der grösste Teil durch Glasfaserleitungen, die zu einem Netz verbunden sind. Für die Kommunikation zwischen zwei Nutzern existieren meist mehrere mögliche Wege und erst bei der tatsächlichen Datenübertragung entscheidet sich, welcher benutzt wird. Wird der Datenverkehr auf einem Tiefseekabel abgehört, heisst dies nicht zwangsläufig, dass die gesamte Kommunikation, sprich eine ganze E-Mail abgefangen werden kann, obschon dies in der Praxis wohl häufig der Fall ist.

XKeyscore

XKeyscore ist eine Analysesoftware, die von der NSA entwickelt wurde und bei verschiedenen Nachrichtendiensten eingesetzt werden soll. Sie soll ermöglichen, dass eine Vielzahl von Daten wie E-Mails, Online-Chats usw. in verschiedenen Datenbanken in Echtzeit einer Zielperson zugeordnet werden können. Dabei lassen sich verschiedenste Kriterien, wie beispielsweise *IP-Adresse*, Sprache, Browser, Einstellungen und Telefonnummern abfragen. Es soll so möglich sein, alle in diesem Zusammenhang erfassten Daten zu finden. Laut der von

[15] http://www.handelsblatt.com/politik/international/abhoerskandal-auch-britischer-geheimdienst-spaeht-daten-aus/8391120.html (Stand: 31. August 2013).

Snowden veröffentlichten geheimen Präsentation aus dem Jahre 2008 besteht das XKeyscore Netzwerk aus mehr als 700 Datenservern verteilt auf 150 Standorte auf der ganzen Welt. Die Auslandsnachrichtendienste von UK, Kanada, Australien und Neuseeland sollen auch an XKeyscore beteiligt sein. Auch der deutsche Bundesnachrichtendienst (BND) soll das Programm einsetzen.[16]

Dass Nachrichtendienste über geeignete Werkzeuge verfügen, welche ein effizientes Auswerten von bereits gesammelten Daten ermöglichen, ist keine Überraschung. Die Analyse eines grossen Datenaufkommens kann heute nur noch mit entsprechenden Analyseprogrammen durchgeführt werden. Alle kennen diese Funktionsweise von den diversen Suchmaschinen: Auch hier ist es entscheidend, in Sekundenbruchteilen die gewünschten Resultate zu erhalten. Abgesehen von der Frage, wer zu welchem Zeitpunkt auf welche Daten eines solchen Systems Zugriff hat, sollte sich die Frage nicht darauf konzentrieren, wie ein Nachrichtendienst Daten analysiert, sondern vielmehr darauf, welche Daten ein Nachrichtendienst überhaupt erheben und speichern darf, respektive welche Abfragen innerhalb dieser Daten tatsächlich zulässig sind.

4.2 Advanced Persistent Threat: Red October, Net Traveller, MiniDuke

Im ersten Halbjahr 2013 sind wiederum einige gezielte und professionelle Angriffe auf Unternehmen oder staatliche Stellen bekannt geworden. Es handelte sich bei diesen Angriffen meist um so genannte *Advanced Persistent Threats (APT)*. Bei APT bezeichnend ist, dass die Angreifer hartnäckig und auf unterschiedlichste Art versuchen, in bestimmte Systeme zu gelangen, um sich dort auf Dauer einzunisten und unbemerkt ihre schädlichen Aktivitäten zu entfalten. Oft erfolgt die ursprüngliche Infektion über *Spear-Phishing*- oder *Watering-Hole-Attacken*. Anschliessend werden Hintertüren (Backdoors) eingerichtet und Administratorenrechte erschlichen. Das Endziel ist, über längere Zeit unbemerkt im Netzwerk zu bleiben, sich dort unbemerkt zu bewegen, Daten auszuspähen und teilweise auch zu verändern oder zu löschen. Um solche Attacken erfolgreich durchzuführen, ist ein erheblicher Aufwand nötig, weshalb oft staatliche Akteure dahinter vermutet werden. Aber auch kriminelle Gruppierungen oder Einzelpersonen mit viel Zeit, hoher Motivation und Aussichten auf einen Verkauf der gesammelten Daten an Dritte, sind als Täterschaft nicht auszuschliessen.

Die IKT-Sicherheitsfirma FireEye schätzt in einem Bericht, dass Firmen, respektive Organisationen alle drei Minuten eine E-Mail mit einem schädlichen Link oder Anhang erhalten.[17] Auch in der Schweiz sind Systeme mit sensiblen Informationen solchen Angriffen tagtäglich ausgesetzt.

Im ersten Halbjahr 2013 jagte eine Meldung über Angriffe dieser Art die andere. Da meist staatliche Akteure hinter den Angriffen vermutet wurden, hatten diese Attacken auch zahlreiche politische Stellungnahmen zur Folge.

---

16 http://www.zeit.de/politik/deutschland/2013-08/bnd-xkeyscore-nsa (Stand: 31. August 2013).

17 http://www2.fireeye.com/WEB2012ATR2H_advanced-threat-report-2h2012.html (Stand: 31. August 2013).

Januar: Operation Red October

Am 14. Januar 2013 gab die russische IKT-Sicherheitsfirma Kaspersky Einzelheiten über eine Spionageoperation gegen diplomatische Missionen, Regierungen und internationale Organisationen bekannt. Die Ziele der Operation namens Red October lagen vor allem in Osteuropa, Zentralasien und den GUS-Staaten. Im Bericht von Kaspersky wurde auch erwähnt, dass von zahlreichen Schweizer IP-Adressen auf die *Kommando- und Kontrollserver Infrastruktur* zugegriffen wurde, was im ersten Moment auf viele Betroffene in der Schweiz hindeutete. MELANI stellte bei einer ersten Analyse fest, dass es sich mehrheitlich um dynamische IP-Adressen handelte. Die Zahl der effektiven Infektionen konnte nach Eliminierung der mehrfach gezählten Verdachtsfälle deutlich nach unten auf fünf Opfer korrigiert werden. Ausserdem handelte es sich bei den Betroffenen nicht um schweizerische Organisationen, sondern um ausländische Infrastrukturen, die in der Schweiz betrieben werden.

Die Opfer wurden durch Schadsoftware in E-Mail-Anhängen infiziert. Eine Besonderheit dieser Angriffe bestand darin, dass die Schadsoftware nicht nur Daten von infizierten Computern, sondern auch Daten von mobilen Geräten beschaffen konnte. Diese Spionageoperation soll schon seit 2007 oder noch länger aktiv gewesen sein. Laut Kaspersky soll die Täterschaft russischsprachiger Herkunft sein.

Februar: APT1

Zu Beginn dieses Jahres nahmen besonders auf US-Firmen abzielende Attacken zu. Diese Angriffsserie führte zu zahlreichen Stellungnahmen hochrangiger US-Politiker, die für eine Stärkung der Abwehr plädierten und häufig China als das Land bezichtigten, von dem die grösste Gefahr im Bereich Cyberspionage ausgehe.

Trotz der Vielfalt der Angriffe und Ziele lassen sich gewisse Muster erkennen. So hatten diese vor allem grosse amerikanische Internetunternehmen wie Apple, Facebook, Google, Microsoft und Twitter im Visier. Infiziert wurden die Systeme hauptsächlich über *Watering-Hole-Attacken* und zwar über eine Website für Entwickler mobiler Anwendungen. Die Besucher dieser Site wurden über einen *Zero-Day-Exploit* im Programm *Java* infiziert. Parallel dazu meldeten auch viele grosse amerikanische Medien (New York Times, Wall Street Journal, Bloomberg, Washington Post) Angriffe insbesondere auf E-Mail-Konten ihrer Journalisten. In beiden Fällen wurde die Urheberschaft mehrfach in China vermutet.

Vor diesem Hintergrund erfolgte die Veröffentlichung eines Berichts des amerikanischen Sicherheitsunternehmens Mandiant im Februar 2013, der beansprucht, die Beteiligung des chinesischen Staates bei Cyberspionage-Operationen gegen die USA und einige europäische Länder aufzeigen zu können. Er basiert auf Recherchen in Zusammenarbeit mit den Opferfirmen. Als wichtigste Schlussfolgerung stellt der Bericht eine Verbindung zwischen einer Gruppe von Cybertätern, welche «APT1» genannt wird, und einer Einheit der chinesischen Armee her. Mandiant behauptet, die Gruppe habe seit 2006 bei 146 ausgesuchten Opfern jahrelang eine Vielzahl von Daten entwendet.

Auch in diesem Fall war die Schweiz nur indirekt betroffen, da es sich bei den betroffenen Systemen um ausländische Infrastrukturen handelt, die in der Schweiz betrieben werden.

Februar: Operation Beebus

Im gleichen politischen Kontext hat auch die amerikanische Firma FireEye im Februar 2013 die Ergebnisse ihrer Arbeit über eine weitere Spionageaffäre, eine APT namens Beebus, veröffentlicht. Diese schien besonders Unternehmen im Bereich Verteidigung und Raumfahrt im Visier zu haben. Die Opfer wurden dabei sowohl über gezielte E-Mails als auch per *Drive-by*-Download-Methode infiziert. Die ersten Spuren des Angriffs gehen laut FireEye auf 2011 zurück. FireEye vermutet, der Angriff könnte chinesischen Ursprungs sein. Es sind keine Ziele in der Schweiz bekannt.

Februar: MiniDuke

Ebenfalls im Februar 2013 hat Kaspersky über einen raffinierten Angriff mit der Schadsoftware MiniDuke berichtet. Diese scheint es vor allem auf staatliche Strukturen und einige andere Ziele abgesehen zu haben, die sich ausschliesslich in Europa befinden. Infiziert wurden die Opfer mittels *Spear-Phishing* und präparierten PDF-Dokumenten. Ein besonderes Merkmal dieser Attacke ist die Verwendung von Twitterkonten als Generator *der Domainnamen* der *Kommando- und Kontrollserver*. Nach aktuellen Erkenntnissen gibt es keine betroffene Infrastruktur in der Schweiz.

Juni: NetTraveler

Anfang Juni 2013 veröffentlichte Kaspersky Einzelheiten zu NetTraveler, einer Reihe von Schadprogrammen, die bei APT-Angriffen verwendet wurden. 350 Opfer in 40 Ländern sind betroffen, allerdings gibt es auch hier nach jetzigem Kenntnisstand keine Verbindungen zu Schweizer Infrastrukturen. Die Ziele waren im Bereich Industrie, Energie, Kommunikation, neue Technologien und Regierung. Interessant ist, dass laut Kaspersky sechs Ziele gleichzeitig von NetTraveler und Red October betroffen waren. Aus dieser Feststellung allein lässt sich aber weder schliessen, dass die beiden Attacken auf die gleiche, noch dass sie auf unterschiedliche Urheberschaft zurückzuführen sind.

Die vielen Berichte von Sicherheitsfirmen, Opfern oder Behörden haben Cyberspionage- und APT-Angriffe erneut ins Rampenlicht gerückt. Bei gezielten Spionageangriffen handelt es sich aber längst nicht mehr um Einzelereignisse oder einzelne Spionagekomplexe. Vielmehr besteht ein ständiges Interesse und demzufolge ein ständiger Druck auf sensible Daten. Davon ist auch die Schweiz betroffen, da gerade hier sehr viele Spitzenunternehmen ansässig sind, die über Knowhow oder Informationen mit grossem Wert verfügen. Neben den gängigen und nötigen technischen Sicherheitsmassnahmen sind aber auch organisatorische Massnahmen notwendig. Zudem muss Prävention grundsätzlich und unabhängig von den neusten Vorfällen immer eine hohe Priorität haben und beispielsweise über eine Sensibilisierung der Mitarbeiterinnen und Mitarbeiter erfolgen, die unter Anderem im sorgsamen Umgang mit E-Mails geschult werden müssen.

