Cyber Security 2017:
Data Breaches & Bug Bounties

Autor: Swisscom Security
Dieser Report wurde durch die enge Zusammenarbeit zwischen Swisscom Security mit weiteren Betriebseinheiten realisiert.

April 2017

Inhaltsverzeichnis

1 Einleitung

In den vergangenen zwei Jahrzehnten wurden durch die Entwicklung von neuen Technologien und insbesondere durch das Internet unglaubliche Möglichkeiten geschaffen, die unser privates wie auch geschäftliches Leben nachhaltig verändert haben und weiter verändern werden. Internet-Sicherheit ist deshalb zu einem kritischen Faktor geworden und wird in dem Masse an Bedeutung gewinnen, in dem Menschen und Geräte zunehmend miteinander verbunden werden. Das Umfeld der Internet-Sicherheit ist geprägt durch rasante Entwicklungen und Veränderungen an der Schnittstelle von Technologie, Wirtschaft und Gesellschaft. Verschiedene Themen im Bereich Cyber-Security haben im vergangenen Jahr wiederum grosse Aufmerksamkeit erregt. Die prominentesten Beispiele sind Distributed Denial of Service (DDoS) Angriffe mit Millionen von Internet of Things (IoT) Geräten[1], anhaltende Angriffswellen von Malware, welche alle Daten der Opfer (Private wie auch Firmen) verschlüsseln und nur gegen Bezahlung wieder freigeben («Ransomware»), Datenlecks mit Millionen von betroffenen Nutzerkonten und politischen Implikationen, sowie die anhaltende Flut von Schwachstellen in Software.

Gegen viele aktuelle Cyber-Bedrohungen gibt es bereits erfolgsversprechende Gegenmassnahmen, sowohl technischer wie auch organisatorischer Natur. Oft kommen bereits bekannte Lösungsansätze jedoch nicht zum Einsatz, sei es aus Unkenntnis der Lösung, Unsicherheit und mangelnder Erfahrung mit neuen Ansätzen oder auch fehlendem Verständnis der Auswirkungen und Zusammenhänge der Bedrohung.

In diesem Bericht beleuchten wir aus Sicht von Swisscom die anhaltenden Cyber-Bedrohungen durch Software-Schwachstellen sowie von massiven Datenlecks und deren Auswirkungen auf die Schweiz. Wir wollen das Verständnis zu diesen Bedrohungen und deren Auswirkungen stärken, Gegenmassnahmen aufzeigen und eigene Erfahrungen mit innovativen Lösungsansätzen teilen. Damit hoffen wir einen Beitrag zur gemeinsamen Bewältigung der Cyber-Risiken in der Schweiz leisten zu können.

Ferner wollen wir mit dieser Publikation einen Einblick in unser Bug-Bounty-Programm geben. Unsere Erfahrungen mit Bug Bounty sind sehr positiv und wir möchten weitere Unternehmen in der Schweiz ermutigen, ebenfalls diesen Schritt zur Erhöhung der Sicherheit zu wagen.

2 Lagebild – Bedrohungsradar

Der Ursprung von Bedrohungen findet sich in der stetigen Entwicklung von neuen Technologien und deren Anwendung und Verbreitung in der Gesellschaft. Potenzielle Bedrohungen gilt es frühzeitig zu erkennen und systematisch zu erfassen. Um die Bedrohungslage und deren Evolution abzubilden, verwenden wir einen Radar (Abbildung 1).

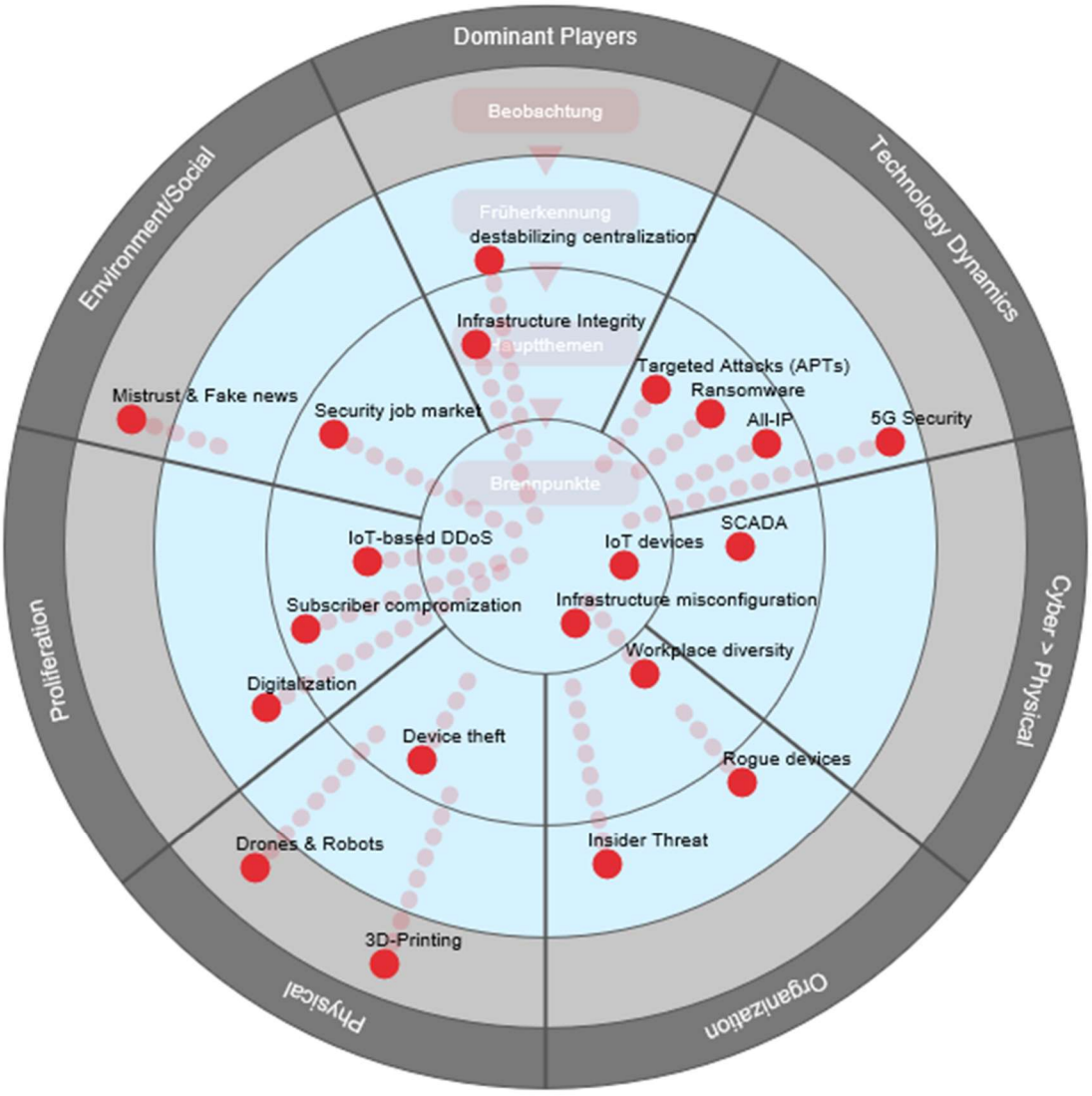

Abbildung 1 – Bedrohungs-Radar

2.1 Methodik

Der Bedrohungsradar ist in sieben Segmente unterteilt, die die unterschiedlichen Domänen der Bedrohungen voneinander abgrenzen. In jedem Segment können die dazugehörenden Bedrohungen in einem von vier konzentrischen Ringen zugeordnet werden. Die Kreise zeigen die Aktualität der Bedrohung an und damit auch die

