Cyber Security 2017:

Data breaches & bug bounties

Author: Swisscom Security
This report was compiled through close collaboration between Swisscom Security and other operational units.

April 2017

Table of contents

1 Introduction

Over the course of the past two decades, the development of new technologies and the Internet, in particular, has opened up incredible opportunities that have already permanently changed our lives, both private and professional, and will continue to do so in the years to come. That being the case, Internet security has emerged as a critical factor and will continue to gain importance as people and devices become increasingly interconnected. The Internet security environment has evolved in response to the fast-paced developments and changes taking place at the interface between technology, economics and society. A number of different topics have aroused a great deal of attention in the area of cyber security over the course of the past year. The most prominent examples include Distributed Denial of Service (DDoS) attacks involving millions of Internet of Things (IoT) devices[1], sustained waves of attacks by malware that encrypt all of a victim's data (both private individuals and companies) that are only released against payment (ransomware), data leaks involving millions of affected user accounts and political repercussions, as well as the ongoing deluge of software vulnerabilities.

Extremely promising countermeasures, both technical and organic in nature, already exist for many of the current cyber threats. Frequently, however, existing solutions are not used for a number of reasons, whether due to ignorance of the solution, uncertainty and a lack of experience with the new approaches or an inadequate understanding of the impact and context of the threat.

This report sheds light on Swisscom's perspective of the situation concerning ongoing cyber threats attributable to software vulnerabilities as well as enormous data leaks and their impact on Switzerland. Our goal is to provide a more in-depth understanding of these threats and their impact, point out countermeasures and share our own experiences with innovative solutions. Ultimately we hope that this report will help us jointly tackle cyber threats in Switzerland.

Another of our goals in publishing this report is to provide an insight into our Bug Bounty programme. Our experience with bug bounties has been very positive and we would like to encourage other companies in Switzerland to follow suit in order to increase their security, as well.

2 Status report – threat radar

Threats are borne of the constant development of new technologies and their application and distribution across society. Potential threats must be recognised at an early stage and systematically reported. We have chosen to depict the current threat status and its evolution using a radar image (Figure 1).