Die Angriffe sind selten einer bestimmten Täterschaft zuzuordnen. Geografisch können sie zwar teilweise ziemlich genau lokalisiert werden. Dass der entsprechende Staat für die Angriffe verantwortlich ist, ist aber in den seltensten Fällen zweifelsfrei nachweisbar.

Interessant ist zudem, dass in einigen dieser Angriffe Infrastrukturen eingesetzt wurden, die auch im Zusammenhang mit kriminellen Vorgängen bekannt sind. Offensichtlich scheinen kriminelle Infrastrukturen nicht nur zur monetären Bereicherung eingesetzt zu werden, sondern sie agieren auch im Interesse und Sold einzelner Staaten und deren Spionageabsichten.

4.3 Korea-Konflikt im Cyberraum

Im ersten Halbjahr 2013 verschärfte sich der Konflikt in Korea. Nach Hinweisen auf Kernwaffentests von Nordkorea[18] und der darauffolgenden Verschärfung der UNO-Sanktionen gegen Nordkorea, verkündete Nordkorea, sich nun mit Südkorea im Kriegszustand zu befinden und drohte den USA erstmals mit einem nuklearen Präventivschlag. Dieser Konfliktherd hatte auch diverse Cyberkomponenten. So berichtete die amtliche nordkoreanische Nachrichtenagentur KCNA am 14. März 2013 von einem lokalen Ausfall des Internets infolge eines feindlichen Computerangriffs. Die USA und Südkorea wurden von Nordkorea beschuldigt, diesen Ausfall verursacht zu haben. Was genau dahintersteckte, konnte nicht eruiert werden. In Nordkorea hat nur ein kleiner Teil der Bevölkerung Zugang zum Internet. Wenige Tage später, nämlich am 20. März 2013, erfolgte dann ein massiver Cyberangriff gegen Südkorea, bei dem drei südkoreanische Fernsehstationen und zwei Finanzinstitute betroffen waren. Die Betroffenen konnten ihre Computer nicht mehr starten, da die Festplatten durch die Schadsoftware gelöscht wurde. Während Geldautomaten, *Points of Sale* und das *Mobile Banking* der betroffenen Banken zum Teil ausfielen, war das Fernsehprogramm der betroffenen Sender nicht eingeschränkt. Zudem wurden Webseitenverunstaltungen durch eine Gruppe mit Namen «Whois Team» festgestellt, die über diesen Weg bekannt gab, dass dies erst der Beginn ihrer Aktionen sei. «Die Daten seien in ihren Händen, aber auf den betroffenen Computern gelöscht.» Auch eine Gruppe mit dem Namen «New Romanic Cyber Army» hatte sich zu diesem Angriff bekannt und behauptet die gesammelten Informationen von Banken und Medienunternehmen weitergegeben zu haben. McAfee publizierte in einem Bericht, dass es bei dieser Attacke Verbindungen zu einer bislang unbekannten Spionageaktion gegen das Südkoreanische Militär gebe, welche seit 2009 aktiv gewesen sein soll. Bei dieser Spionageaktion mit dem Namen «Operation Troy» wurden Computer auf gewisse Stichworte aus dem Bereich Militär durchsucht. [19] Die Hacktivismus-Aktionen könnten somit auch als Ablenkungsmanöver für diese Spionageaktion gedient haben.

Am 25. Juni 2013, dem 63. Jahrestag des Beginns des Koreakrieges, erfolgte ein weiterer Angriff – diesmal in Form einer DDoS-Attacke gegen *DNS-Server* der südkoreanischen Regierung. Amtliche Websites, darunter auch die Website des Präsidialamts, waren in der Folge nicht mehr erreichbar. Vertreter der Bewegung Anonymous, welche auf verschiedenen Seiten als Urheberin genannt wurde, distanzierten sich von den Angriffen. Von südkoreanischer Seite wurde Nordkorea beschuldigt, sowohl für die Angriffe im März als auch für diejenigen im Juni verantwortlich zu sein. Dabei wurden Nordkoreanische IP-Adressen und Schadsoftwaremuster als mögliche Beweise vorgelegt.[20]

Symantec hat nach diesem letzten Angriff ebenfalls einen Bericht[21] veröffentlicht, dass es eindeutige Hinweise dafür gebe, dass eine dieser *DDoS-Attacken* vom 25. Juni 2013 mit den

---

[18] http://www.seismologie.bgr.de/sdac/erdbeben/kernexplosion/nkorea_20130212_deu.html (Stand: 31. August 2013).

[19] http://blogs.mcafee.com/mcafee-labs/dissecting-operation-troy-cyberespionage-in-south-korea (Stand: 31. August 2013).

[20] http://www.csoonline.com/article/736531/south-korea-blames-north-korea-for-cyberattacks (Stand: 31. August 2013).

[21] http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war (Stand: 31. August 2013).

verschiedenen Angriffen der letzten vier Jahre gegen Südkorea, also auch den Angriffen vom Juli 2009 und März 2011[22] zusammenhänge und der Gruppe «DarkSeoul» zugeordnet werden könne. Symantec vermutete dahinter eine Gruppe mit 10-50 Personen, welche laut diesem Bericht auch mit der E-Banking-*Malware* Castov in Zusammenhang gebracht wird. Die Gruppe sei auch schon mit Angriffen gegen die USA aufgefallen. Den Ursprung der Angriffe zu eruieren und diesen dann einem möglicherweise staatlichen Akteur zuzuordnen, ist erfahrungsgemäss sehr schwierig.

4.4 Twitter Account von Associated Press gehackt

Das soziale Netzwerk Twitter ist im ersten Halbjahr 2013 vermehrt in das Visier von Angreifern geraten. Der schwerwiegendste Fall passierte am 23. April 2013, als das Twitter-Konto der Associated Press (AP) kompromittiert wurde. Hacker hatten sich Zugang zum Twitter-Konto der Nachrichtenagentur AP verschafft und in deren Namen einen Tweet veröffentlicht, dass es zwei Explosionen im Weissen Haus gegeben habe und Präsident Obama verletzt sei. Fast 2 Millionen Benutzer folgen diesem Tweet. Die US-Märkte wurden dadurch kurzzeitig beeinflusst. Innerhalb von drei Minuten verlor der amerikanische S&P-Index vorübergehend 136.5 Milliarden Dollar an Wert, dieser erholte sich aber kurz darauf wieder. Ebenfalls wurden Twitter-Konten von BBC, CBS, France 24 TV, Al Jazeera und vom National Public Radio (NPR) gehackt. Die britische Zeitung «The Guardian» war am 29. April 2013 von einem Angriff dieser Art betroffen. Dabei wurden anti-israelische Parolen und Texte wie «Long Live Syria» oder the «Syrian Electronic Army was here» verbreitet. Ebenfalls zu den Opfern gehörten die FIFA und ihr Präsident Joseph Blatter. Über dessen Konto wurde die Falschmeldung verbreitet, dass Blatter wegen Korruptionsvorwürfen von seinem Posten zurücktritt, weil er für die Vergabe der WM 2022 Geld vom Emir von Katar angenommen habe.

Hinter den Angriffen soll die Gruppe «Syrian Electronic Army (SEA) » stehen, die für «Chaos und Peinlichkeiten» sorgen will. Klar dürfte sein, dass sich die SEA damit eine höhere Bekanntheit verschaffen wollte. Die SEA beschuldigte ihrerseits westliche Medien «Lügen und üble Nachrede über Syrien» zu verbreiten.

Die Methode ist immer dieselbe: Von den Angreifern werden glaubwürdige E-Mails mit einem Link zu einer infizierten Seite an die Twitter-Kontoinhaber/innen gesendet. Die so installierte Schadsoftware greift den Benutzernamen und das Passwort ab, mit denen sich der Angreifer anschliessend in das Konto einloggen und Nachrichten verbreiten kann.

Der Einfluss der Sozialen Medien auf die Informationsverbreitung wächst stetig. Der Konkurrenzkampf zwischen den Medien führt zudem dazu, dass immer weniger Zeit für die Verifikation einer Meldung bleibt, insbesondere dann, wenn die Meldung von einer renommierten Quelle zu stammen scheint. Dabei geht leicht vergessen, dass Twitter-Konten nur durch Login und Passwort geschützt sind. Es genügt ein gezielter Angriff via die gängigen *Phishing*- oder *Malware*-Methoden, um an die Passwörter zu gelangen. Twitter hat deshalb eine Warnung an die Medienbranche versendet, dass man davon ausgehe, dass solche Angriffe andauern würden und besonders gegen angesehene und populäre Medien gerichtet seien. Um das Risiko einer Malware Infektion klein zu halten, empfiehlt Twitter neben den üblichen

[22] MELANI Halbjahresbericht 2009/2, Kapitel 4.2: http://www.melani.admin.ch/dokumentation/00123/00124/01109/index.html?lang=de (Stand: 31. August 2013).

Massnahmen, einen separaten Computer zu verwenden um die Tweets abzusetzen. Zudem soll Twitter auch technische Massnahmen in Erwägung ziehen und an der Einführung einer *Zwei-Faktor Authentisierung* arbeiten, wie sie beispielsweise im E-Banking implementiert ist.[23]

Falschmeldungen über Twitter sind auch möglich, wenn kein Konto kompromittiert wurde, wie das Beispiel von Andrea Caroni im November 2011 gezeigt hat. Obschon Nationalrat Caroni kein Twitter-Konto hatte, wurde mit einem gefälschten Konto in seinem Namen die Wiederwahl der Bundesrätin Eveline Widmer-Schlumpf bestätigt, noch bevor das offizielle Ergebnis bekannt war.[24]

Neben all den technischen Massnahmen sollte im Vorfeld ebenfalls überlegt und definiert werden, wie und über welche Kanäle eine Falschmeldung möglichst effizient dementiert, respektive richtiggestellt werden kann, um damit grössere Verwirrung und andere Auswirkungen zu verhindern.

4.5 SCADA-Systeme und Industriesteuerungen: Offene Zugänge, Sicherheitslücken, Angriffe und Schutz

Kontroll- oder Steuerungssysteme bestehen aus einem oder mehreren Geräten, welche das Verhalten von anderen Geräten oder Systemen steuern, regeln und/oder überwachen. In der industriellen Produktion ist der Begriff «Industrielle Kontrollsysteme» (engl. Industrial Control Systems, ICS) geläufig. Industrielle Kontroll- und Steuerungssysteme finden seit einiger Zeit vermehrt auch ausserhalb der produzierenden Industrie Anwendung, zum Beispiel bei der Hausautomation oder der Verkehrsregelung. Im Prinzip kann man bei jedem System, welches einen physischen Prozess regelt und/oder überwacht von einem Industriellen Kontrollsystem sprechen. Die meisten Grundregeln für den Schutz solcher Systeme finden auch ausserhalb der industriellen Produktion Anwendung.

Serial-Port Server offen am Internet

Serial-Port Server bieten den Übergang von einem Telekommunikationsnetzwerk zu seriellen *Schnittstellen* von Geräten an. Untersuchungen des Sicherheitsforschers HD Moore[25] zeigten auf, dass von über 100‘000 solcher Server auf rund 10% relativ ungehindert in der einen oder anderen Form via Internet zugegriffen werden konnte. Darunter befanden sich diverse Anlagen – von ICS für Kesselanlagen in einer Brauerei über Unternehmens-*VPN*-Server zu *Smart-Metern* bis Verkehrsampelsteuerungen – deren offene Zugänge erhebliches Missbrauchspotenzial bieten.

---

[23] http://www.zdnet.de/88155870/twitter-fuhrt-zwei-faktor-authentifizierung-ein/?ModPagespeed=noscript (Stand: 31. August 2013).

[24] MELANI Halbjahresbericht 2011/2, Kapitel 3.6: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=de (Stand: 31. August 2013).

[25] https://community.rapid7.com/community/metasploit/blog/2013/04/23/serial-offenders-widespread-flaws-in-serial-port-servers (Stand: 31. August 2013).