Unschärfe, die in der Beurteilung der Bedrohung liegt. Je näher dem Kreismittelpunkt die Bedrohung verortet ist, desto konkreter ist sie und umso wichtiger sind angemessene Gegenmassnahmen. Die Ringe kennzeichnen wir als

- **Brennpunkte** für Bedrohungen, die bereits real sind und mit relativ grossem Einsatz von Ressourcen gemanaged werden.
- **Hauptthemen** für Bedrohungen, die bereits vereinzelt eingetreten sind und mit normalem Ressourcen-Einsatz gemanaged werden. Oft bestehen geregelte Prozesse, um derartigen Bedrohungen effizient zu begegnen.
- **Früherkennung** für Bedrohungen, die noch nicht eingetreten sind oder aktuell nur sehr wenig Wirkung zeigen. Es wurden Projekte gestartet, um der zukünftig wachsenden Bedeutung dieser Bedrohungen frühzeitig begegnen zu können.
- **Beobachtung** für Bedrohungen, die erst in einigen Jahren eintreten werden. Es gibt keine konkreten Massnahmen für den Umgang mit diesen Bedrohungen.

Weiter weisen die einzelnen, durch benannte Punkte gekennzeichneten Bedrohungen einen Trend auf. Dieser kann in seiner Kritikalität zunehmend, rückläufig oder stabil sein. Die Länge des Trend-Strahls zeigt die erwartete Schnelligkeit auf, mit der sich die Kritikalität der Bedrohung ändern wird.

2.2 Bedrohungen

2.2.1 Dominant players

Bedrohungen, die von Abhängigkeiten von dominanten Herstellern, Diensten oder Protokollen ausgehen.

Hauptthemen	**Infrastructure Integrity:** Wesentliche Komponenten kritischer Infrastrukturen können fahrlässig oder bewusst Schwachstellen eingebaut haben, die die System-Sicherheit gefährden.
Früherkennung	**Destabilizing Centralization:** Starke Zentralisierung in der Struktur des Internets führt zu Klumpenrisiken. Der Ausfall eines Services kann weltweit Auswirkungen haben, wie zum Bespiel bei einem Ausfall von Amazon Web Services (AWS).

2.2.2 Technology dynamics

Bedrohungen, die von der rasanten technologischen Innovation ausgehen und damit einerseits den Angreifern neue Möglichkeiten geben, andererseits durch die Entwicklung selber neue Bedrohungen schaffen.

Hauptthemen	**Targeted attacks (APTs):** Schlüsselpersonen werden identifziert und gezielt angegriffen, um relevante Informationen zu erhalten oder maximalen Schaden anzurichten. **Ransomware:** Kritische Daten werden grossflächig verschlüsselt und gegen Lösegeld (möglicherweise) wieder entschlüsselt. **All-IP:** Im Zuge der flächendeckenden All-IP Einführung steigen Risiken im Zusammenhang mit der VoIP-Technologie.
Früherkennung	**5G Security:** 5G ist eine noch junge Technologie, die Einführung wird neben vielen Chancen auch noch unbekannte Bedrohungen mit sich bringen.

2.2.3 Cyber goes physical

Angriffe über die Infrastruktur im Cyberspace werden vermehrt Schaden in der physischen Welt verursachen.

Brennpunkt	**IoT Devices:** Schwach geschützte Geräte können kompromittiert und sabotiert werden. So können sie in der eigenen Funktion, z. B. der Verfügbarkeit oder Datenintegrität eingeschränkt werden.
Hauptthemen	**SCADA:** Es existieren nach wie vor viele schlecht oder gar nicht geschützte Kontrollsysteme für Anlagen der kritischen Infrastruktur.

2.2.4 Organization

Bedrohungen, die von Veränderungen in Organisationen ausgehen oder Schwächen in Organisationen ausnutzen.

Brennpunkt	**Infrastructure misconfiguration:** Ausnutzung fehlkonfigurierter Infrastruktur-Komponenten und/oder von Schwachstellen, die spät identifiziert und behoben werden.
Hauptthemen	**Workplace diversity:** Neben den vielen Chancen, die neue Arbeitsmodelle mit sich bringen, führt der unkontrollierte Einsatz solcher Modelle, wie z. B. «Bring your own Device» (BYOD) oder verstärkter Einsatz von Remote-Arbeitsplätzen zu einer grösseren Risiko-Exposition.
Früherkennung	**Rogue devices:** Unbekannte Geräte im Firmennetz können direkt Angriffe durchführen oder aufgrund schlechten Schutzes für Angriffe ausgenutzt werden. **Insider threat:** Partner oder Mitarbeitende manipulieren, missbrauchen oder verkaufen Informationen fahrlässig oder vorsätzlich.

2.2.5 Physical

Bedrohungen, die von der physischen Umgebung ausgehen und in der Regel eher auf physische Ziele ausgerichtet sind.

Hauptthemen	**Device theft:** Der Diebstahl insbesondere von Komponenten der kritischen Infrastruktur oder zukünftig mehr von IoT-Geräten kann zum Datenverlust führen oder die Verfügbarkeit der Services beeinträchtigen.
Früherkennung	**Drones and Robots:** Aufklärung oder Angriffe über weite Entfernungen werden einfacher und günstiger. **3D-Printing:** Die Herstellung von z. B. Schlüsseln oder anderen physischen Geräten wird mit der besseren Qualität der 3D-Drucker günstiger und einfacher.

2.2.6 Proliferation

Bedrohungen, die von der immer einfacheren und günstigeren Verfügbarkeit von IT-Medien und Know-how profitieren. Einerseits, weil die Verbreitung zu mehr Angriffsflächen führt und andererseits, weil sie die Verfügbarkeit von Angriffswerkzeugen erhöht.

Hauptthemen	**IoT-based DDoS:** Starkes Wachstum bei geringem Schutz von IoT-Geräten führt zu mehr "Übernahme-Kandidaten" für Botnetze. **Subscriber compromization:** Schadsoftware greift private Daten der Mobile-Nuzter an oder wird für Angriffe auf die Telekommunikations- bzw. IT-Infrastruktur genutzt.
Früherkennung	**Digitalization:** Immer stärkere Vernetzung der realen und virtuellen Welt und von Privat- und Geschäftsleben führt zu mehr Angriffswegen.

2.2.7 Environmental / Social

Bedrohungen, die von gesellschaftlich-politischen Änderungen ausgehen oder durch solche Änderungen für Angreifer einfacher oder wertvoller werden.

Hauptthemen	**Security job market:** Der Bedarf an Security-Professionals kann nur sehr schwer gedeckt werden, was weniger Know-how im Einsatz gegen immer komplexere und intelligentere Angriffe zur Folge hat.
Früherkennung	**Mistrust & fake news:** Schwindendes Vertrauen gegenüber staatlichen oder gesellschaftlichen Stellen kann dazu führen, dass der Informationsaustausch zur Identifikation und Abwehr potentieller Angriffe reduziert wird.