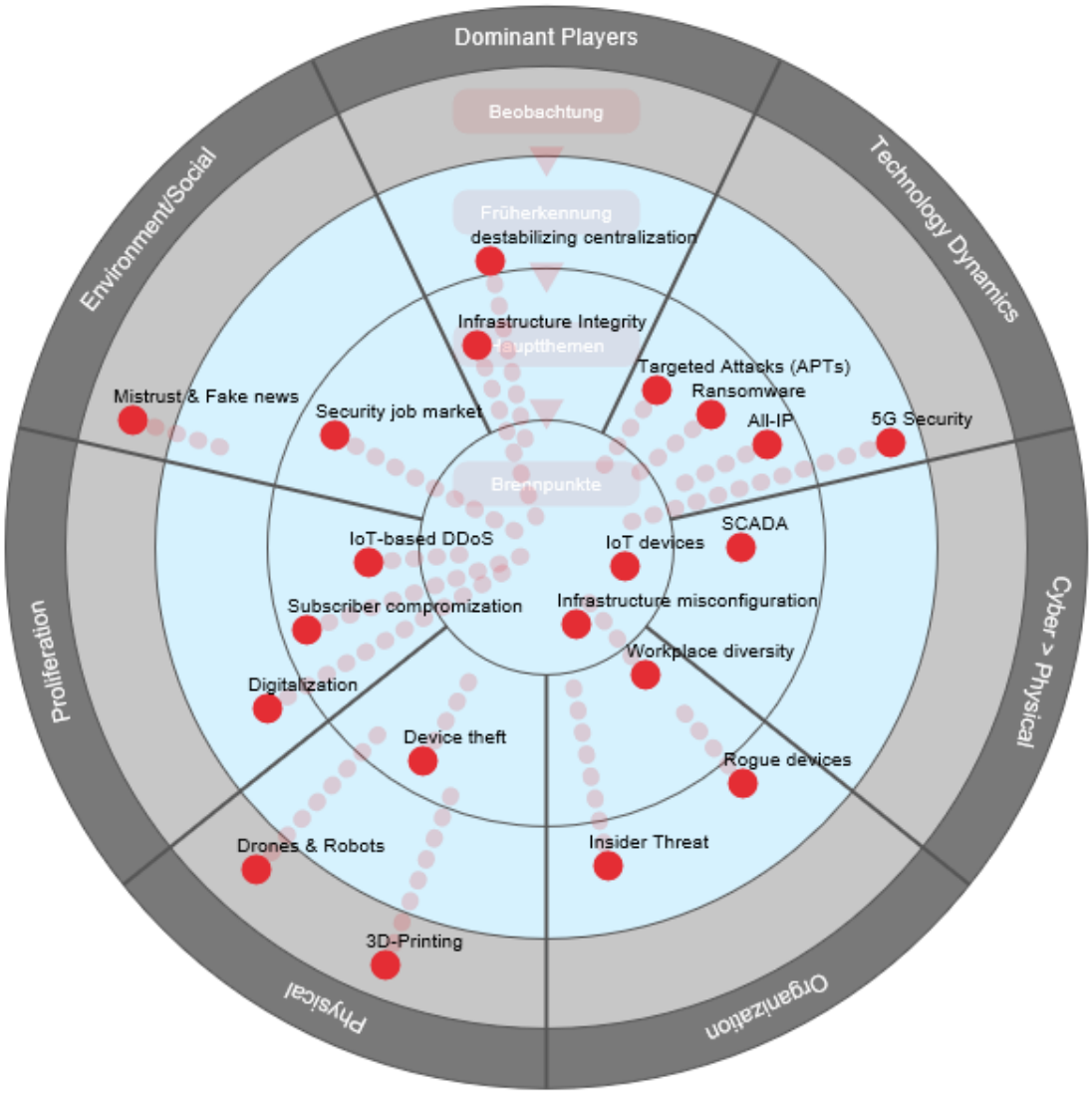

Figure 1 – Threat radar

2.1 Methodology

The threat radar is broken down into seven segments that demarcate the different threat domains. The threats belonging to each of these segments can be assigned to one of four concentric rings. These circles indicate a threat's urgency and thus also the vagueness inherent in assessing such threats. The closer the threat is to the

centre of the circle, the more concrete it is and the more important it is to take appropriate countermeasures. We refer to the rings as

- urgent issues in the case of threats that are already a reality and are being managed with a relatively large deployment of resources.
- main topics in the case of threats that have already materialised on occasion and can be managed with a normal deployment of resources. Frequently, defined processes already exist to efficiently counter threats of this nature.
- **early recognition** for threats that have not yet materialised or whose impact is currently very minor. Projects have been launched with the goal of addressing the growing importance of these threats at an early stage.
- **observation** for threats that will only arise in a few years. No concrete measures have been defined for handling these threats.

Moreover, the individual threats indicated by the points mentioned display a trend which can be increasing, decreasing or stable criticality. The length of the trend beam indicates how swiftly the threat's criticality is expected to change.

2.2 Threats

2.2.1 Dominant players

Threats arising through dependencies on dominant manufacturers, services or protocols.

Main topics	**Infrastructure integrity:** Key components of critical infrastructures can have vulnerabilities incorporated, either through negligence or deliberately, that endanger the security of the system.
Early recognition	**Destabilising centralisation:** Strong centralisation in the structure of the Internet leads to cluster risks. The outage of one service, such as Amazon Web Services (AWS), can have a global impact.

2.2.2 Technology dynamics

Threats arising through the swift pace of technological innovation, which offers attackers not only new opportunities to launch attacks but also enables them to develop new threats themselves.

Main topics	**Targeted attacks (APTs):** Key individuals are identified and attacked in a targeted manner to obtain relevant information or maximise the amount of damage inflicted. **Ransomware:** Large amounts of critical data are encrypted and only (possibly) encrypted in exchange for the payment of a ransom.

	All-IP: The rollout of universal All-IP also increases the risks associated with VoIP technology.
Early recognition	**5G security:** 5G is still a recent technology and its launch will not only offer up a large number of opportunities, but also open the door to unknown threats.

2.2.3 Cyber goes physical

Attacks through the cyberspace infrastructure will increasingly cause damage in the physical world.

Urgent issue	**IoT devices:** Devices with weak protection could be compromised and sabotaged. Such acts could limit the devices' integral functions, such as availability or data integrity.
Main topics	**SCADA:** Many control systems for critical infrastructure installations still exist which are protected either poorly or not at all.