Viele Geräte, welche über eine serielle Schnittstelle angesteuert werden können, benötigen keine weitere Authentifizierung, da sie bei physischer Verbindung via serieller Schnittstelle (die bis anhin lokal erfolgte) annehmen, dass der Verbundene gleichermassen zu Zugriff wie auch Konfiguration des Geräts berechtigt ist. Diesem Umstand ist bei der Nachrüstung von Fernzugriffen Rechnung zu tragen. Fernzugriffe müssen immer vor Missbrauch geschützt werden. Dazu können VPN-Tunnels und/oder Einschränkungen des Zugriffs auf wenige, bekannte IP-Adressen verwendet werden. Darüber hinaus muss darauf geachtet werden, dass der Zugriff verschlüsselt erfolgt und nur starke Passwörter oder eine *2-Faktor-Authentifizierung* zum Einsatz kommen.

Sicherheitslücke in Steuerungsmodulen: Passwörter auslesbar

Das Mikro-Blockheizkraftwerk «ecoPower 1.0» ist ein Strom- und Wärmesystem mit Gas-Verbrennungsmotor für die private Nutzung des Konzerns Valliant. Die Heizung produziert ebenfalls Strom, welcher selbst genutzt oder ins öffentliche Netz eingespiesen werden kann. Die Anlage wird über den eingebauten Touchscreen, eine iPad-*App* oder über ein *Webinterface* gesteuert. Bei der Implementierung der Fernsteuerung über das Internet sind jedoch verschiedene Sicherheitsmechanismen nicht optimal konzipiert oder überhaupt weggelassen worden. So können durch eine Sicherheitslücke sämtliche Passwörter abgefragt werden. Neben dem Konfigurationspasswort des Besitzers sind dies auch die Passwörter für den Fernwartungsservice und sogar für Systementwickler – alle wurden vom System im Klartext ausgegeben. Dies ermöglichte unbefugten Dritten, auf das Mikro-Kraftwerk zuzugreifen, Daten über dessen Besitzer auszulesen und Betriebseinstellungen zu verändern. Nachdem ein Betreiber eines solchen Geräts sich bei Sicherheitsexperten[26] gemeldet hatte und diese die Probleme untersuchten, wurde die Herstellerin über die Ergebnisse informiert. Diese empfahl in der Folge allen betroffenen Kunden brieflich, die Heizungen durch Ziehen des Netzwerkkabels vom Internet zu trennen, bis Lösungen erarbeitet seien und ein Servicetechniker die Probleme vor Ort beheben werde.

Obschon sich Valliant den Vorwurf gefallen lassen muss, dass ihre Produkte entgegen aller Sicherheitsempfehlungen direkt – und nicht via verschlüsseltem *VPN*-Tunnel – ans Internet angeschlossen wurden, sollte sich insbesondere Saia-Burgess, die Schweizer Herstellerin der Steuerungsmodule, dem Problem annehmen, da sie für die Speicherung der Passwörter im Klartext und das Sicherheitsleck, über welche diese ausgelesen werden können, verantwortlich zeichnet. Diese Steuerungsmodule werden nämlich nicht nur von Valliant für ihre Heizungen, sondern in diversen, zum Teil grossen und bedeutsamen Anlagen verwendet.

Sowohl Valliant wie auch Saia-Burgess sind dabei[27], die Lücken zu schliessen und haben entsprechende Updates veröffentlicht[28]. Vaillant hat zudem eine Hotline für betroffene Kunden eingerichtet und installiert bei betroffenen Kunden Updates und eine *VPN*-Box für einen sicheren Zugang. Bis die entsprechenden Updates und zusätzlichen Sicherheitsmassnahmen jedoch bei allen betroffenen Systemen implementiert sind, braucht es einige Anstrengungen.

---

[26] http://www.bhkw-infothek.de/nachrichten/18555/2013-04-15-kritische-sicherheitslucke-ermoglicht-fremdzugriff-auf-systemregler-des-vaillant-ecopower-1-0/; http://heise.de/-1840919 (Stand: 31. August 2013).

[27] http://www.heise.de/newsticker/meldung/Kritisches-Sicherheitsupdate-fuer-200-000-Industriesteuerungen-1934787.html (Stand: 31. August 2013).

[28] Firmware Update von Saia: http://www.sbc-support.com/de/product-index/firmware-for-pcd-cosinus.html (Stand: 31. August 2013).

Dieser Fall zeigt exemplarisch die Problematik auf, welche eine zunehmend (nur mehr durch ein einziges Netz) vernetzte Gesellschaft bei ihrer Entwicklung berücksichtigen muss. Der Fernzugriff auf ein Gerät bietet sowohl dem Besitzer bei der Bedienung als auch dem Servicetechniker beim Unterhalt neue Möglichkeiten und bedeutende Vorteile, birgt jedoch auch neue Angriffsflächen und entsprechende Risiken. Deshalb ist es wichtig, dass alle in der Lieferkette eines Produkts beteiligten Unternehmen nicht nur die Benutzerfreundlichkeit von neuen Geräten kritisch begutachten, sondern auch Sicherheitsanforderungen stellen, damit diese bereits in den Entwicklungsprozess Eingang finden: Sicherheit ist eine gemeinsame Aufgabe! Zwar empfiehlt der Hersteller des Steuerungsmoduls (spätestens seit dem beschriebenen Vorfall sehr deutlich und mit Nachdruck), seine Geräte nicht direkt ans Internet anzuschliessen – dies entbindet ihn aber nicht von der Pflicht, sein Produkt gemäss Sicherheitsvorgaben zu bauen und gegebenenfalls auch Sicherheitsupdates in nützlicher Frist nachzuliefern.

ICS wurden schon vor dem Internetzeitalter teilweise an das Fernmeldenetz angeschlossen – meist via eigene Telefonleitung. Über diesen Anschluss konnte sich in der Regel nur der Hersteller/Lieferant bei Bedarf zu Diagnose- und Servicezwecken mit der Anlage verbinden, um sich nicht vor Ort begeben zu müssen. Wird für solche Zugänge nun das Internet verwendet, müssen dessen Eigenheiten berücksichtigt werden. Das Risiko, dass jemand die Telefonnummer einer Anlage in Erfahrung bringen, ein allfälliges Passwort knacken und schliesslich auch noch das typischerweise proprietäre Protokoll der Steuerung verstehen würde, ist wohl geringer einzustufen, als dass jemand via spezialisierte Suchmaschine[29] eine Anlage im Internet aufspüren und deren eingebetteten Webserver mit Standard-Tools nach Sicherheitslücken durchsuchen kann. Besteht die Notwendigkeit, solche Systeme aus der Ferne zu administrieren, kann dies zum Beispiel via verschlüsselten VPN-Tunnel mit starker Authentifizierung ermöglicht werden.

Der Wirbel um die verwundbaren Steuerungen hat auch eine positive Seite: Das Thema Sicherheit wird nun in der Branche aktiver diskutiert.

Industrielle Kontrollsysteme (ICS) werden angegriffen

Kyle Wilhoit, ein Forscher bei Trendmicro, hat während eines längeren Zeitraums Angriffe auf ICS mit Hilfe von *Honeypots* untersucht[30]. Dabei hat er festgestellt, dass es kontinuierlich automatisierte und halbautomatische Angriffen gegen ICS gibt.

Dabei hat er folgende Erkenntnisse gewonnen:

- Über 16‘000 automatisierte Angriffe im Zeitraum von 5 Monaten, welche von 605 verschiedenen *IP Adressen* ausgegangen sind. Nicht gezählt wurden dabei Angriffe, welche nichts mit ICS zu tun hatten.

- Festgestellt wurden unter Anderem folgende Angriffe:
    - versuchter Zugriff auf Diagnose-Seiten der simulierten Systeme

[29] siehe beispielsweise Suchmaschine Shodan: http://www.shodanhq.com (Stand: 31. August 2013).

[30] Trendmicro: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-whos-really-attacking-your-ics-equipment.pdf und Blackhat: https://media.blackhat.com/us-13/US-13-Wilhoit-The-SCADA-That-Didnt-Cry-Wolf-Whos-Really-Attacking-Your-ICS-Devices-Slides.pdf (Stand: 31. August 2013).

- versuchter Zugriff und Modifikation von *Modbus/DNP3* Traffic
- Versuche, das (simulierte) Pumpensystem zu modifizieren
- Zugriffsversuche auf geschützte Bereiche
- nicht autorisierte Lese- und Schreibzugriffe auf *SPS* (PLCs).[31]

- Gegen eine auf dem Honeypot publizierte E-Mail Adresse wurden gezielte Angriffe mit Malware beobachtet. Der Angreifer versuchte auf diese Weise Daten zu stehlen, welche für weitergehende Angriffe hilfreich sind (Informationen über *VPN* Konfigurationen, Netzwerkeinstellungen sowie die Passwort Datenbank von Windows).

Die Analyse von Kyle Wilhoit zeigt auf, dass ICS, welche an das Internet angeschlossen sind, regelmässig angegriffen werden und zwar unabhängig davon, ob sie zu einer bekannten und besonders exponierten Anlage gehören oder nicht. ICS sollten deshalb in keinem Fall ohne zusätzliche Schutzmechanismen direkt an das Internet angeschlossen werden.

Was tun zum Schutz der Industriellen Kontrollsysteme (ICS)?

SANS[32], ein Sicherheitsinstitut aus den USA, hat 20 Schlüsselelemente[33] publiziert, wie IKT-Infrastrukturen generell geschützt werden können. Diese Elemente können teilweise auch auf ICS angewendet werden. Weitere Empfehlungen sind vom US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT[34]) sowie vom National Institute of Standards and Technology (NIST[35]) herausgegeben worden.

Die folgenden 11 Sicherheitsempfehlungen basieren auf diesen Dokumenten. Ausführlichere Erklärungen dazu sind auf der MELANI Webseite[36] zu finden.

1. Asset Datenbank für alle Geräte erstellen und pflegen
2. Life Cycle und Patchmanagement für Software etablieren
3. Sichere Konfigurationen definieren und verwenden
4. Robuste Netzwerkarchitekturen planen und bauen
5. Mehrstufigen Malwareschutz implementieren
6. Authentisierung und Autorisierung
7. Zentrale Logauswertung aufbauen
8. Physischen Schutz gewährleisten
9. Backup und Recovery durchführen und regelmässig testen

---

31 SPS bedeutet Speicherprogrammierbare Steuerung und wird zur Steuerung einer Anlage eingesetzt. PLC ist der entsprechende englische Ausdruck (Programmable Logic Controller)

32 SANS, http://www.sans.org (Stand: 31. August 2013).

33 SANS Top 20 Critical Security Controls: http://www.sans.org/critical-security-controls/ (Stand: 31. August 2013).

34 ICS CERT: http://ics-cert.us-cert.gov/ (Stand: 31. August 2013).

35 NIST: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf (Stand: 31. August 2013).

36 Checklisten und Anleitungen: http://www.melani.admin.ch/dienstleistungen/00132/index.html?lang=de (Stand: 31. August 2013).

10. Security Incident Management Prozesse etablieren und üben
11. Sicherheitskultur etablieren

Es ist wichtig zu verstehen, dass in den meisten Fällen die Sicherheit nicht schlagartig und mit einer einmaligen Aktion gewährleistet werden kann, sondern dass die Verbesserung ein kontinuierlicher Prozess ist, der nie endet. So ist es sinnvoll, sich realistische, erreichbare Ziele zu setzen und zuerst die Punkte abzuarbeiten, die mit einem relativ geringen Aufwand die Sicherheit spürbar erhöhen, z. B. alle Default-Passwörter zu ändern und von aussen erreichbare Steuerungsinterfaces zu schützen.