2.3 Fazit

Unser Lagebild zeigt, dass die Bedrohungslage komplexer wird. Angreifer profitieren vom steigenden Wert der schützenswerten Assets, was die Motivation für einen gezielten und intelligenten Angriff erhöht. Weiter schaffen technische Innovationen und das Zusammenwachsen der physischen und virtuellen Welt neue Angriffsmöglichkeiten. Gesellschaftliche Veränderungen haben Wirkung auf das Vertrauen untereinander und auf die Art, wie wir zusammen arbeiten. Beides können Angreifer für ihre Zwecke nutzen.

Sicherheitsfunktionen, die mit dem Schutz von Personen, Daten und Anlagen beauftragt sind, können diese gesellschaftlichen und technologischen Veränderungen gleichwohl nutzen, um die Angriffe gezielt und effizient abzuwehren.

Swisscom Security interpretiert das Lagebild als weiterhin anspruchsvoll mit immer neuen Herausforderungen, die aber dank geeigneter Massnahmen gemeistert werden können.

3 Datendiebstahl („Data Breaches“)

Durch die zunehmende Digitalisierung unserer Gesellschaft und Wirtschaft entstehen in Unternehmen, bei Behörden sowie bei Privatpersonen fortwährend grössere und kritischere Datensammlungen aller Art. Wenig überraschend hat sich die seit Jahren anhaltende Serie von massiven Datendiebstählen (im folgenden “Data Breach” bezeichnet) im Jahr 2016 eindrücklich fortgesetzt. In der Vergangenheit wurden Data Breaches lediglich als Problem der betroffenen Firma und deren Kunden angesehen. Im vergangenen Jahr wurden jedoch die Auswirkungen auf die Entwicklung von Gesellschaft und Politik deutlich aufgezeigt. In der Folge betrachten wir die von Data Breaches ausgehenden Risiken aus Sicht der Gesellschaft, von Swisscom und des Benutzers um die Auswirkungen auf Schweizer Benutzer und Firmen abzuschätzen. Diese Risikobetrachtung unterlegen wir einer Analyse von aktuellen Daten aus sieben grossen Data Breaches mit über 890 Millionen betroffenen Nutzerkonten.
Der bekannteste Data Breach Monitoring Dienst haveibeenpwned.com (HIBP) listet derzeit über 2 Milliarden gestohlene Nutzerkonten aus 187 bestätigten Data Breaches der letzten Jahre.[2]

3.1 Schweizer Konten in Data Breaches

Zur Veranschaulichung der Gefährdung für Schweizer Benutzer haben wir die frei verfügbaren Daten von sieben grösseren Data Breaches der jüngsten Vergangenheit ausgewertet. Die Tabelle in Abbildung 2 zeigt für unterschiedliche Industriesektoren und Behörden der Schweiz die Anzahl Benutzerkonten welche durch die Data Breaches von *Adobe, Ashley-Madison, Badoo, Dropbox, Gawker, Linkedin* und *MySpace* exponiert wurden. Insgesamt wurden durch diese sieben Data Breaches 890 Millionen Nutzerkonten exponiert.

Kategorie	Total	Adobe	Ashley-Madison	Badoo	Dropbox	Gawker	LinkedIn	MySpace	mehrfach Breach
Datum Einbruch		Oct 2013	Jul 2015	Jun 2013	Jul 2012	Dec 2010	May 2012	Jul 2008	
Datum Publikation		Dec 2013	Aug 2015	Jul 2016	Aug 2016	Dec 2013	May 2016	May 2016	
Total Nutzerkonten (Mio)		**152.4**	**30.8**	**112.0**	**68.6**	**1.2**	**164.6**	**359.4**	
Firmenindex									
Fortune 500 (International)	2'958'767	441'355	46'143	999'781	200'325	1'039	743'295	616'274	3%
Beratung (Big 6, International)	89'672	24'737	207	2'207	15'925	39	48'038	4'611	7%
Swiss Market Index SMI	70'280	9'180	209	3'832	7'402	9	35'421	17'021	4%
Industriezweige - Schweiz									
Banken	18'565	2'792	53	512	1'100	22	13'831	677	2%
Versicherungen	5'921	936	44	671	584	1	3'595	309	4%
Energieunternehmen	6'107	1'622	34	466	2'061	1	2'214	213	8%
Pharma/Chemie	2'988	519	18	174	351	1	1'917	127	4%
Medien - Schweiz									
Printmedien	599	193	10	36	216	0	118	84	10%
Fernsehen & Radio	93	23	2	18	28	0	22	14	16%
Verwaltung - Schweiz									
Bundesverwaltung	3'070	907	28	532	545	1	1'123	89	5%
Kantonsverwaltung	7'963	2'276	45	1'622	2'453	0	1'867	188	6%
Bundesbetriebe	4'680	1'222	42	832	1'384	0	1'385	124	7%
Hoch- & Fachhochschulen	66'124	16'794	153	2'937	43'708	6	6'905	2'431	11%
Mailprovider - Schweiz									
Maildienste	291'277	84'242	28'875	110'834	56'317	42	12'769	43'458	16%
Internet Provider (ISP)	547'796	241'725	19'234	148'319	118'277	66	54'290	54'731	17%

Abbildung 2 – Anzahl durch Data Breaches exponierte Benutzerkonten für unterschiedliche Industriesektoren in der Schweiz

Für diese Analyse wurden die Domainnamen der Nutzerkonten aus den Data Breaches mit den Domainnamen der Organisationen aus den unterschiedlichen Sektoren abgeglichen. Die letzte Spalte in Abbildung 2 zeigt zudem, wieviele der Nutzerkonten bei mehr als einem Data Breach kompromittiert wurden. Diese Zahlen sind eine Minimalabschätzung, da wir nur die Daten von sieben Data Breaches analysiert haben, während HIBP derzeit 187 bestätigte grössere Data Breaches auflistet.

Die Analyse zeigt auch, dass Behörden und Verwaltungen ebenso von diesen Data Breaches betroffen sind wie Grossfirmen, kritische Infrastrukturprovider, Hochschulen oder private Benutzer. Der Sektor «Mailprovider Schweiz» fasst die Nutzerkonten der zwölf grössten Schweizer Internet Service Provider und der bekannten Freemail-Portale hotmail.ch, gmx.ch und gmail.ch zusammen. Dieser Sektor repräsentiert damit die Mehrheit der privaten schweizerischen Mailkonten, wovon mindestens 800'000 von Data Breaches betroffenen sind.