2.2.4 Organisation

Threats that arise through changes in the organisation or exploit weaknesses in the organisation.

Urgent issue	**Infrastructure misconfiguration:** Exploitation of misconfigured infrastructure components and/or vulnerabilities that are identified and rectified at a late stage.
Main topics	**Workplace diversity:** Apart from the many opportunities associated with the new working models, the uncontrolled use of such models, like “Bring your own Device” (BYOD) or the increased use of remote workplaces, exposes companies to greater risks.
Early recognition	**Rogue devices:** Unknown devices in a company's network could launch direct attacks or be exploited for attacks if they are poorly protected. **Insider threat:** Partners or employees manipulate, misuse or sell information, whether through negligence or intentionally.

2.2.5 Physical

Threats that arise from the physical environment that are generally more focused on physical targets.

Main topics	**Device theft:** The theft of critical infrastructure components, in particular, or in future of IoT devices, can lead to a loss of data or impair service availability.

Early recognition	**Drones and robots:** Clarification and attacks across long distances will become easier and cheaper. **3D printing:** Improvements in the quality of 3D printers will make it cheaper and easier to produce e.g. keys or other physical devices.

2.2.6 Proliferation

Threats that benefit from simpler, cheaper accessibility to IT media and expertise. Not only does the spread of these open up new potential areas of attack, they also increase the availability of tools that can be used for attacks.

Main topics	**IoT-based DDoS:** Strong growth in the number of IoT devices coupled with low-level protection produces more “takeover candidates” for botnets. **Subscriber compromisation:** Malware attacks mobile users' private data or is used to attack telecommunication and IT infrastructures.
Early recognition	**Digitalisation:** Increasing levels of networking between the real and virtual world and between individuals' private and work lives open up more avenues of attack.

2.2.7 Environmental / social

Threats arising as a result of socio-political changes or which are facilitated or become more valuable to attackers as a result of such changes.

Main topics	**Security job market:** Difficulties meeting demand for security professionals mean that less expertise is being deployed against attacks that are becoming increasingly complex and intelligent.
Early recognition	**Mistrust & fake news:** Dwindling trust in governmental or social agencies can cause a reduction in the exchange of information needed to identify and fend off potential attacks.

2.3 Conclusion

Our view of the situation reveals that the complexity of the threat landscape is growing. Attackers are profiting from the increasing value of protected assets, which also boosts their motivation to launch an intelligent, targeted attack. Furthermore, technical innovations and the convergence of the physical and virtual worlds are creating new opportunities for attack. Social changes are impacting how we trust one another and the way we work together. Attackers can use both of these factors for their purposes.

Likewise, security functions commissioned with the protection of individuals, data and systems can also make use of these social and technological changes in a targeted, efficient way to ward off attacks.

As Swisscom Security sees it, the situation remains difficult with new challenges arising on an ongoing basis, yet suitable measures exist that can be employed to tackle these.

3 Data breaches

Increasing digitisation in our society and economy means that business, authorities and private individuals are storing larger, more critical pools of data of all types. It comes as no big surprise that the years-long series of enormous data breaches persisted at a high level 2016. In the past, data breaches were merely considered to be a problem affecting the company in question and its customers. In the past year, however, the repercussions on developments in society and politics were illustrated very clearly. Becuase of this, we now assess the risks arising through data breaches from the perspective of society, Swisscom and users in order to estimate their impact on Swiss users and companies. To supplement this risk assessment, we provide an analysis of current data from seven large data breaches affecting mover 890 million user accounts.

The best-known data breach monitoring service haveibeenpwned.com (HIBP) currently lists more than 2 billion stolen user accounts from 187 confirmed data breaches over the past few years.[2]

3.1 Swiss accounts in data breaches

To illustrate the hazard level for Swiss users, we evaluated the freely available data from seven larger data breaches that occurred just recently. The table in Figure 2 shows the number of user accounts exposed through data breaches at *Adobe, Ashley-Madison, Badoo, Dropbox, Gawker, Linkedin* and *MySpace* for different industrial sectors and authorities in Switzerland. These seven data breaches exposed a total of 890 million user accounts.