Während bei klassischen Informatiksystemen die Verfügbarkeit, die Vertraulichkeit und die Integrität einen in etwa gleich hohen Stellenwert haben, steht bei ICS die Verfügbarkeit stärker im Mittelpunkt. Der Schutz der Vertraulichkeit und der Integrität dient dabei ebenfalls dem Erhalt der Verfügbarkeit. So ist ein System, das über ein Protokoll kommuniziert, welches die Vertraulichkeit und die Integrität der übertragenen Daten schützt, besser gegen Angriffe auf Netzwerkebene geschützt und kann so eine höhere Verfügbarkeit erreichen.

4.6 Softwarepannen und ihre Auswirkung

Fehler in Buchungssystem – Zahlreiche Flüge von American Airlines ausgefallen

Am Vormittag des 16. April 2013 hat ein Computerfehler im Buchungssystem von American Airlines zu einem Ausfall geführt. In der Folge konnten für mehrere Stunden keine Flugzeuge mehr abgefertigt werden. Erst am Nachmittag konnten die Systeme wieder zum Laufen gebracht werden. Insgesamt fielen 700 Flüge aus, noch mehr Flüge waren verspätet. Die US-Fluggesellschaft wickelt täglich 3400 Flüge ab[37]. Die Ursache dieser Panne wurde nicht kommuniziert.

Dieses Beispiel illustriert, dass nicht nur Störungen in SCADA- und Industriellen Kontrollsystemen für Ausfälle kritischer Infrastrukturen sorgen können. Insbesondere wenn physische Prozesse auf die Verfügbarkeit von Daten(banken) angewiesen sind, können entsprechende Probleme ernsthafte Auswirkungen zeitigen.

Aufgrund eines Software-Fehlers ruft Chrysler hunderttausende Geländewagen zurück

Rückrufaktionen in der Automobilbranche sind nichts aussergewöhnliches. Immer öfter haben solche Ruckrufaktionen auch mit fehlerhaften Software zu tun. Im Mai 2013 hat Chrysler beispielsweise wegen einer fehlerhaften Software über 400‘000 Geländewagen zurückgerufen. Bei einigen Fahrzeugen wurde die Gangschaltung durch die Software ungewollt verstellt, was im schlimmsten Fall zu einem Unfall führen kann.

Immer mehr Funktionen werden in modernen Autos durch Software gesteuert und damit ist es nur eine Frage der Zeit, bis Software-Fehler vermehrt auch in Autos auftauchen.

[37] http://www.handelszeitung.ch/news/peinlicher-computerfehler-american-airlines-kann-nicht-fliegen (Stand: 31. August 2013).

4.7 Operationen, Anklagen und Verhaftungen gegen Cyberkriminelle

Im ersten Halbjahr 2013 kam es zu verschiedenen Polizeioperationen, Verhaftungen und Verurteilungen von Cyberkriminellen.

DDoS: Operation Payback

Im Januar 2013 hat die englische Justiz Christopher Weatherhead von der Anonymous-Bewegung für seine Rolle in der Operation Payback[38] gegen Paypal, Mastercard und Visa zu 18 Monaten Gefängnis verurteilt. Die Strafen für weitere Anonymous-Aktivisten fielen geringer aus. Das Gericht war der Meinung, Weatherhead habe bei der Operation eine führende Rolle gespielt.

E-Banking-Malware: Gozi

Ebenfalls im Januar 2013 erhob die amerikanische Justiz Anklage gegen drei Personen wegen Urheberschaft und Vertrieb der E-Banking *Malware* Gozi. Gozi soll über eine Million PCs in der ganzen Welt infiziert und Schäden in Millionenhöhe verursacht haben.

Ransomware: Reveton

Im Februar 2013 verhaftete die spanische Polizei mehrere Urheber und Betreiber der *Ransomware* Reveton, darunter auch den mutmasslichen Kopf der kriminellen Gruppierung. Die Schadsoftware Reveton blockiert einen infizierten PC und zeigt auf dem Bildschirm eine angebliche Polizeimeldung, die das Opfer diverser Straftaten beschuldigt. Wird eine bestimmte Summe bezahlt, soll die Strafverfolgung abgewendet und der PC entsperrt werden. Die Ransomware wurde länderspezifisch angepasst und hat zahlreiche PCs in fast dreissig Ländern befallen, darunter auch Computer in der Schweiz, siehe hierzu den MELANI Halbjahresbericht 2012/I[39]. Die Festnahmen erfolgten dank der Zusammenarbeit zwischen der spanischen Polizei, Europol, Interpol und der Internetsicherheitsfirma Trend Micro. Reveton und die diversen Varianten sind allerdings auch nach der Verhaftung weiterhin aktiv, auch in der Schweiz.

Botnetzwerk: Citadel

Das amerikanische Federal Bureau of Investigation (FBI) und die Softwarefirma Microsoft haben in einer am 6. Juni 2013 publik gemachten, gemeinsamen Aktion fast 1400 von Citadel verwendete Server deaktiviert. Diese weitverbreitete *Schadsoftware* existiert seit 2011 und dient dem E-Banking-Betrug, auch in der Schweiz. Gemäss Microsoft ist Citadel für Verluste in der Höhe von 500 Millionen Dollar für Kunden zahlreicher Finanzinstitute verantwortlich. Citadel ist eine personalisierbare E-Banking-Schadsoftware, welche auf dem Unter-

---

[38] MELANI Halbjahresbericht 2010/2, Kapitel 3.2: http://www.melani.admin.ch/dokumentation/00123/00124/01122/index.html?lang=de (Stand: 31. August 2013).

[39] MELANI Halbjahresbericht 2012/1, Kapitel 3.3: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=de (Stand: 31. August 2013).

grundmarkt im Internet erhältlich ist und von zahlreichen kriminellen Gruppen verwendet wird.

Das FBI und Microsoft haben die Aktion namens «b54» in Zusammenarbeit mit Finanzinstituten und Strafverfolgungsbehörden verschiedener Länder geführt. Die deaktivierten *Kommando- und Kontrollserver* waren für die Steuerung und Verwaltung von Botnetzwerken verwendet worden. Das FBI sucht in diesem Zusammenhang eine Person, die sich Aquabox nennt und verdächtigt wird, Urheberin der Schadsoftware zu sein.

Die Operation "b54" wird zweifellos das gute Geschäft der verschiedenen kriminellen Gruppen stören, die Citadel verwenden. Dennoch ist es wenig wahrscheinlich, dass diese Operation lang anhaltende Auswirkungen haben wird. Ebenso wenig dürfte die Existenz der Schadsoftware gefährdet worden sein. Die Fähigkeit von Schadsoftware und Botnetzen, sich nach solchen Aktionen wieder zu regenerieren, hat sich in der Vergangenheit bereits gezeigt. Es können sogar neue Funktionen ergänzt werden, wodurch es noch schwieriger wird, die entsprechende Schadsoftware ausfindig und unschädlich zu machen.

4.8 Vierte internationale Übung Cyberstorm

Am 20. und 21. März 2013 fand die vierte internationale Übung Cyberstorm statt. Hierbei testen jeweils die Mitgliedsländer des International Watch and Warning Networks (IWWN), darunter auch die Schweiz, ihre Zusammenarbeit und Reaktionsfähigkeit bei einem Cyberangriff. Die diesjährige Übung hatte vor allem das Ziel, Standardprozeduren zu testen, die die Bewältigung eines Cybervorfalls erleichtern sollen.

Cyberstrom ist eine internationale Cyberüberübung, die durch die USA und im Speziellen durch das Department of Homeland Security initiiert worden ist, um die Reaktionsfähigkeit bei Cybervorfällen zu testen. Die Übung ist mehrheitlich auf die USA und deren Sicherheitsorganisationen ausgerichtet, hat aber bereits seit der ersten Durchführung eine internationale Komponente. Die erste Übung dieser Art fand im Jahre 2006 statt. Analog zu der europäischen Übung Cyber Europe 2012 wurden bei «Cyberstorm IV» sogenannte Standard Operating Procedures (SOP) auf ihre Effektivität hin überprüft . Diese SOP regeln die Kontaktaufnahme, den Informationsaustausch und die Zusammenarbeit im Falle eines internationalen Cybervorfalles.

Das diesjährige Übungsszenario ging von einer Infektion grosser Medienportale und Verwaltungsrechner, sowie einem Datenabfluss an ausländische Server aus. Die Komplexität der mehr als 32 Stunden dauernden Übung erlaubte es, die Kooperation zwischen den Teilnehmern auszutesten. Insgesamt wurden 300 Ereignisse simuliert.

Vorfälle im Cyberbereich sind praktisch immer grenzüberschreitend. Es braucht deshalb einen gemeinsamen internationalen Ansatz, um in Cyberkrisen effizient bestehen zu können. Die Übung hat gezeigt, dass der Informationsaustausch auf technischer und operativer Stufe zwischen den Ländern gut und effizient funktioniert. Eine Herausforderung ist aber insbesondere die Auswertung der zahlreichen verfügbaren Daten, damit im Ernstfall zeitgerecht eine Lageanalyse mit allen relevanten Informationen als Basis für Entscheidungsträger erstellt werden kann.

5 Tendenzen / Ausblick

5.1 Von Staaten, der Wirtschaft und dem Recht

Jedes Unternehmen, ob es nur in seinem Heimatmarkt oder aber global tätig ist, untersteht der jeweiligen Gesetzgebung des Staates, in dem es aktiv ist. Dabei kommt dem Ort des Hauptsitzes eine besondere Bedeutung zu. Dort ist mit der Geschäftsleitung die typischerweise letzte Entscheidungsinstanz angesiedelt und – je nach Geschäftsfeld – wohl auch der Hauptort der Produktion, Logistik und Administration sowie die für Geschäftstätigkeit relevanten Informationen.

Diese eherne Grundregel gilt genauso für den Maschinenbauer und die Fast-Food-Kette, wie auch für die grossen Unternehmen, welche mit ihren Produkten und Dienstleitungen das Fundament und die Grundinfrastruktur für die weltweite Vernetzung liefern. Dass dabei unter all den nationalen anwendbaren Rechtsnormen auch Sicherheitsgesetze zu finden sind, die im Rahmen von Strafverfolgungen oder Verdacht auf terroristische Aktivitäten dazu geeignet sind, den Datenschutz in gewissen Fällen aufzuheben, versteht sich von selbst. Die Tatsache, dass hochspezialisierte Technikunternehmen gewisse Auslandsgeschäfte bei der nationalen Kontrollbehörde offenlegen müssen, um Exporte sogenannter Dual-Use-Güter in Länder zu verhindern, die sich nicht an das grundsätzliche Menschenrecht halten, wird gemeinhin akzeptiert. Das Hauptproblem liegt weniger im Sinn und der Stossrichtung, denn in den Auswirkungen und der Anwendung dieser Gesetze.

Im Falle der Anbieter von Informations- und Kommunikationstechnologien gesellt sich zu dieser Logik allerdings ein verschärfendes Element: Die überwältigende Mehrheit der Anbieter von Informations- und Kommunikationstechnologien – seien es Software- oder Hardwarehersteller, *Cloud*-Anbieter oder Datenübermittlungsdienste – haben ihren Hauptsitz in den USA und unterstehen somit in erster Linie der amerikanischen Gesetzgebung und Rechtsprechung. Die Zentralisierung der Marktmacht eines Bereiches in einem Land führt auch zu einer Ballung der Möglichkeiten seitens eines einzelnen Staates, auf der Basis seiner Gesetzgebung auf die Kerninfrastrukturanbieter der weltweiten Vernetzung zurückzugreifen. Es erscheint dabei klar, dass in einem solchen Falle die Anwendung nationaler Gesetze immer auch eine globale Auswirkung mit sich bringen werden. So gesehen verfügt die USA im Bereich der IKT-Unternehmen und deren Rolle als Treiber und Unterhalter der globalen Vernetzung de facto über eine unipolare, hegemoniale Stellung in der Welt. Zwar könnte eingewendet werden, China vereine im Bereich der Herstellung von Hardwarebausteinen ebenfalls eine überwältigende Marktmacht auf sich – Stichwort Supply Chain. Gerade dieses Thema wird in Zukunft noch einigen Klärungsbedarf mit sich bringen. Doch der Endbetrieb dieser Hardware ausserhalb Chinas, die Entwicklung der Firmware, die diese Komponenten ansteuert, etc… liegen oft nicht in Chinesischer Hand. Speziell bei Suchmaschinenanbietern, E-Mail-Lösungen oder Social-Media verfolgt China lokale Lösungen die somit keine globalen Implikationen mit sich bringen und die Vormachtstellung der in den USA ansässigen Unternehmen in diesem Bereich nicht konkurrieren.