3.2 Die Risiken der «Passwort vergessen» Funktion

Man könnte argumentieren, dass sich der Schaden durch die Data Breaches von LinkedIn und MySpace für die Betroffenen in Grenzen hält – handelt es sich doch um Social Media Portale auf denen man freiwillig Daten preisgibt. Bei Dropbox als Cloud-Speicherlösung sieht dies schon ganz anders aus. Auf jedem Fall greift diese einfache

Betrachtung zu kurz, wenn man berücksichtigt, dass ein Grossteil der Benutzer dasselbe Passwort bei unterschiedlichen Internetdiensten wiederverwendet. Kritisch wird die Situation, wenn Passwörter auch für E-Mail-Konten wiederverwendet werden. Ist ein solches E-Mail-Konto bei weiteren Internet-Diensten als Kontakt hinterlegt, wird durch die Funktion «Passwort vergessen» ein neues Passwort direkt an diese E-Mail-Adresse gesandt, und somit in die Hände des Angreifers gespielt. In der Folge hat der Angreifer nicht nur Zugriff auf das Mailkonto des Opfers, er kann sich daduch auch den Zugriff auf weitere Dienste des Kunden beschaffen. Die lange Zeitspanne zwischen dem tatsächlichen Einbruch und dem Bekanntwerden ist fatal – die Auswirkungen sind global, auch für Benutzer aus der Schweiz.
Das folgende Beispiel illustriert, dass dieses Risiko sehr real ist. Gegen Ende August 2016 mehrten sich in der Security Community Stimmen, dass die Daten von Dropbox in einschlägigen Foren im Untergrund gehandelt werden. Kurz danach waren die Daten im Internet frei verfügbar. Am 8. September verzeichnete Swisscom auf den Mailservern von Bluewin an einem einzelnen Tag über 10’000 verdächtige, jedoch erfolgreiche Logins von einer einzigen IP-Adresse aus dem Ausland. Abbildung 3 zeigt diese Aktivität dieses Tages eindrücklich.

Abbildung 3 – Anzahl verdächtige Anmeldungen auf den Mailservern von bluewin 2016

Die IP-Adresse von der die Anmeldungen ausgingen wurde sofort blockiert, die bereits betroffenen 10'000 Mailkonten wurden gesperrt und die Benutzer informiert. Swisscom hat im Zeitraum März bis Dezember 2016 insgesamt 83’928 Sperrungen (inklusive Mehrfachsperrungen) von 74’602 unterschiedlichen Mailadressen vorgenommen. Etwa die Hälfte oder 34’892 dieser Mailadressen wurden durch einen oder mehrere Data Breaches exponiert.
Dieses Ereignis dokumentiert das systematische wie auch schnelle Vorgehen von Kriminellen nach einem Data Breach, wie auch deren Fähigkeit im Cracken von Passwörtern (oder die Schwierigkeit von Nutzern, starke und unterschiedliche Passwörter zu wählen).
Der effektive Schutz von Passwörtern durch Hashing hängt erheblich von folgenden, durch den Benutzer oder den Betreiber kontrollierten Kriterien ab:

Benutzer	> Länge des Passworts > Mögliche Zeichen zur Bildung des Passworts > Unvorhersehbarkeit des Passworts
Betreiber	> Wahl der eingesetzten Hash-Funktion > Zugelassene Zeichen zur Bildung des Passworts > Minimal und/oder Maximallänge des Passwortes > Sichere Implementation

Unterschiedliche Analysen von Passwörtern aus den grössten Data Breaches der Vergangenheit zeigen leider wiederkehrend das gleiche Bild[3]:

> Die meisten Passwörter sind zu kurz, zu einfach und damit vorhersehbar. Die Liste der meistgewählten Passwörter ändert sich kaum über die Zeit: «123456», «password», «12345», «12345678», «qwerty» sind die Top 5.
> Benutzer verwenden eine kleine Zahl von Passwörtern für eine grosse Zahl von unterschiedlichen Diensten. Im Durchschnitt werden sechs unterschiedliche Passwörter für 24 Dienste verwendet.

3.3 Stationen gestohlener Daten

Je nach Angreifer durchlaufen die Daten nach einem erfolgten Einbruch unterschiedliche Stationen. In erster Linie werden die Daten zuerst durch die Angreifer selbst gesichtet, ausgewertet und verwertet – ohne irgendwelche Publizität gegen aussen. Hält die Kompromittierung des Ziels an, so hat der Angreifer ein grosses Interesse den Data Breach möglichst lange geheim zu halten, um den Zugang zum Opfer nicht zu gefährden. Zur Maximierung des Profits bieten sich weiter folgende Optionen an:

> die Daten werden in einem Untergrund-Markt zum Verkauf angeboten
> die betroffene Firma wird erpresst, es wird mit der Publikation der Daten gedroht
> die Daten werden im Internet frei zugänglich publiziert

Diese Optionen kommen zum Zug, falls der Angreifer die Daten nicht selbst verwerten kann oder will, die Auswertung beendet und das Primärziel erreicht wurde, oder der Einbruch durch Dritte oder die betroffene Organisation detektiert wurde.
Staatliche Akteure werden die Daten entweder ausschliesslich selbst verwerten, oder aber zu einem bestimmten Zeitpunkt auf geeigneten Kanälen publizieren, um politischen Profit daraus zu erzielen. Typischerweise vergeht eine lange Zeit zwischen dem Einbruch und dem Zeitpunkt, an dem die Betroffenen (das Unternehmen oder die Kunden) von einem Data Breach erfahren.
Oft werden die Daten vieler Data Breaches irgendwann auch im Internet frei verfügbar und für jederman zugänglich, teilweise begleitet mit viel Publizität.

Unterdessen bieten mehrere Organisationen Dienste an, welche Kunden alarmieren, wenn deren Daten im Internet oder Untergrund verfügbar gemacht werden[4]. Oder weniger seriöse Organisationen bieten die gesamten Daten eines Data Breaches als sogenannten "Data Dump" jedem zahlenden Kunden zum Download an – inklusive der gecrackten Passwörter. Die Zeitspanne zwischen dem tatsächlichen Einbruch und der ersten Publikation des Einbruchs (z. B. Bekanntmachung des Data Breaches durch die betroffene Firma selbst, oder aber durch Dritte) kann mitunter Jahre dauern.

3.4 Auswirkungen auf Gesellschaft und Wirtschaft

Neben der primären Verwertung von gestohlenen Daten für Spionage und Identitätsdiebstahl zum Schaden der Direktbetroffenen, zeigen die Data Breaches von 2016 eine neue Dimension der Gefährdung. Folgende Ereignisse haben die Auswirkungen von Data Breaches auf den Lauf der Geschichte und die Entwicklung der Gesellschaft deutlich aufgezeigt:

Panama Leaks / Mossack Fonseca

Über 11.5 Millionen vertrauliche Dokumente der Anwaltskanzlei Mossack Fonseca aus den Jahren 1970 bis 2015 gelangen im April 2016 an die Medien[5]. Nach Einschätzung der beteiligten Medien belegen die Unterlagen legale Strategien der Steuervermeidung, aber auch Steuer- und Geldwäschedelikte, den Bruch von UN-Sanktionen sowie andere Straftaten durch Kunden von Mossack Fonseca. Zu den durch den Data Breach identifizierten Kunden zählen zahlreiche Prominente aus aller Welt, darunter 143 Politiker, frühere und noch amtierende Staats- und Regierungschefs. Das Datenleck bei Mossack Fonesca hatte für einige Kunden weitreichende Folgen, das prominenteste Beispiel ist der Rücktritt des isländischen Ministerpräsidenten nach Massenprotesten in Folge der Bekanntmachungen durch die Panama Papers.

Wahlkampf in den USA

Während des U.S. Wahlkampfs wird die Gesellschaft mit Interna aus dem Leak des Democratic National Committee (DNC) Netzwerkes und internen E-Mails des Kampagnenleiters John Podesta überflutet[6]. Die Informationen dokumentieren die mannigfaltigen Verflechtungen zwischen Politik, Wall Street und internen Seilschaften in der Demokratischen Partei – mit potentiellem Einfluss auf die Wahl.