Category	Total	Adobe	Ashley-Madison	Badoo	Dropbox	Gawker	LinkedIn	MySpace	Multiple breaches
Date of breach		Oct 2013	Jul 2015	Jun 2013	Jul 2012	Dec 2010	May 2012	Jul 2008	
Date of disclosure		Dec 2013	Aug 2015	Jul 2016	Aug 2016	Dec 2013	May 2016	May 2016	
Total user accounts (million)		**152.4**	**30.8**	**112.0**	**68.6**	**1.2**	**164.6**	**359.4**	
Company index									
Fortune 500 (international)	**2'958'767**	441'355	46'143	999'781	200'325	1'039	743'295	616'274	3%
Consulting (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%
Branches of industry - Switzerland									
Banks	**18'565**	2'792	53	512	1'100	22	13'831	677	2%
Insurance companies	**5'921**	936	44	671	584	1	3'595	309	4%
Energy companies	**6'107**	1'622	34	466	2'061	1	2'214	213	8%
Pharma/chemicals	**2'988**	519	18	174	351	1	1'917	127	4%
Media - Switzerland									
Print media	**599**	193	10	36	216	0	118	84	10%
TV & radio	**93**	23	2	18	28	0	22	14	16%
Administration - Switzerland									
Federal administration	**3'070**	907	28	532	545	1	1'123	89	5%
Cantonal administration	**7'963**	2'276	45	1'622	2'453	0	1'867	188	6%
Federal corporations	**4'680**	1'222	42	832	1'384	0	1'385	124	7%
Universities & technical college	**66'124**	16'794	153	2'937	43'708	6	6'905	2'431	11%
E-mail providers - Switzerland									
E-mail services	**291'277**	84'242	28'875	110'834	56'317	42	12'769	43'458	16%
Internet Service Providers (ISP)	**547'796**	241'725	19'234	148'319	118'277	66	54'290	54'731	17%

Figure 2 – Number of user accounts exposed through data breaches in different industrial sectors in Switzerland

This analysis was performed by comparing the domain names of user accounts from the data breaches with the domain names of the organisations in the different sectors. The last column in Figure 2 also shows how many of the user accounts were compromised in more than one data breach. These figures are a low estimate since we only analysed the data from seven breaches while HIBP currently lists 187 confirmed major data breaches.

The analysis also shows that authorities and administrations are impacted by these breaches just like large corporations, critical infrastructure providers, universities and private users. The "E-mail providers - Switzerland" sector includes the user accounts of the twelve largest Swiss Internet service providers as well as the popular freemail portals hotmail.ch, gmx.ch and gmail.ch. This sector thus represents the majority of private Swiss e-mail accounts, of which at least 800,000 were affected by data breaches.

3.2 Risks of the "Password forgotten" function

It could be argued that the damage caused to those affected by data breaches at LinkedIn and MySpace was limited – after all, these are social media portals where users voluntarily disclose their data. However the same cannot be said about the breach at Dropbox, a cloud storage solution. In any case, this simple assessment falls short considering the fact that a majority of the users re-use the same password for

different Internet services. The situation then takes a more critical turn if passwords are also re-used for e-mail accounts. If one of these e-mail accounts is stored as the contact e-mail address for other Internet services, the “Password forgotten” function sends a new password directly to that e-mail address and thus right into the attacker's hands. That not only gives the attacker access to the victim's e-mail account, but also makes it possible for them to gain access to additional services used by the customer. The long period of time that passes between the actual breach and any announcement of the breach is fatal and the impacts of this are felt around the globe, including by users from Switzerland.
The following example illustrates that this risk is quite real. In late August 2016, a growing number of people from the security community were reporting that Dropbox data were being bought and sold in relevant underground forums. The data were freely available on the Internet shortly thereafter. On 8 September, within the space of just one day, Swisscom logged more than 10,000 suspicious yet successful logins on Bluewin e-mail servers from one single foreign IP address. Figure 3 clearly visualises the activities of that day.