In der Geschichte brachten hegemoniale Stellungen aus sicherheitspolitischer Sicht immer auch einen Strauss heikler Fragen für andere Staaten, deren Wirtschaft und Bevölkerung mit sich. Um den Kern dieser Problematik kreist dabei immer die Frage, inwieweit ein Hegemon bereit ist, seine Dominanz gegenüber anderen auszuspielen, respektive die Frage, ob sich der Hegemon über seine Vormachtstellung und die globalen Implikationen, die sie mit sich bringt, überhaupt im Klaren ist. Am Ende zielen diese Fragen auf die Berechenbarkeit des

Hegemonen im Sinne eines Schutzes vor Willkür, respektive Machtmissbrauch, welche einen wichtigen Faktor für andere Staaten im Umgang mit Hegemonen bildet. Und am Ende bildet diese Berechenbarkeit (im Sinne einer Planungs- und Rechtssicherheit) auch das Fundament für die Wirtschaft zum Umgang mit notwendigen Partnern im rechtlichen Einflussbereich des Hegemonen.

Es sollte im Interesse jenes Staates sein, der über eine solche Vormachtstellung verfügt, gerade diese Fragen früh und abschliessend zu klären. Dabei handelt es sich nicht um eine Frage seiner gesetzlichen Souveränität, sondern in erster Linie um die (politische) Klarstellung, welche Ziele er mit seinen Gesetzen verfolgt und wie weit er beabsichtigt, solche zu Gunsten seiner (Eigen-)Interessen auf Kosten ausländischer Interessen zu erlassen und anzuwenden. Sprich, inwiefern er gewillt ist, mit seiner Rechtsordnung und somit seinem Einfluss auf die einheimische (aber ggf. global tätige) Industrie, seine eigenen sicherheitspolitischen (und möglicherweise wirtschaftlichen) Interessen zum Nachteil anderer Staaten zu verfolgen oder darauf explizit zu verzichten. Es ist aber auch Aufgabe der internationalen Staatengemeinschaft, diese Fragen im internationalen Diskurs zu lancieren und auf eine Klärung in die eine oder andere Richtung hinzuarbeiten. Gerade die Schweiz ist hier aktiv in multilateralen und bilateralen Foren aktiv tätig.

Eine längerfristig andauernde Phase der Unklarheiten und Unberechenbarkeit hätte unweigerlich zur Folge, dass Staaten auf eigene, unabhängige IKT-Lösungen setzen müssten, dies allerdings nicht im Rahmen des sportlichen, marktwirtschaftlichen Wettbewerbs, sondern als sicherheitspolitisches Instrument und Abgrenzung zu den Produkten aus dem Lande des Hegemons. Dass dies mit Ineffizienz und ungebührenden Kosten auch für die Wirtschaft und speziell die kritischen Infrastrukturen verbunden sein wird, versteht sich dabei von selbst und sollte deshalb immer die schlechtere der Lösungen sein.

Die Melde- und Analysestelle Informationssicherung Schweiz (MELANI) propagiert seit jeher einen risikobasierten Umgang im Bereich der Informationssicherheit und dem Schutz im Bereich der IKT-Infrastrukturen, wie er nun auch von der bundesrätlichen «Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)» aufgenommen wurde. Dies anstelle eines rein technischen Ansatzes auf Basis der IKT-Möglichkeiten. Alternativen dazu im Bereich der Router-Produkte und marktwirtschaftlich induzierte Programme in diesem Bereich ausserhalb der USA und China existieren dabei schon heute und werden auch eingesetzt.[40]

Damit dieser Umgang mit Cyber-Risiken auch gelingen kann, ist es essentiell, dass die Bedrohung in ihren mannigfachen Ausprägungen abgeschätzt und verstanden werden kann. Dabei spielen nicht nur Akteure, technische Verletzlichkeiten und die neusten Erkenntnisse zu Vorfällen eine Rolle, sondern auch nicht-technische Faktoren im Bereich der physischen, personellen und organisatorischen Ausgestaltung, sowie die rechtlichen Rahmenbedingungen und hoheitlichen Eingriffe im Land der Produkthersteller, Dienstleistungsanbieter und eingesetzten Datenspeicher. Es soll dabei jedem Unternehmen belassen sein, jene Risikofaktoren stärker oder weniger stark zu gewichten, die seinem Profil, seinen kritischen Prozessen und Exponiertheit im Ausland, sowie seiner Geschäftstätigkeit am ehesten entspricht.

[40] http://www.fp7-ofelia.eu/about-ofelia/ (Stand: 31. August 2013).
http://www.change-project.eu (Stand: 31. August 2013).
http://www.openflow.org/wk/index.php/MPLS_with_OpenFlow/SDN (Stand: 31. August 2013).
http://www.heise.de/ix/artikel/Alles-fliesst-1643457.html (Stand: 31. August 2013).

Um in Zukunft in diesem Bereich den Unternehmen und speziell den kritischen Infrastrukturen verstärkt Unterstützung bieten zu können, wurde mit der „Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (Nationale Cyber-Strategie; NCS) neben der Aufstockung von MELANI bis 2017 auch eine Stärkung jener Ressourcen vorgenommen, die im internationalen, sicherheitspolitischen Bereich die Positionen der Schweiz und ihrer Wirtschaft einbringen sollen.

5.2 Tallinn Manual

Im März 2013 wurde das «Tallinn Manual» (Originaltitel: Tallinn Manual on the International Law Applicable to Cyber Warfare) veröffentlicht.[41] Es handelt sich dabei um eine Studie, wie internationales Recht – insbesondere das «Recht zum Krieg» (ius ad bellum), sowie das humanitäre Völkerrecht («Recht im Krieg», ius in bello) – auf Cyber-Operationen Anwendung finden kann.

In 95 kommentierten Regeln beschäftigt sich das Tallinn Manual unter anderem mit Fragen bezüglich staatlicher Souveränität, Gerichtsbarkeit und Verantwortlichkeiten, wie auch mit neutralitätsrechtlichen Implikationen. Es wird eruiert, wann ein ziviler Hacker als aktiver Kriegsteilnehmer («Kombattant») gelten kann und dadurch zu einem legitimen Angriffsziel wird, respektive inwiefern dessen Aktivitäten einem Staat zugerechnet werden dürfen. Weiter werden auch der Schutz kritischer ziviler Infrastruktur sowie Angriffe auf Kernkraftwerke und Staudämme thematisiert.[42]

Das Manual wurde auf Einladung des in der estnischen Hauptstadt Tallinn angesiedelten NATO Cooperative Cyber Defence Center of Excellence von einer rund 20-köpfigen internationalen Expertengruppe aus verschiedenen Bereichen zwischen 2009 und 2012 erarbeitet. Es ist kein offizielles NATO Dokument, sondern eine rechtlich nicht bindende akademische Publikation, welche Ansätze und (z. T. voneinander abweichende) Meinungen aufzeigt, wie bestehendes internationales Recht auf die neuartige Umgebung «Cyber» angewendet werden könnte. Da es sich um eine erste ausführliche Publikation in diesem Bereich handelt, ist trotz ihres nicht-offiziellen Charakters damit zu rechnen, dass verschiedene Staaten und Organisationen die darin vertretenen Meinungen bei der Formulierung ihrer Positionen und Leitfäden beachten.

5.3 Baldiges Supportende für Microsoft Windows XP SP3 und Microsoft Office 2003

Am 8. April 2014 endet der Support für Microsoft Windows XP SP3 und Microsoft Office 2003. Allen Unternehmen, die mit diesen Versionen arbeiten, wird dringend ein Upgrade auf neuere, weiterhin unterstützte Betriebssystem- und Softwareversionen empfohlen.

Nach dem 8. April 2014 werden für Windows XP SP3 und Office 2003 weder Support noch Sicherheits*patch*es oder Problembehebungen mehr vom Hersteller frei erhältlich sein. Schwachstellen nicht mehr unterstützter Betriebssysteme und Applikationen werden nicht

[41] http://issuu.com/nato_ccd_coe/docs/tallinnmanual?e=5903855/1802381 (Stand: 31. August 2013).
[42] http://ccdcoe.org/249.html (Stand: 31. August 2013).

behoben, was gezielt für Cyberangriffe auf Computer genutzt werden könnte, die weiterhin mit Windows XP SP 3 und/oder Office 2003 betrieben werden. Die Chance auf Erfolg solcher Angriffe ist erhöht und entsprechend steigt das Sicherheitsrisiko bei Benutzern, die alte Versionen verwenden.

Die neusten Softwareversionen bieten Verbesserungen bezüglich Sicherheit, da sie die aktuellsten Sicherheitstechnologien enthalten. Zudem beseitigt der Hersteller weiterhin Schwachstellen, welche bekannt werden. Die Verwendung der aktuellsten Betriebssysteme und Applikationen ist neben dem *Patch*-Management eines der effektivsten Mittel im Hinblick auf die Sicherheit.

Für Unternehmen, die das Upgrade nicht bis zum 8. April 2014 vornehmen können, besteht die Möglichkeit, einen Servicesupportvertrag mit Microsoft abzuschliessen. Die Kosten für den Servicesupport sind deutlich höher als für den normalen Support und steigen sukzessive an. Auch wer den Servicesupport wählt, muss als Teil des Vertrags mit Microsoft einen Plan für den Umstieg von Windows XP SP3 und Office 2003 auf neuere Produkte vorlegen.

Der Support für Microsoft Exchange Server 2003 und Microsoft Office SharePoint Server 2003 endet ebenfalls am 8. April 2014.[43]

5.4 Problemzone Content Management System (CMS)

In den vergangenen Jahren ist die Anzahl von Webauftritten im Internet geradezu explodiert. Dies unter anderem, weil auch technisch nicht versierte Benutzer dank einfach handzuhabenden Werkzeugen und immer tieferen Preisen eine eigene Webseite ins Internet stellen können. Dazu werden oftmals so genannte *Content Management Systeme (kurz CMS)* verwendet, mittels welchen eine Website mit nur ein paar wenigen Klicks und ohne fundierte Kenntnisse in Webdesign erstellt und aufgeschaltet werden kann. Heutzutage gibt es Dutzende solcher CMS, welche von Hobby-Website-Betreibern bis hin zu KMU eingesetzt werden. Die zunehmende Verbreitung solcher Systeme macht diese auch für Cyberkriminelle interessant, welche umso mehr Energie und Aufwand in die Suche von Sicherheitslücken stecken, je weiter verbreitet eine Software und entsprechend grösser die Anzahl möglicher Angriffsziele ist. Nicht nur CMS, sondern jede Software hat potenziell Sicherheitslücken – es gibt keine garantiert sichere Software. Zudem implementieren die Softwarenwickler immer neue Funktionalitäten. Mit jeder zusätzlichen Codezeile erhält die Software aber nicht nur mehr Funktionen, auch ihre Komplexität steigt und damit das Risiko, dass sie irgendwo eine Sicherheitslücke enthält.