Durch den Missbrauch von vertrauchlichen Dokumenten kann eine Zielperson offen oder verdeckt beeinflusst, manipuliert oder gar erpresst werden. Werden auf diese Weise Prominente, Wirtschaftsführer oder Politiker in ihren Entscheiden und Aktionen beeinflusst, sind die Folgen für die Wirtschaft oder Gesellschaft potentiel weitreichend. Die Manipulation ist schwer nachweisbar und erfolgt verdeckt. Der Einbruch bei Mossack Fonseca war aufgrund der grob vernachlässigten Sicherheit

der technischen Systeme trivial, während hinter dem Einbruch ins DNC-Netzwerk das anspruchsvolle Werk der russischen Geheimdienste vermutet wird.

Wir müssen in der Folge davon ausgehen, dass sowohl Geheimdienste wie auch Cyber-Kriminelle bereits seit langem (und auch heute) im Besitz kritischer Daten weiterer Organisationen sind und diese verdeckt für ihre Zwecke ausnutzen, die Manipulation von Entscheidungsträgern und Politikern eingeschlossen.

Der Schutz gegen solche Risiken ist aufwändig und bedingt viel Disziplin, sowohl im Aufbau und Betrieb der IT-Infrastruktuer als auch in der täglichen Arbeit der Mitarbeitenden. Die Güterabwägung zwischen Sicherheit und Arbeitskomfort hat sorgfältig zu erfolgen und muss gut kommuniziert und verstanden sein. Es zeigt sich immer wieder, dass Benutzer, meist aus nachvollziehbar eigenem Interesse, sehr kreativ sind in der Umgehung von Auflagen und technischen Schutzmassnahmen.

4 Bug-Bounty-Programm

Software hat sich in den letzten Jahrzehnten zu einem tragenden und kritischen Element für unsere Wirtschaft wie auch Gesellschaft entwickelt. Durch die fortschreitende Vernetzung im Internet kommuniziert Software heute ununterbrochen in allen Arten von Geräten mit Menschen und Maschinen – und ermöglicht somit die digitale Gesellschaft. Trotz enormen Investitionen der Industrie und Forschung in die Entwicklung sicherer Software, sind Schwachstellen oder Sicherheitslücken ein dauerhaftes Problem. Durch das Ausnutzen von Schwachstellen in Software kann ein Angreifer die betroffenen Systeme oder Dienste kompromittieren, manipulieren, kontrollieren, ausspionieren oder sabotieren. Weiter zeigt die Geschichte des Internets unverkennbar, dass das Entdecken von Sicherheitslücken in Software durch den Hersteller, den Benutzer oder gar durch den Staat weder verhindert, noch unterbunden werden kann. Nicht überraschend ist das Interesse an kritischen Softwareschwachstellen in den letzten Jahren beachtlich gestiegen, besonders bei Kriminellen (Profit) oder staatlichen Akteuren (Spionage, Sabotage). Entsprechend ist ein Markt entstanden, der hohe Preise für kritische Softwareschwachstellen bietet.[7] Die Firma Zerodium bietet beispielsweise über eine Million USD für eine Schwachstelle, die es erlaubt Apple-Mobilgeräte zu kompromittieren[8].

4.1 Grenzen des Altruismus

Glücklicherweise verhalten sich viele Entdecker von Schwachstellen ethisch und folgen dem sogenannten «Coordinated Disclosure» Prozess[9]. Der Entdecker meldet die Schwachstelle dem Hersteller und gibt diesem Zeit zur Entwicklung eines Security Patches, bevor er die Schwachstelle publiziert. Dies bedingt jedoch, dass der Entdecker auf Profit durch den Verkauf der Schwachstelle verzichtet. Im Lichte der rasanten Entwicklung des Marktes für Software-Schwachstellen mit immer höheren Preisen kommt dieses Model jedoch vermehrt unter Druck. Weiter ist es bedenklich, dass die Cyber-Sicherheit der Gesellschaft massgeblich und immer mehr vom altruistischen Verhalten von Entdeckern abhängt.

In der Industrie setzt sich allmählich die Erkenntnis durch, Entdecker von Schwachstellen für ihr ethisches Verhalten zu belohnen. In sogenannten Bug-Bounty-Programmen bieten ihnen Unternehmen für das Melden von Schwachstellen in Produkten oder Diensten Preisgelder, sogenannte (Bug) Bounties. Grosse Software-Hersteller sind mit diesem Modell vorangegangen. Die Erfahrungen mit Bug Bounties sind sowohl finanziell wie auch aus Sicht der Sicherheit positiv, wie eine umfassende Studie der Bug-Bounty-Programme von Google und Mozilla zeigte[10]. Langsam aber sicher entwickeln sich Bug-Bounty-Programme von einer Ausnahme zur Norm – die aktuelle «The Bug Bounty List» von BugCrowd belegt dies eindrücklich mit derzeit gegen 500 eingetragenen Firmen mit einem Bug-Bounty-Programm[11].

4.2 Das Swisscom Bug-Bounty-Program

Swisscom betreibt seit September 2015 als erstes grosses Unternehmen in der Schweiz ein eigenes Bug-Bounty-Programm, welches durch unser «Computer Security Incident Response Team» (CSIRT) verantwortet wird[12]. Das Bug-Bounty-Programm wurde mit folgenden Zielen gestartet:

- Zentrale Anlaufstelle für Schwachstellenmeldungen schaffen
- Anreize schaffen, gefundene Schwachstellen uns direkt zu melden
- Optimierte Prozesse zur Behandlung von Schwachstellen schaffen (interne wie auch externe Prozesse)
- Transparenz bezüglich Sicherheitslücken, welche unsere Infrastruktur betreffen (Reality Check)
- Unterstützung des kontinuierlichen Härtungsprozesses unserer Infrastruktur

Mit dem Bug-Bounty-Programm wollen wir die Entdecker für ihre Aufwände im Zusammenhang mit der Berichterstattung und Dokumentation der Schwachstelle belohnen. Alle Aktivitäten die im Zusammenhang der Entdeckung der Schwachstelle stehen, müssen sich im legalen Rahmen abspielen und dürfen den Betrieb unserer kritischen Infrastruktur nicht beeinträchtigen.

4.3 Bewertung einer Schwachstelle

Die Höhe der Bounty (Preisgeld) bemisst sich anhand des Risikos durch die Schwachstelle, und nicht an der technischen Art oder Komplexität der Schwachstelle. Beispielsweise wird eine «SQL Injection» Schwachstelle höher abgegolten, wenn durch diese sensitive Daten exponiert werden als bei unkritischen Daten. Die Preisspanne unseres Bug-Bounty-Programms liegt zwischen 150 CHF und 10’000 CHF pro Schwachstelle.

4.4 Bug-Bounty-Meldungen

Im Jahr 2016 sind durch das Swisscom Bug-Bounty-Programm 281 Meldungen von 54 Entdeckern eingegangen, die von Swisscom eingesetzte Produkte oder Dienste betreffen. Von diesen haben sich bisher mehr als die Hälfte (157) der Schwachstellen für eine Bounty qualifiziert. Der Grossteil der Schwachstellen, etwa 75%, betreffen diverse Web-Applikationen. Die folgende Tabelle zeigt die Verteilung der eingegangenen Schwachstellen nach Kritikalität.