Figure 3 – Number of suspicious log-ins on Bluewin e-mail servers in 2016

The IP address from where the log-ins originated was blocked immediately, the 10,000 e-mail accounts already affected were blocked and the users notified.
From March to December 2016, Swisscom blocked e-mail addresses a total of 83,928 times (including multiple blocks) which affected 74,602 different e-mail addresses. Around half, or 34,892, of these e-mail addresses were exposed through one or more data breaches.
This event documents criminals' swift, systematic methodology following a data breach as well as their ability to crack passwords (or else users' inability to select different, strong passwords).
Just how effectively passwords can be protected by hashing hinges on the following criteria over which either users or operators have control:

Users	> Password length
	> Characters available to create the password

	>	Password unpredictability
Operators	>	Choice of hash function used
	>	Characters permitted for creating the password
	>	Minimum and maximum password length
	>	Secure implementation

Unfortunately, several different analyses performed on the passwords exposed in the largest breaches paint the same picture over and over again[3]:

- Most passwords are too short, too simple and thus predictable. The list of the most popular passwords has changed little over the years: “123456”, “password”, “12345”, “12345678”, “qwerty” are the Top 5.
- Users use a small number of passwords to protect a large number of different services. On average, six different passwords are used for 24 services.

3.3 Stations of stolen data

Depending on the attacker, data stolen in a successful breach pass through different stations following the attack. First and foremost, the data are personally viewed, evaluated and exploited by the attacker, without any outward publicity at all. If the target remains compromised, attackers are highly interested in keeping the data breach a secret for as long as possible so as not to endanger their access to the victim. Other profit-maximising options are also available:

> data are offered for sale on an underground market
> the company affected is blackmailed and threatened with disclosure of the data
> the data are made freely accessible online

These options are used if attackers are unable to or have no interest in exploiting the data themselves, have already finished analysing the data and attained their primary goal, or the breach has been detected by a third party or the organisation affected.
State actors either exclusively exploit the data themselves or also disclose it through suitable channels at a specific point in time in order to make political capital out of it. The period of time between the breach's occurrence and its discovery by the company or customer is typically quite long.
Data obtained through a large number of breaches are often made freely available on the Internet at some point and accessible to anybody, sometimes accompanied by a great deal of publicity. Several organisations now exist that notify customers as soon as their data are made available on the Internet or underground[4]. There are also less reputable organisations that offer the entire contents of a data breach as a “data dump” for any paying customer to download – including the passwords cracked. Once a breach occurs, it can take years before information about it is first disclosed

(e.g. announcement of the data breach by the affected company itself or a third party).

3.4 Impact on society and the economy

Besides the primary use of breached data for espionage and identity theft to harm the direct victim, the data breaches that occurred in 2016 reveal an entirely new dimension of endangerment. The following events clearly showed how data breaches could affect the course of history and developments in society:

Panama Leaks / Mossack Fonseca

More than 11.5 million confidential documents from the law firm of Mossack Fonseca from the years 1970 to 2015 were leaked to the media in April 2016[5]. According to the media outlets involved, the documents provided evidence not only of legal tax avoidance strategies but also of tax-related offences and money laundering, violations of UN sanctions and other crimes committed by clients of Mossack Fonseca. Among the clients identified in the data breach were numerous celebrities from around the world including 143 politicians, both current and former heads of states and governments. The data leak at Mossack Fonseca had far-reaching repercussions for some clients, the most prominent being the resignation of Iceland's prime minister following huge demonstrations triggered by the Panama Paper announcements.

US elections

The Democratic National Committee (DNC) network's leak during US elections brought a deluge of details about internal matters and internal e-mails from John Podesta, the campaign manager[6]. This information documents many close ties between politicians, Wall Street and networks within the Democratic Party – which could potentially have had an impact on the election.

Confidential documents can be misused to overtly or covertly influence, manipulate or even blackmail a target. If the decisions and actions of celebrities, business leaders or politicians are influenced through these means, the consequences for the economy or society could potentially be far reaching. Manipulation such as this is hard to prove and takes place covertly. Given that the breach at Mossack Fonseca was made possible through grossly negligent security in the firm's technical systems, this breach was trivial; the breach of the DNC network, on the other hand, is suspected to be the sophisticated work of Russian intelligence agencies.

As a result, we have to presume that both intelligence agencies and cybercriminals are in possession of critical data from other organisations, and have been for some time now, and that they are secretly exploiting those data to promote their own causes and even manipulate decision makers and politicians.

Protecting against risks of this nature is a complex undertaking that requires a great deal of discipline, both in terms of building and operating the IT infrastructure and also with regard to employees' day-to-day work. Given the conflicting interests of security and convenience, this balance needs to be struck with care, communicated well and also understood. Over and over again we see users creatively circumventing rules and technical protective measures, usually for understandable personal reasons.