Sicherheitslücken bleiben den Software-Entwicklern in der Regel nicht lange verborgen und oftmals vergehen nur wenige Tage von der Entdeckung einer Sicherheitslücke bis zur Auslieferung eines entsprechenden Sicherheitsupdates durch den Hersteller, welches diese beheben soll. Da solche Sicherheitsupdates nicht automatisch auf dem System installiert werden, ist die Aktion des Website-Betreibers gefragt. Da mittlerweile viele Websites von technischen

[43] Genaue Angaben zum MS Support Lifecycle: http://support.microsoft.com/lifecycle (Stand: 31. August 2013). Genaue Angaben zum Supportende Windows XP SP3 und Office 2003: http://www.microsoft.com/endofsupport (Stand: 31. August 2013).

Laien betrieben werden, denen zwar die Erstellung einer Website vereinfacht, aber die nötigen Massnahmen zum sicheren Unterhalt nicht erklärt werden, gibt es entsprechend viele Webauftritte, welche ein CMS verwenden, das seit Monaten oder sogar Jahren nicht mehr aktualisiert worden ist und die unter Umständen bereits Dutzende (bekannte) Sicherheitslücken aufweisen.

Solche verwundbaren Websites können mit entsprechenden Tools automatisiert aufgefunden und angegriffen werden. Es ist für Kriminelle relativ einfach, auf diese Weise eine grosse Zahl von Webauftritten derart zu manipulieren, dass ihre Besucher mit Schadsoftware infiziert werden.

Angriffe auf CMS lassen sich durch das erwähnte *Patch*ing (zeitnahes Einspielen von Sicherheitsaktualisierungen) massiv reduzieren. Es gibt jedoch eine Reihe weiterer Massnahmen, welche zur Sicherheit von CMS beitragen. Erklärungen zu den aufgelisteten Massnahmen finden Sie auf der MELANI-Webseite unter «Checklisten und Anleitungen»[44].

1. Zeitnahes Einspielen von Sicherheitsaktualisierungen
2. Zwei-Faktor-Authentifizierung
3. Einschränkung der Administrator-Zugriffe auf bestimmte IP Adressen
4. Einschränkung der Administrator-Zugriffe mittels .htaccess-Datei
5. Absichern des Computers des Webmasters
6. Web Application Firewall
7. Frühzeitige Erkennung von Sicherheitslücken.

5.5 Wo man sich trifft (und infiziert) – das Wasserloch

In trockenen Regionen finden sich früher oder später alle Tiere am Wasserloch zum Trinken ein. Dieses Phänomen ist namensgebend für eine Angriffsart, welche in letzter Zeit vermehrt beobachtet werden konnte: Der Wasserloch-Angriff (engl. *Watering-Hole Attack*). Auch im Internet gibt es Orte, an welchen sich Internetnutzende regelmässig aufhalten – nicht um sich Wasser oder Nahrung, sondern um Informationen zu besorgen. Während Suchmaschinen, Newsportale und soziale Netzwerke eine grosse Zahl von verschiedensten Personen anziehen, gibt es Websites von thematisch spezialisierten Informationsanbietern, welche regelmässig von entsprechend interessierten Nutzerinnen und Nutzer aufgesucht werden. Dies kann ein Angreifer ausnützen, welcher es auf eine bestimmte Berufs- oder Interessengruppe abgesehen hat. Kann er eine solche Webseite hacken und *Schadsoftware* darauf platzieren, wird ihm danach ein gezieltes Publikum präsentiert.

Im Frühling 2013 wurde zum Beispiel die Website des amerikanischen Arbeitsministeriums gehackt und darauf eine *Drive-by* Infektion platziert, welche eine vorher unbekannte *Sicherheitslücke* im Internet Explorer 8 ausnutzte. Auf der betroffenen Seite können sich die Angestellten von Energiekonzernen über Entschädigungsprogramme nach dem Kontakt mit Uran informieren. Die Computer der Interessierten, welche diese Seite aufriefen, wurden mit Spio-

[44] Checklisten und Anleitungen http://www.melani.admin.ch/dienstleistungen/00132/index.html?lang=de (Stand: 31. August 2013).

nagesoftware infiziert. Diese gezielte Platzierung lässt darauf schliessen, dass es die Angreifer auf Personen aus dem Energiesektor – insbesondere Atomkraftwerken – und Regierungsmitarbeitenden in diesem Bereich abgesehen haben. Aber auch Personen, die mit Atomwaffen arbeiten, standen im Fokus der Angreifer.

Meldungen über solche Watering-Hole-Angriffe haben in der Berichtsperiode zugenommen. Im Unterschied zu herkömmlichen Drive-by Infektionen, bei welchen Kriminelle undifferenziert schlecht geschützte Webseiten für die Verbreitung ihrer Schadsoftware auf beliebige Computer ausnützen, wird bei Watering-Hole-Angriffen erheblich mehr Aufwand betrieben, um spezifische Webseiten ungeachtet der vorhandenen Sicherheit zu hacken.

Obwohl diese Angriffe primär auf Büro-Computer ausgerichtet sind, können je nach betroffenem Unternehmen neben Geschäftsgeheimnissen auch andere schutzwürdige Informationen (Netzpläne, Adressierungen und Zugangsdaten für Kontrollsysteme usw.) beschafft werden, welche sich für verschiedene weitere Angriffe nutzen lassen. Die Hacker können in einem ungenügend segmentierten Unternehmensnetzwerk auch von System zu System gelangen, bis sie schliesslich ein Kontrollsystem erreichen, welches physische Prozesse steuert, um dieses zu manipulieren.

Früher oder später taucht bei jedem Browser eine *Sicherheitslücke* auf. Im Kapitel 5.1 des MELANI Halbjahresberichts 2012/2[45] haben wir Möglichkeiten zur Risikominderung bei Bekanntwerden von Browserlücken aufgezeigt. Es besteht jedoch immer die Möglichkeit, dass Watering-Hole-Angriffe mit bis zu diesem Zeitpunkt noch unbekannten Sicherheitslücken (auch in *Plug-Ins*) durchgeführt werden.

5.6 Smartphone-Trojaner

Der Trend von Schadsoftware auf Smartphones hat sich im letzten Halbjahr erneut fortgesetzt und hat in den letzten Monaten stark zugenommen. Im Fokus steht dabei vor allem das Betriebssystem Android. Die Gründe dafür liegen in der starken Verbreitung von Android, in der offenen Struktur, wie sie bereits im letzten Halbjahresbericht[46] diskutiert worden ist, aber auch in der Tatsache, dass sehr viele Hersteller Sicherheitsupdates nicht oder erst lange nach Bekanntwerden einer Lücke nachliefern.

Die Ziele der Angreifer sind sehr unterschiedlich:

- Angriffe auf Bankkonten: Stehlen von *mTANs*
- Versenden von kostenpflichtigen SMS
- Angriffe auf mobile Micropayment Applikationen

---

[45] MELANI Halbjahresbericht 2012/2, Kapitel 5.1: http://www.melani.admin.ch/dokumentation/00123/00124/01535/index.html?lang=de (Stand: 31. August 2013).

[46] MELANI Halbjahresbericht 2012/2, Kapitel 4.8: http://www.melani.admin.ch/dokumentation/00123/00124/01535/index.html?lang=de (Stand: 31. August 2013).

- Diebstahl von Zugangsdaten für soziale Netzwerke und E-Mail-Konten
- Adressdaten: Namen, Telefonnummern, E-Mail-Adressen und Geburtstage der Kontakte
- Identitätsdiebstahl
- Allgemeiner Datendiebstahl.

Sehr oft wird eine Social Engineering-Komponente für die Verbreitung der Malware eingesetzt. Zum Beispiel werden bekannte Apps trojanisiert und via einen nicht offiziellen App-Store in Umlauf gebracht. Vorgängig werden E-Mails mit den entsprechenden Links verschickt, beispielsweise gefälschte E-Mails von einer Bank, welche über eine neue App informieren, die man benötigen würde, um Online-Banking zu machen. Es wurden auch *Drive-by Infektionen* beobachtet, bei denen prinzipiell der Besuch einer Website ausreicht, um das Gerät zu infizieren. Eine neue Dimension wird mit dem Aufkommen von ersten Botnets, welche ausschliesslich aus Android Geräten bestehen, erreicht. Diese werden beispielsweise für das Versenden von Spam-Mails verwendet.

Interessanterweise scheint ein grosser Teil dieser sich im Umlauf befindenden *Malware* auf dem gleichen Grundcode aufzubauen. So wurde eine bestimmte Bibliothek (libvadgo) in verschiedenen Malware-Varianten gefunden und dient der Kommunikation mit *Command and Control Servern*. Diese Bibliothek kann sich zudem vor Analysetools verbergen, indem sie gewisse Prozesse beendet oder bestimmte Befehle manipuliert.

Die meiste Malware für Mobilgeräte wird im Augenblick für Android geschrieben. Aber auch die anderen Plattformen sind angreifbar. Geht es um gezielte Angriffe gegen bestimmte Firmen oder Personengruppen, hat ein iPhone oder Windows-Phone eine ähnliche Angriffsfläche wie ein Android-Gerät. Mobile Geräte können – insbesondere bei ansonsten gut gesicherten Umgebungen – als Eintrittstor dienen, um in interne Netze einzudringen. Diese Problematik muss insbesondere bei *Bring Your Own Device (BYOD)* Projekten beachtet werden.

MELANI empfiehlt folgende Verhaltensregeln, um mobile Geräte sicher zu nutzen:

1. Setzen Sie die vorhandenen Sicherheitsmechanismen auf Ihrem Smartphone richtig ein (z. B. PIN Eingabe und automatisches Sperren des Homescreens).
2. Installieren Sie nur Anwendungen aus offiziellen AppStores. Vergleichen Sie dort die Bewertungen und Rückmeldungen von Benutzern. Installieren Sie nie Anwendungen via Links aus E-Mails.
3. Prüfen Sie vor einer Installation die Rechte, welche eine Anwendung verlangt und überlegen Sie, ob diese wirklich notwendig sind, resp. ob Sie diese gewähren wollen (z.B. Zugriff auf das Adressbuch oder das Lesen und Versenden von SMS). Verzichten Sie im Zweifelsfall lieber auf eine Installation.
4. Seien Sie vorsichtig beim Verwenden von unbekannten WiFi-Hotspots. Konfigurieren Sie Ihr Smartphone so, dass es sich nicht automatisch mit neuen Wireless-Netzwerken verbindet.
5. Bei Android Geräten ab Version 4.2: Stellen Sie sicher, dass der Reputations-Dienst von Google aktiv ist; dieser schützt Ihr Gerät vor bekannten Bedrohungen (bösartigen Apps). Der Dienst kann in der App «Google Einstellungen» im Menü-Punkt «Apps bestätigen» konfiguriert werden. Die Einstellung «Apps überprüfen» sollte aktiviert sein.

6. Bei Android Geräten: Vergewissern Sie sich, dass die Installation von Apps nur aus dem offiziellen Google Play Store erlaubt ist (die Option «Unbekannte Quellen» unter Einstellungen -> Sicherheit -> Geräteverwaltung sollte deaktiviert sein).

Im Anhang 7.1 ist eine Analyse des in der ersten Hälfte 2013 in der Schweiz aufgetretenen Android-Trojaners publiziert.

5.7 Missbrauch der und Angriffe auf die Internettelefonie (VoIP)

Die Risiken bei der Verwendung der VoIP-Technologien und die Möglichkeiten missbräuchlicher Nutzung betreffen sowohl Privatpersonen als auch Unternehmen. Das Schadenspotenzial eines Missbrauchs der VoIP-Infrastruktur bei Unternehmen ist jedoch viel grösser. Schliesslich müssen die unbestreitbaren wirtschaftlichen Vorteile der VoIP-Telefonie immer gegen die möglichen Nachteile in Bezug auf die Sicherheit abgewogen werden. Betrug, der ganz oder teilweise via Telefon erfolgt, benutzt heute weitgehend die VoIP-Technologie. Ein Beispiel aus der Schweiz ist in Kapitel 3.6 beschrieben. Andere möglichen Angriffsarten sind nachfolgend beschrieben:

Angriff auf die Verfügbarkeit (Telephony Denial of Service)

Anfang 2013 haben amerikanischen Behörden auf die Gefahr von *Telephony Denial of Service* hingewiesen, also Angriffe auf die Verfügbarkeit von Telefondiensten. Dabei wird eine Telefonzentrale mit Anrufen überschwemmt, damit diese nicht mehr erreicht werden kann. Diese Anrufe werden von einer (kompromittierten) VoIP-Anlage automatisiert und ohne grosse Kosten durchgeführt. Meist wird ein solcher Angriff von einer Geldforderung begleitet. Die Betreiber der Linie sollen eine bestimmte Summe zahlen, damit der Angriff aufhört. Das Phänomen ist äusserst besorgniserregend, wenn es öffentliche Dienste und namentlich medizinische Notfallnummern betrifft.