Kritikalität	Anzahl	Art und Auswirkung
Hoch	1	> Kritische Schwachstellen in weit verbreiteten Kundengeräten > Kritische Schwachstellen in Authentisierungsfunktionen > Remote Code Execution
Mittel	14	> Nur bedingt ausnutzbare Schwachstellen in Kundengeräten > SQL Injection ohne Exponierung sensitiver Daten > Cross Site Scripting (XSS) auf hochfrequentierten Webseiten
Tief	142	> Cross-Site-Scripting (XSS) in unkritischen Applikationen > Exponierung von nicht sensitiven Daten

Insgesamt wurden im letzten Jahr im Rahmen des Bug-Bounty-Programms ca. 50'000 CHF an Entdecker aus elf unterschiedlichen Ländern von vier Kontinenten ausbezahlt.

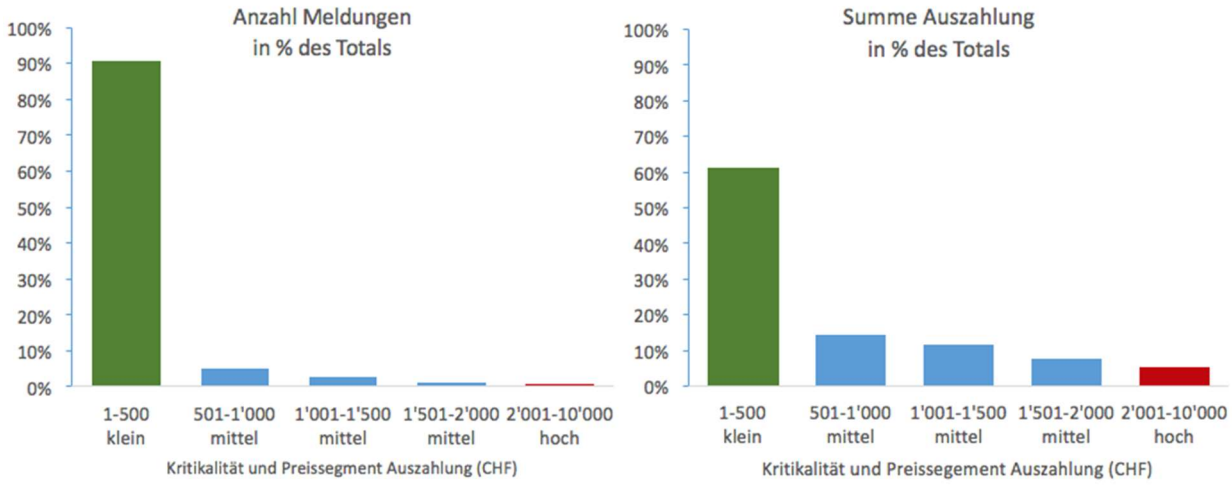

Abbildung 4 – Prozentsatz der Auszahlungen und Anzahl Meldungen pro Preissegment

Für das Jahr 2016 zeigt Abbildung 4 das Verhältnis von Bounty Auszahlungen und der Anzahl Meldungen in unterschiedlichen Preissegmenten.

> Im Segment der weniger kritischen Schwachstellen (Bounty zwischen 1 bis 500 CHF) finden sich 90% der Schwachstellen für welche 60% der Gesamtsumme ausgegeben wurde. Die überragende Mehrheit dieser Schwachstellen betreffen diverse Web-Applikationen, meist kleine Spezialapplikationen für individuelle Projekte. Die Komplexität der Schwachstelle und deren Behebung ist oft nicht gross (z.B. Behebung durch eine Konfigurationsänderung). Dank dem Bug-

Bounty-Programm werden solche «Altlasten» nun rasch identifiziert und behoben.

> Im Segment der kritischen Schwachstellen (Bounty ab 2'000 CHF) finden sich ein paar wenige, dafür den Entdeckern gut bezahlte Meldungen zu Schwachstellen. Das Schadenspotential bei Missbrauch der Schwachstelle ist hoch bis sehr hoch. In diese Kategorie fällt unter anderem eine Schwachstelle im Internet Router von Kunden.

4.5 Erfahrungen

Durch das noch junge Bug-Bounty-Programm wurden bereits in kurzer Zeit wichtige Erkenntnisse gewonnen und die Sicherheit unserer Infrastruktur weiter erhöht:

> Die Effektivität der internen Security-Initiativen wird messbar:
Swisscom intern entwickelte Software weist deutlich weniger Schwachstellen auf als eingekaufte Software. Unsere Investitionen in die sichere Software-Entwicklung gehen Hand in Hand mit dem Bug-Bounty-Programm.
> Bereiche mit Nachholbedarf und solche mit hohem Sicherheitsniveau werden klar erkannt.
> Das Bewusstsein für Sicherheit im Unternehmen wird gestärkt.
> Die Prozesse zur Behandlung von Schwachstellen wurden rationalisiert.

Unsere Erfahrungen mit dem Swisscom Bug-Bounty-Programm sind ausgesprochen positiv. Das Programm erhöht die Sicherheit unserer Infrastruktur kosteneffektiv, hilft wichtige Security Prozesse zu etablieren und bestehende zu rationalisieren und steigert das Bewusstsein für Sicherheit auf allen Stufen und in allen Bereichen. Der Entscheid als erstes Grossunternehmen in der Schweiz ein Bug-Bounty-Programm ins Leben zu rufen, war mutig und richtig, bedingt aber auch die volle Unterstützung des Managements. Das rechtliche Umfeld zum Betrieb eines Bug-Bounty-Programms in der Schweiz ist nicht trivial, eine Unterstützung diesbezüglich seitens der Gesetzgebung ist wünschenswert.
Bug-Bounty-Programme haben sich in den letzten Jahren in der Industrie weltweit etabliert und werden in Zukunft eine wichtige Rolle im Portfolio von Massnahmen zur Erhöhung der Sicherheit einnehmen. Für Unternehmen, die (noch) kein eigenes Bug-Bounty-Programm aufbauen wollen, bieten Unternehmen wie z. B. Hackerone[13] diese Dienstleistung an.

5 Was macht Swisscom?

Als grosser Schweizer Internet Service Provider (ISP) mit mehreren Millonen Internetzugängen und E-Mail-Konten ist Swisscom täglich und in grossem Mass direkt mit Data Breaches, Phishing Kampagnen, Malware Angriffen und dergleichen gegen uns und unsere Kunden konfrontiert. Unsere Hauptaufgabe ist es, einen performanten, sicheren und barrierefreien Internet-Zugang für unsere Kunden sicherzustellen. Einerseits können wir nicht verhindern, dass Kundensysteme kompromitiert oder deren Nutzerdaten durch externe Data Breaches missbraucht werden. Andererseits müssen wir sicherstellen, dass durch den unwissentlichen Missbrauch von Kundenzugängen oder Nutzerkonten keine Kollateralschäden entstehen, welche den Betrieb der Infrastruktur oder weitere Kunden beeinträchtigen. Die Massnahmen zur Meisterung dieser Herausforderungen gliedern sich in die drei Bereiche *Prävention*, *Detektion* und *Reaktion*.