Spionage

Mit VoIP werden Gespräche in digitale Daten umgewandelt. Analog zu allen anderen digitalen Daten können Angreifer versuchen, auch an diese Daten zu kommen. Es gibt verschiedene Abhör-Methoden: Einige Schadprogramme sind so konzipiert, dass sie direkt auf einem Computer installiert werden und dort die Signale von Gesprächen erfassen, bevor diese chiffriert und via *IP-Protokoll* verschickt werden. Andere Angriffe erfolgen direkt auf den VoIP-Servern, um den darüber laufenden Kommunikationsverkehr auszuspionieren. Weiter ist darauf hinzuweisen, dass der Abtransport gestohlener Daten in einigen Fällen als VoIP-Verkehr getarnt wird.

1. Eine erste Grundregel zur Minimierung der Risiken bei der Verwendung dieser Technologien ist, so einfach es klingt, das Ändern der initialen Zugangscodes durch komplexe Passwörter.
2. Wie bei allen anderen Softwareprodukten müssen auch bei VoIP die verwendeten Programme permanent aktualisiert werden.
3. Eine konkretere Sicherheitsmassnahme besteht darin, VoIP-Telefone so zu konfigurieren, dass nur Anrufe an bestimmte Rufnummernbereiche möglich sind und Anrufe an Mehrwertnummern nach Möglichkeit gesperrt werden.

6 Glossar

App	Der Begriff App (von der englischen Kurzform für Application) bezeichnet im Allgemeinen jede Form von Anwendungsprogrammen. Im Sprachgebrauch sind damit mittlerweile jedoch meist Anwendungen für moderne Smartphones und Tablet-Computer gemeint.
Advanced Persistent Threats (APT	Diese Bedrohung führt zu einem sehr hohen Schaden, der auf eine einzelne Organisation oder auf ein Land wirkt. Der Angreifer ist bereit, sehr viel Zeit, Geld und Wissen in den Angriff zu investieren und verfügt in der Regel über grosse Ressourcen.
Botnetz	Eine Ansammlung von Computern, die mit Malicious Bots infiziert sind. Diese lassen sich durch einen Angreifer (den Botnetzbesitzer) komplett fernsteuern. Je nach Grösse kann ein Botnetz aus einigen Hundert bis Millionen kompromittierter Rechner bestehen.
Bring Your Own Device (BYOD)	Bring Your Own Device (BYOD) ist eine Organisationsrichtlinie, die regeln soll, auf welche Weise Mitarbeitende ihre eigenen elektronischen Bürogeräte zu dienstlichen Zwecken nutzen dürfen.
Brute Force	Die Brute-Force-Methode ist eine Lösungsmethode für Probleme aus den Bereichen Informatik, Kryptologie und Spieltheorie, die auf dem Ausprobieren aller (oder zumindest vieler) möglichen Fälle beruht.
Cloud Computing	Cloud Computing (Synonym: Cloud IT, deutsch etwa Rechnen in der Wolke) ist ein Begriff aus der Informations- und Kommunikationstechnik (IKT). Die IKT-Landschaft wird durch den Anwender nicht mehr selbst betrieben/bereitgestellt, sondern über einen oder mehrere Anbieter bezogen. Die Anwendungen und Daten befinden sich nicht mehr auf dem lokalen Rechner oder im Firmenrechenzentrum, sondern in der Wolke (Cloud). Der Zugriff auf diese entfernten Systeme erfolgt über ein Netzwerk.
Kommando- und Kontrollserver Infrastruktur	Die meisten Bots können von einem Botmaster über einen Kommunikationskanal überwacht werden und Befehle empfangen. Dieser wird als Command and Control Server bezeichnet.
Content Management System	Ein Content Management System (kurz: CMS, übersetzt: Inhaltsverwaltungssystem) ist ein Sys-

	tem, das die gemeinschaftliche Erstellung und Bearbeitung von Inhalt, bestehend aus Text- und Multimedia-Dokumenten, ermöglicht und organisiert, meist für das World Wide Web. Ein Autor kann ein solches System auch ohne Programmier- oder HTML-Kenntnisse bedienen. Der darzustellende Informationsgehalt wird in diesem Zusammenhang als Content (Inhalt) bezeichnet.
Distributed Denial Of Service (DDoS)	Denial of Service Attacke. Hat zum Ziel, einen bestimmten Dienst für deren Benutzer unerreichbar zu machen oder zumindest die Erreichbarkeit des Dienstes erheblich einzuschränken.
DNS	Domain Name System. Mit Hilfe von DNS lassen sich das Internet und deren Dienste benutzerfreundlich nutzen, da die Benutzer anstelle von IP-Adressen Namen verwenden können (z.B. www.melani.admin.ch).
DNS-Reflektionsattacke	Siehe DNS-Amplifikationsattacke.
DNS-Amplifikationsattacke	Denial of Service (DoS)-Angriff, der öffentlich zugängliche DNS-Server missbraucht und als Amplifier (Verstärker) benutzt.
Drive-by	Infektion eines Computers mit Malware allein durch Besuch einer Web-Seite. Vielfach beinhalten die betroffenen Web-Seiten seriöse Angebote und sind zwecks Verteilung der Malware zuvor kompromittiert worden. Die Infektion erfolgt meistens durch das Ausprobieren von Exploits für vom Besucher noch nicht geschlossene Sicherheitslücken.
Fernwartung	Die Fernwartungssoftware (englisch: Remote Administration Tool) stellt eine Anwendung des Konzeptes Fernwartung für beliebige Rechner oder Rechnersysteme dar.
Firewall	Eine Firewall (engl. für Brandmauer) schützt Computersysteme, indem sie ein- und ausgehende Verbindungen überwacht und gegebenenfalls zurückweist. Im Gegensatz dazu ist eine Personal Firewall (auch Desktop-Firewall) für den Schutz eines einzelnen Rechners ausgelegt und wird direkt auf dem zu schützenden System – das heisst auf Ihrem Rechner – installiert.
Flash	Adobe Flash (kurz Flash, ehemals Macromedia Flash) ist eine proprietäre integrierte Entwicklungsumgebung zur Erstellung multimedialer Inhalte. Flash findet heutzutage auf vielen Webseiten Anwendung, sei es als Werbebanner, als Teil einer Website z.B. als Steuerungsmenü oder in Form

	kompletter Flash-Seiten.
FTP	FTP ist ein Netzwerkprotokoll zur Dateiübertragung über TCP/IP-Netzwerke. FTP kann beispielsweise verwendet werden, um Webseiten auf einen Webserver zu laden.
Gateways	Ein Gateway verbindet Rechnernetze, die auf völlig unterschiedlichen Netzwerkprotokollen basieren können.
Geolocation	Geolocation ordnet IP-Adressen ihrer geografischen Herkunft zu.
Honeypots	Als Honigtopf oder auch englisch Honeypot wird eine Einrichtung bezeichnet, die einen Angreifer oder Feind vom eigentlichen Ziel ablenken soll oder in einen Bereich hineinziehen soll, der ihn sonst nicht interessiert hätte.
Hyperlink	Ein Hyperlink, kurz Link, oder elektronischer Verweis ist ein Querverweis in einem Hypertext, der funktional einen Sprung an eine andere Stelle innerhalb desselben oder zu einem anderen elektronischen Dokument ausführt.
Internet Service Provider (ISPs)	Ein Internet Service Provider ist ein Internet-Dienstanbieter, die meist gegen Entgelt verschiedene Leistungen erbringen, die für die Nutzung oder den Betrieb von Internet-Diensten erforderlich sind.
Intrusion Detection Systeme	Systeme, mit denen man unautorisierte Zugriffe auf Daten oder Rechner erkennen kann.
IP address spoofing	Spoofing nennt man in der Informationstechnik verschiedene Täuschungsversuche in Computernetzwerken zur Verschleierung der eigenen Identität.
IP-Adresse	Adresse, welche einen Computer im Internet (oder einem TCP/IP-Netzwerk) identifiziert (Beispiel: 172.16.54.87).
IP-Protokoll	Das Internet Protocol (IP) ist ein in Computernetzen weit verbreitetes Netzwerkprotokoll und stellt die Grundlage des Internets dar. Es ist die Implementierung der Vermittlungsschicht des TCP/IP-Modells bzw. der Vermittlungsschicht (engl. Network Layer) des OSI-Modells.
Java	Java ist eine objektorientierte Programmiersprache und eine eingetragene Marke des Unternehmens Sun Microsystems (2010 von Oracle aufgekauft).

Malware	Oberbegriff für Software, die schädliche Funktionen auf einem Rechner ausführt (wie beispielsweise Viren, Würmer, Trojanische Pferde). Siehe auch Schadsoftware.
Mobile Banking	Mit dem Begriff Mobile-Banking wird die Abwicklung von Bankgeschäften bezeichnet, die unter Zuhilfenahme von mobilen Endgeräten wie Mobiltelefonen oder PDAs stattfindet.
Modbus/DNP3	Modbus und DNP3 (Distributed Network Protocol) sind Kommunikationsprotokolle bei Systemen der Prozessautomation.
mTAN	Einmalpasswort, welches via SMS versendet wird und vorwiegend im Online-Banking verwendet wird.
Open DNS resolvers	DNS-Server, die für alle Benutzer im Internet erreichbar und verwendbar sind.
Open Source	Open Source ist eine Palette von Lizenzen für Software, deren Quelltext öffentlich zugänglich ist und durch die Lizenz Weiterentwicklungen fördert.
Packer	Kompressionsprogramm oder Kompressionsalgorithmus eines Programmes. Ursprünglich dazu gedacht, die Grösse eines Programmes auf der Festplatte zu optimieren. Malware nutzt oft vorgelagerte Packer, um einerseits ihre Erkennung durch Antivirensoftware zu verhindern und um andererseits die Analyse der Malware (Reverse Engineering) zu erschweren. Rhythmus
Datenpaket	Ein Datenpaket ist in der Datenverarbeitung ganz allgemein eine der Bezeichnungen für in sich geschlossene Dateneinheiten, die ein Sender oder auch ein sendender Prozess einem Empfänger sendet.
Patch	Eine Software, die den fehlerhaften Teil eines Programms durch einen fehlerfreien ersetzt und dadurch z.B. eine Sicherheitslücke behebt.
Phishing	Mittels Phishing versuchen Betrüger, an vertrauliche Daten von ahnungslosen Internet-Benutzern zu gelangen. Dabei kann es sich beispielsweise um Kontoinformationen von Online-Auktionsanbietern (z.B. eBay) oder Zugangsdaten für das Internet-Banking handeln. Die Betrüger nutzen die Gutgläubigkeit und Hilfsbereitschaft ihrer Opfer aus, indem sie ihnen beispielsweise E-Mails mit gefälschten Absenderadressen zustellen.

PHP-Script	PHP ist eine Skriptsprache, die hauptsächlich zur Erstellung von dynamischen Webseiten oder Webanwendungen verwendet wird.
Plug-Ins	Eine Zusatzsoftware, welche die Grundfunktionen einer Anwendung erweitert. Beispiel: Acrobat Plug-Ins für Internet Browser erlauben die direkte Anzeige von PDF-Dateien.
Point of Sales	Ein POS-Terminal (in der Schweiz EFT/POS-Terminal) ist ein Online-Terminal zum bargeldlosen Bezahlen an einem Verkaufsort (Point of Sale).
Ransomware	Malware, mit der die Besitzer der infizierten Rechner erpresst werden sollen (ransom: englisch für Lösegeld). Typischerweise werden Daten verschlüsselt oder gelöscht und erst nach Lösegeldzahlungen der zur Rettung nötige Schlüssel vom Angreifer zur Verfügung gestellt.
Remote Access Tool (RAT)	Die Fernwartungssoftware (englisch: Remote Administration Tool) stellt eine Anwendung des Konzeptes Fernwartung für beliebige Rechner oder Rechnersysteme dar.
Schadsoftware	Oberbegriff für Software, die schädliche Funktionen auf einem Rechner ausführt (wie beispielsweise Viren, Würmer, Trojanische Pferde).
Schnittstelle	Die Schnittstelle oder das Interface ist der Teil eines Systems, welcher der Kommunikation dient. Siehe Webinterface.
Serial-Port Server	Ein Serial-Port Server ist ein Gerät, welches Daten zwischen einer seriellen Schnittstelle und dem Ethernet transferiert.
sFTP	sFTP ist eine Methode zur Verschlüsselung des File Transfer Protocol (FTP), die im RFC 4217 beschrieben ist.
Sicherheitslücke	Schwachstelle in Hard- oder Software, über die Angreifer Zugriff auf ein System erlangen können.
Sicherheitspatches	Eine Software, die den fehlerhaften Teil eines Programms durch einen fehlerfreien ersetzt und dadurch z.B. eine Sicherheitslücke behebt.
Smart-Meter	Ein Smart-Meter (deutsch: intelligenter Zähler) ist ein Zähler für Energie, der dem jeweiligen Anschlussnutzer den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit anzeigt, die auch an das Energieversorgungsunternehmen

	übertragen werden können.
SMS	Short Message Service Dienst zum Versenden von Kurzmitteilungen (maximal 160 Zeichen) an Mobiltelefonbenutzer.
Spam Score	Punktesystem, das von Filtern genutzt wird, um E-Mails als Spam zu erkennen.
Spam	Unaufgefordert und automatisiert zugesandte Massenwerbung, worunter auch Spam-E-Mails fallen. Als Spammer bezeichnet man den Absender dieser Mitteilungen, während das Versenden selbst als Spamming bezeichnet wird.
Spear-Phishing	Gezielte Phishing Attacke. Dem Opfer wird zum Beispiel vorgegaukelt, mit einer ihr vertrauten Person via E-Mail zu kommunizieren.
SPS	Eine speicherprogrammierbare Steuerung (SPS) ist ein Gerät, das zur Steuerung oder Regelung einer Maschine oder Anlage eingesetzt wird und auf digitaler Basis programmiert wird.
Telephony Denial of Service	Angriff auf die Verfügbarkeit bei Telefonsystemen, vorwiegend bei VoIP.
VoIP Toll Fraud	Missbrauch einer VoIP-Anlage um auf Mehrwertnummern anzurufen, die dem Angreifer gehören.
Virus	Ein selbstreplizierbares, mit schädlichen Funktionen versehenes Computerprogramm, welches sich zur Verbreitung an ein Wirteprogramm oder eine Wirtedatei hängt.
Voice-Phishing	Voice Phishing ist eine Form des Trickbetrugs im Internet und ist von dem englischen Begriff für abfischen (fishing) sowie der Methode der eingesetzten VoIP-Telefonie abgeleitet.
VoIP	Voice over IP Telefonie läuft über das Internet Protokoll (IP). Häufig verwendete Protokolle sind H.323 und SIP.
VPN	Virtual Private Network ermöglicht durch Verschlüsselung des Datenverkehrs eine sichere Kommunikation zwischen Rechnern über öffentliche Netzwerke (z.B. das Internet).
Watering-Hole-Attacken	Gezielte Infektion durch Schadsoftware über Webseiten, welche bevorzugt nur von einer spezifischen Benutzergruppe besucht werden.
Web Application Firewall	Eine Web Application Firewall (WAF) ist ein Ver-

(WAF)	fahren, das Webanwendungen vor Angriffen über das Hypertext Transfer Protocol (HTTP) schützen soll.
Web Hosting	Unter Webhosting oder auch Nethosting versteht man die Bereitstellung von Webspace sowie die Unterbringung (Hosting) von Webseiten auf dem Webserver eines Internet Service Providers.
Webinterface	Das Webinterface ist der Teil eines Systems, welches die Kommunikation zwischen Anwendung und Nutzer meist grafisch bewerkstelligt.
Webserver	Ein Webserver ist ein Server, der Dokumente an Clients wie z. B. Webbrowser überträgt.
QR-Code	Der QR-Code ist ein zweidimensionaler Strichcode und besteht aus einer quadratischen Matrix aus schwarzen und weißen Punkten, die die kodierten Daten binär darstellen.
Zero-Day-Exploit	Sicherheitslücke, für welche noch kein Patch exisitiert.
zip-Datei	zip ist ein Algorithmus und Dateiformat zur Datenkompression, um den Speicherbedarf von Dateien für die Archivierung und Übertragung zu verringern.
Zwei-Faktor Authentifizierung	Dafür sind mindestens zwei der drei Authentifikationsfaktoren notwendig: 1. Etwas, das man weiss (z.B. Passwort, PIN, usw.) 2. Etwas, das man besitzt (z.B. Zertifikat, Token, Streichliste, usw.) 3. Etwas, das man ist (z.B. Fingerabdruck, Retina-Scan, Stimmerkennung, usw.)

7 Anhang

7.1 Analyse einer Android-Schadsoftware, welche gegen Schweizer E-Banking Kunden gerichtet ist

Die Funktionen

- Die Malware leitet SMS an eine mobile Nummer im russischen Sprachraum weiter.
- Das Ziel ist das Stehlen von mTANs.
- Bei der Installation verlangt sie die Berechtigung, SMS zu lesen, zu senden sowie Schreibrechte für die SD Karte.
- Sie tarnt sich als Zertifikatsanwendung von Metaforic.
- Mittlerweile wird die Malware von recht vielen Virenscannern erkannt (Android/TrojanSMS.Agent.NV).

Die Infektion

Die Infektion geschieht in folgenden Schritten:

1. Der Kunde wird von einer Website dazu aufgefordert, eine Anwendung für das Mobilgerät zu installieren. Er muss sein Betriebssystem auswählen.
2. Ein QR-Code wird angezeigt, der auf die Seite mit der effektiven Malware weiterleitet. Die Malware ist ein normales Installationspaket für Android Anwendungen (eine APK Datei).
3. Der Kunde muss gewisse Sicherheitseinstellungen ausgeschaltet haben, damit die Installation funktioniert.
4. Sobald die Installation ausgeführt ist, wird die Malware aktiv und überwacht das Eintreffen von SMS. Die Anwendung selbst tarnt sich als Sicherheitsanwendung.
5. Die SMS werden an eine mobile Telefonnummer in Russland weitergeleitet.

Das Ziel des Angreifers ist es, mTANs abzufangen und diese für Angriffe auf E-Banking Konten zu verwenden.

Die Malware

Die Malware präsentiert sich nach der Installation als Sicherheitsanwendung von Metaforic. Metaforic ist tatsächlich ein Sicherheitsdienstleister, der sich auf Mobilgeräte spezialisiert hat. Es ist nicht nur bei mobiler Malware ein häufig beobachteter Trick, dass sich der Schäd-

ling als vertrauenswürdiges Produkt aus dem Sicherheitsbereich ausgibt, um dem Opfer Vertrauen vorzugaukeln. Auffällig ist die schlechte Übersetzung. Der Benutzer muss ein Passwort (Wort Dordine) wählen und zur Bestätigung erneut eingeben:

Abbildung 7: Eingeblendeter Login-Bildschirm mit Passworteingabe (=Wort Dordine).

Nach der Installation der Malware gibt die Anwendung vor, ein Zertifikat erfolgreich erstellt zu haben.

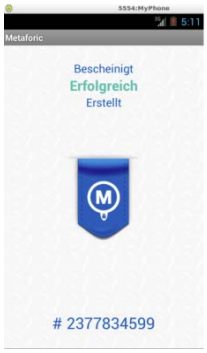


Abbildung 8: Bestätigung der Zertifikatsinstallation.

Die Malware verlangt auf dem Smartphone folgende Berechtigungen:

```
In [19]: a.get_permissions()
Out[19]:
['android.permission.WRITE_EXTERNAL_STORAGE',
 'android.permission.RECEIVE_SMS',
 'android.permission.SEND_SMS']
```

Abbildung 9: Berechtigungsvergabe der Malware

Insbesondere die Tatsache, dass eine Anwendung Rechte für das Lesen und Versenden von SMS verlangt, deutet darauf hin, dass diese keine guten Absichten hat. Im Hintergrund läuft die Anwendung mit folgendem Prozess:

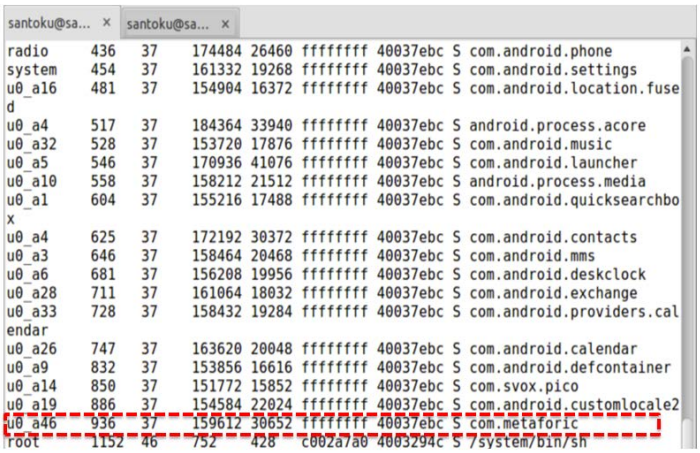


Abbildung 10: Rot gekennzeichnet ist der Prozess der Malware, der im Hintergrund läuft.

Der Programm Code lässt folgende Schlussfolgerungen zu:

- Die Anwendung war ursprünglich auf Holländisch verfasst worden und nachträglich teilweise (mehr schlecht als recht) auf Deutsch übersetzt worden.

- Die Nummer, an welche die gestohlenen SMS übermittelt wurden, steht im Klartext in der Malware drin. Die Nummer ist im russischen Sprachraum lokalisierbar.

```
geben Sie das Passwort
Passwort best
tigen
Metaforic
Ya TuT :)
Wachtwoord komen niet overeen
^L^L+[redacted]
^L^LVerladung...
Wort Dordine:
^LBest
tigen:
Zertifikat erstellen
Erstellen eines Zertifikats...
Bescheinigt
Erfolgreich
Erstellt
```

Abbildung 11: Quelltext mit einprogrammierter Telefonnummer an welche das abgefangene SMS weitergeleitet werden sollen.

Android Anwendungen sind immer digital signiert. In diesem Fall wurde die Anwendung mit einem Debug Certificate signiert, was keine Verteilung via offiziellen Appstore erlaubt und dessen Einsatz eigentlich ausschliesslich für das Entwickeln und Testen von Android Anwendungen reserviert ist.

Generell ist die Malware sehr einfach aufgebaut und verfügt weder über eine Rootkit Funktionalität, um sich zu verbergen, noch enthält sie Verschlüsselung oder Obfuskation, um eine Analyse zu erschweren. Sie dient einzig und alleine dem Zweck, mTANs zu stehlen. Es gibt eine Vielzahl vergleichbarer Trojaner für die Android Plattform. Die Erkennungsrate für die Malware durch die diversen Virenscanner war am Anfang sehr schlecht, stieg aber danach auf knapp 50% an (Stand: Anfang Juli 2013).