Während die Prävention zum Ziel hat, Angriffe abzuwehren, greifen die Detektion und Reaktion, wenn Angriffe bereits stattfinden. Durch intelligente Detektion können reaktive Massnahmen eingeleitet werden, die eine weitere Ausbreitung («*lateral movement*») und Verstärkung der Angriffe verhindern und diese abwehren können. Somit sind Detektion und Reaktion eng miteinander verknüpft. Die reaktiven Massnahmen müssen effizient sein und ohne Inhaltsüberwachung des Kundenverkehrs funktionieren.

5.1 Detektion

Einzelne Aspekte der Detektion zum Schutz der privaten Internetzugänge sowie der Mobilfunkkunden sind *Spam Traps*, unsere Eigenentwicklung *Phishing Inspector* sowie *Kundenmeldungen*.

Spam Traps	Spam Traps sind E-Mail-Adressen ohne Benutzer, welche zum Zweck erstellt wurden, illegitime E-Mails zu identifizieren. Da kein realer Benutzer hinter diesen Mailboxen steht, handelt es sich bei eingehenden E-Mails ausschliesslich um illegitime Sendungen wie Spam, Phishing oder Malware Attacken. Swisscom betreibt tausende solcher Mailkonten, deren Inhalt automatisiert analysiert wird und in die Schutzfilter einfliesst.
Phishing Inspector	Phishing Inspector analysiert die Webseiten von verdächtigen Adressen/URL, um Phishing-Seiten zuverlässig zu identifizieren. Die Adressen der Phishing-Seiten fliessen in die Schutzfilter ein.
Kundenmeldungen	Über die Mailbox spamreport@bluewin.ch können Kunden Phishing-E-Mails direkt an Swisscom melden. Dieser Kanal hat sich als sehr effektiv in der Bekämpfung von Phishing

	erwiesen. Nach einer Überprüfung des Inhalts fliesst diese Information in die Schutzfilter ein.
Austausch mit Peers	Swisscom pflegt einen regen Austausch von relevanten Sicherheitsinformationen direkt mit anderen Providern und den Behörden. Viele Internet-Provider, so auch Swisscom, nutzen den von MELANI betriebenen Dienst www.antiphishing.ch, um sich gegenseitig zeitnah über Phishing-Angriffe auszutauschen und ihre Schutzfilter zeitnah aufzudatieren.
Blacklists	Blacklists sind Listen von Domainnamen, IP- oder E-Mail-Adressen welche in der Vergangenheit negativ aufgefallen sind, z.B. durch den Massenversand von Spam oder Malware oder durch aktive Angriffsversuche. Verschiedene Security-Organisationen führen spezielle Blacklists. ISPs und generel E-Mail-Server-Betreiber prüfen beim Verbindungsaufbau ob die Adresse der Gegenseite auf einer Blacklist eingetragen ist. Ist dies der Fall, führt dies in der Regel zu Ablehnung, Verzögerung, spezieller Behandlung oder Kennzeichnung als Spam. Zum Schutz der Kunden setzt Swisscom ebenfalls mehrere Blacklists ein.

5.2 Machine Learning im Einsatz - Phishing Inspector

Phishing Inspector analysiert automatisiert Webseiten von verdächtigen Adressen/URL, um mit Machine Learning aus über 100 Eigenschaften Phishing Seiten zuverlässig zu identifizieren. Verdächtige Web-Adressen aus den Proxy-Logs des Swisscom Mobilnetzes werden automatisch und anonymisiert an den Phishing Inspector geliefert.

Phishing Inspector wurde durch Swisscom entwickelt, im ersten Quartal 2016 eingeführt und erweist sich seither als robuste und sehr effiziente Sicherheitslösung. Die Genauigkeit der automatischen Klassifizierung liegt bei über 97%. Dies ermöglicht Swisscom eine grosse Zahl von Phishing-Angriffen zeitnah, zuverlässig und mit geringem Resourcenaufwand zu identifizieren. Zwischen 80% und 90% der von Phishing Inspector detektierten Angriffe werden zum Zeitpunkt der Erkennung von Google SafeBrowsing nicht blockiert.

Pro Tag werden zwischen 10'000 und 20'000 URLs untersucht und 50 bis 100 Phishingseiten identifiziert. Die Top-10 der am häufigsten durch Phishing-Angriffe betroffenen Organisationen sind *Apple, PayPal, UBS, Google, Swisscom, MasterCard, Amazon, Cembra, Facebook* und *PostFinance*.

Derzeit sind durch Phishing Inspector 2'652 Domänen von Phishing-Seiten gesperrt. Täglich werden gegen 35’000 Aufrufe von Kunden aus dem Mobile und Fixnet auf unsere Phishing-Warnseite (siehe Abbildung 5) verzeichnet.

5.3 Prävention

Aus den Informationen der unterschiedlichen Detektions-Mechanismen werden die Domainnamen extrahiert und durch die Namensauflösung unserer DNS-Nameserver auf eine Warnseite umgeleitet. D.h. der DNS-Nameserver antwortet nicht mit der IP-Adresse der Domain des Angreifers, sondern mit der IP-Adresse, welche auf eine Swisscom Seite mit einem Warnhinweis führt.
Durch diesen Mechanismus werden die Privat- und Mobilfunknetze sowie die öffentlichen WLAN-Hotspots, welche unsere DNS-Nameserver verwenden, effektiv und zeitnah vor Angriffen geschützt.

Abbildung 5 - *Warnseite beim versuchten Zugriff auf eine Phishing Seite*

5.4 Reaktion

Wir müssen davon ausgehen, dass ein Teil unserer Kunden bereits kompromittiert wurde oder dass die Vertraulichkeit von Passwörtern zu Mailboxen oder dem Swisscom-Login durch einen Data Breach nicht weiter gegeben ist. Dabei unterscheiden wir folgende Fälle einer Kompromitierung:

Kompromittierung des Kunden

Eines oder mehrere Geräte des Kunden sind kompromittiert und der Internetzugang des Kunden wird missbraucht.

Kompromittierung von Mailbox oder Swisscom-Login

Ist die Vertraulichkeit der Zugangsinformation nicht mehr gegeben, hat der Angreifer Zugang zu den Mailboxen des Opfers und kann gegebenenfalls über die

«Passwort vergessen» Funktion Konten des Opfers bei weiteren Diensten kompromittieren. Mit den Zugangsinformationen des Swisscom Logins kann der Angreifer die Swisscom Dienste des Opfers, inklusive Internet-Zugang, missbrauchen.

Typischerweise weiss der Betroffene nichts von der Kompromittierung. Aus seiner Sicht verhalten sich seine Systeme normal, denn Angreifer verhalten sich möglichst lange unauffällig, um den Profit aus einem Angriff zu maximieren. Dies bedeutet einerseits eine direkte und anhaltende Gefährdung des Kunden. Andererseits werden durch den Missbrauch des Internetanschlusses und der Systeme des Kunden weitere Internetbenutzer und Dienste gefährdet, beispielsweise:

- durch den Massenversand von Malware oder Spam,
- durch Einbruchsversuche auf weitere Systeme im Internet ausgehend vom Internetanschluss des Kunden,
- durch die Teilnahme an Distributed Denial of Service (DDoS) Angriffen gegen Dritte.

Findet ein solcher Missbrauch statt, wird riskiert, dass Mailserver, Systeme oder Netzwerke von Swisscom in sogenannten Blacklists eingetragen werden. In der Folge werden weitere Kunden und unbeteiligte Dritte stark beeinträchtigt, da Systeme und Netzwerke auf der Blacklist von der Kommunikation mit der Aussenwelt weitgehend ausgesperrt werden. Die Herausforderung für einen Internet Service Provider liegt darin, den kompromittierten Kunden mit minimaler Beeinträchtigung bestmöglich zu schützen und negative Auswirkungen auf die Infrastruktur und weitere Kunden zu vermeinden.

Zum Schutz des Kunden und der Vermeidung von Kollateralschäden stehen uns zwei Massnahmen zur Verfügung. Diese werden entweder automatisch oder manuel nach Feststellung eines Missbrauchs oder Kompromittierung ausgelöst:

Fall (A) – Netzwerk-Quarantäne

Swisscom hat über Jahre einen mehrstufigen Quarantäne-Prozess für kompromittierte Internetanschlüsse aufgebaut. Stellen wir fest, dass eine Kompromittierung (oder ein absichtlicher Missbrauch) eines Internet-Anschlusses vorliegt, wird dieser Anschluss in einem isolierten Quarantänenetzwerk terminiert. Bis auf wenige Ausnahmen sind damit alle Internetverbindungen gesperrt. Dem Kunden wird bei einem Verbindungsversuch eine Informationsseite angezeigt, welche über die Massnahme sowie deren Grund informiert und weitere Information mit Hilfe zur Selbsthilfe anbietet. Nicht betroffen von der Sperre sind Swisscom TV sowie die Telefonie. Weiterhin möglich sind auch Verbindungen, welche dem Kunden helfen das Problem zu beheben, z.B. durch Antivirenprogramme, Software Updates etc.

Hat der Kunde das Problem behoben, kann er den Internetzugang mit Hilfe der Hinweisseite selbst wieder freischalten. Ab der Dritten Sperre innert einer vorgegebenen Frist kann die Sperre nur noch durch einen Anruf beim Callcenter aufgehoben werden.

Fall (B) – Sperrung des Kontos

Bei einer Kompromittierung oder einem Missbrauch einer Mailbox wird diese gesperrt.
Damit wird verhindert, dass der Angreifer die Mailbox auslesen kann oder darüber die Passwörter weiterer Dienste erlangen kann. Über den Swisscom Login kann sich der Kunde ein neues Passwort setzen. Bei einer Kompromittierung des Swisscom Login wird dieser gesperrt. Erst nach eindeutiger Identifikation des berechtigten Kunden wird die Sperre aufgehoben und ein neues Passwort gesetzt.

Im Durchschnitt erfolgen pro Tag gegen 200 solcher Sperrungen. Die Mehrheit dieser Sperrungen werden durch den Kunden nach der Behebung des Problems selbst aufgehoben. Abbildung 6 zeigt die Anzahl Sperrungen pro Tag für einen Ausschnitt im Jahr 2016.

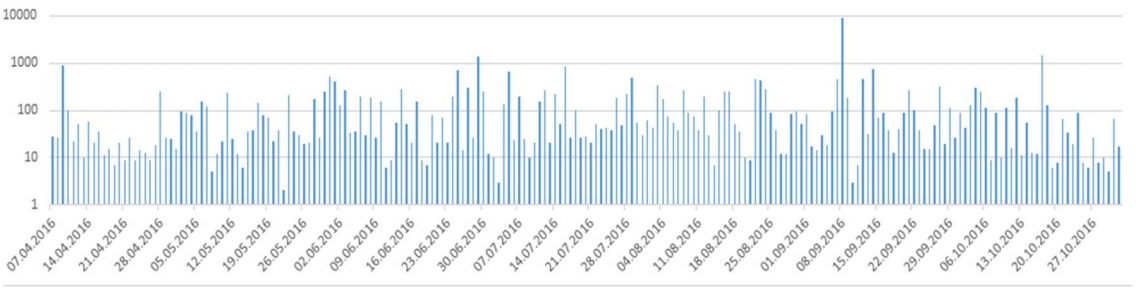

Abbildung 6 – Kontosperrungen pro Tag zwischen April und Oktober 2016 (Logarithmische Skala)

6 Zusammenfassung

Das Internet hat disruptive Umwälzungen ausgelöst. Wir sind sowohl als Gesellschaft als auch in der Wirtschaft immer noch in der frühen Phase der Adaption dieser Möglichkeiten. Selbstverständlich entstehen aus diesen Entwicklungen auch neue Bedrohungen und Gefahren. Es gilt, diese Bedrohungen zu erkennen und effektive Gegenmassnahmen aktiv einzuleiten.
Wir müssen davon ausgehen, dass derzeit und auch in Zukunft sowohl nicht publizierte Software-Schwachstellen wie auch umfangreiche Daten von noch nicht publizierten Data Breaches im Umlauf sind. Die Ursachen vieler Cyber-Bedrohungen sind oft technischer Natur, effektive Gegenmassnahmen sind jedoch nicht nur in technischen Ansätzen zu suchen. Bug-Bounty-Programme verhindern keine Schwachstellen, ermöglichen jedoch eine koordinierte, effiziente und faire Kommunikation (und Kompensation) über Sicherheit zwischen den Beteiligten und führen zu einer effektiven und messbaren Erhöhung der Sicherheit. Es wäre wünschenswert, wenn Firmen das Thema Bug Bounty seriös prüfen und allenfalls einführen, während der Gesetzgeber Unsicherheiten zum Thema bereinigt.
Mit Wissen über die Zusammenhänge und etwas Disziplin kann auch jeder Benutzer bei der Wahl und Verwendung seiner Passwörter die Auswirkungen von unvermeidbaren künftigen Data Breaches stark minimieren.
Es gilt die Lehren aus den umfangreich vorhandenen Erkenntnissen der Vergangenheit zu ziehen. Bekannte und vermeidbare Fehler sind zu vermeiden.
In diesem Report haben wir die Themen Data Breaches und Software Schwachstellen beleuchtet, unsere Erfahrungen geteilt und auch mögliche Lösungsansätze skizziert.

Wir wollen damit einen Beitrag zur gemeinsamen Bewältigung der Cyber-Risiken in der Schweiz zu leisten.

---

[1] «Mirai: Telekom-Router nur Kollateralopfer», http://www.inside-it.ch/articles/45843
[2] Have I been pwned (HIBP) - https://haveibeenpwned.com
[3] Password Statistics: The Bad, the Worse and the Ugly - https://www.entrepreneur.com/article/246902
[4] https://haveibeenpwned.com
[5] https://de.wikipedia.org/wiki/Panama_Papers
[6] https://en.wikipedia.org/wiki/2016_Democratic_National_Committee_email_leak
[7] The Known Unknowns / Analysis of publicly unknown vulnerabilities
- http://www.techzoom.net/Papers/The_Known_Unknowns_(2013).pdf
[8] Zerodium – Exploit Acquisition Platform - https://www.zerodium.com
[9] Coordinated Disclosure Guideline - http://www.nzitf.net.nz/pdf/NZITF_Disclosure_Guidelines_2014.pdf
[10] «*An Empirical Study of Vulnerability Reward Programs*» - http://devd.me/papers/vrp-paper.pdf
[11] https://bugcrowd.com/list-of-bug-bounty-programs
[12] Swisscom Bug Bounty - https://www.swisscom.ch/de/about/unternehmen/nachhaltigkeit/digitale-schweiz/sicherheit/bug-bounty.html
[13] https://www.hackerone.com/about