4 Bug Bounty programme

Over the past few decades, software has become both a fundamental and critical element for both our economy and our society. Increasing online interconnectivity now permits uninterrupted communication between software in all types of devices and both people and machines – thus facilitating a digital society. Despite enormous investments by industry and research in the development of secure software, vulnerabilities and security loopholes are a lasting problem. Attackers can exploit software vulnerabilities to compromise, manipulate, control, spy on or sabotage the affected systems and services. What's more, the history of the Internet has unmistakably shown us that manufacturers, users and even governments are powerless when it comes to preventing or even prohibiting the discovery of security vulnerabilities in software. It comes as no surprise, however, that interest in critical software vulnerabilities has risen considerably over past few years, particularly among cybercriminals (for profit) and state actors (for spying, sabotage). Accordingly, this has given rise to a market that offers high bounties for critical software vulnerabilities.[7] Zerodium, for instance, is offering one million US dollars in exchange for a vulnerability that would make it possible to compromise mobile Apple devices[8].

4.1 Limits of altruism

Luckily, many people who discover vulnerabilities behave ethically and follow the "Coordinated Disclosure" process[9]. The discoverer reports the vulnerability to the manufacturer and gives it time to come up with a security patch before publishing the vulnerability. This, however, hinges on the discoverer's willingness to refrain from making a profit by selling the vulnerability. Yet given swift developments on the software vulnerability market where prices are constantly on the rise, this model is coming under increasing pressure. What's more, a situation in which a company's cybersecurity relies (increasingly) heavily on the altruistic behaviour of vulnerability discoverers is cause for concern.

The realisation that discoverers of vulnerabilities should be rewarded for their ethical behaviour is slowly starting to gain acceptance in the industry. Under bug bounty programmes, companies offer prize money, referred to as (bug) bounties, to anybody who reports vulnerabilities in products or services. Large software manufacturers led the way with this model. Experience with bug bounties has been positive, both from a financial and a security perspective, as shown by a comprehensive study on bug bounty programmes conducted by Google and Mozilla[10]. Slowly but surely, bug bounty programmes are becoming the norm rather than an exception – something made impressively clear in the latest version of BugCrowd's "The Bug Bounty List" which currently contains some 500 companies that operate a bug bounty programme[11].

4.2 The Swisscom Bug Bounty programme

In September 2015 Swisscom became the first major company in Switzerland to offer its own Bug Bounty programme which is run by our "Computer Security Incident Response Team" (CSIRT)[12]. The Bug Bounty programme was launched with these objectives:

- Create a central point of contact for reporting vulnerabilities
- Create incentives for reporting any vulnerabilities found directly to us
- Create optimised processes for dealing with vulnerabilities (both internal and external)
- Establish transparency regarding security gaps affecting our infrastructure (reality check)
- Support our infrastructure's continuous hardening process

With the Bug Bounty programme, we want to reward the discoverers of those bugs for the time and effort they invested in reporting and documenting the vulnerability. All activities connected to the discovery of the vulnerability must be conducted within the bounds of the law and they must not interfere with the operation of our critical infrastructure.

4.3 Vulnerability rating

The amount of the bounty (reward) is based on the risk posed by the vulnerability, not on its technical nature or complexity. The bounty offered for an "SQL Injection" vulnerability, for example, is higher if it exposes sensitive data than if it relates to uncritical data. The bounties offered within the scope of our Bug Bounty programme range from CHF 150 to CHF 10,000 per vulnerability.

4.4 Bug Bounty reports

In 2016, Swisscom's Bug Bounty programme received 281 reports from 54 discoverers concerning products and services used by Swisscom. Of these, more than half (157) of the vulnerabilities have qualified for a bounty. The lion's share of vulnerabilities reported, around 75%, relate to a variety of Web applications. The table below shows a breakdown of vulnerabilities reported based on their criticality.

Criticality	Quantity	Type and impact
High	1	> Critical vulnerabilities in devices commonly used by customers > Critical vulnerabilities in authentication functions

		>	Remote code execution
Medium	14	>	Vulnerabilities in customer devices for which the exploitation potential is limited
		>	SQL Injection with no exposure of sensitive data
		>	Cross-site scripting (XSS) on high-frequency websites
Low	142	>	Cross-site scripting (XSS) in uncritical applications
		>	Exposure of non-sensitive data

Under the Bug Bounty programme last year, a total of around CHF 50,000 was paid out to discoverers from eleven different countries on four continents.

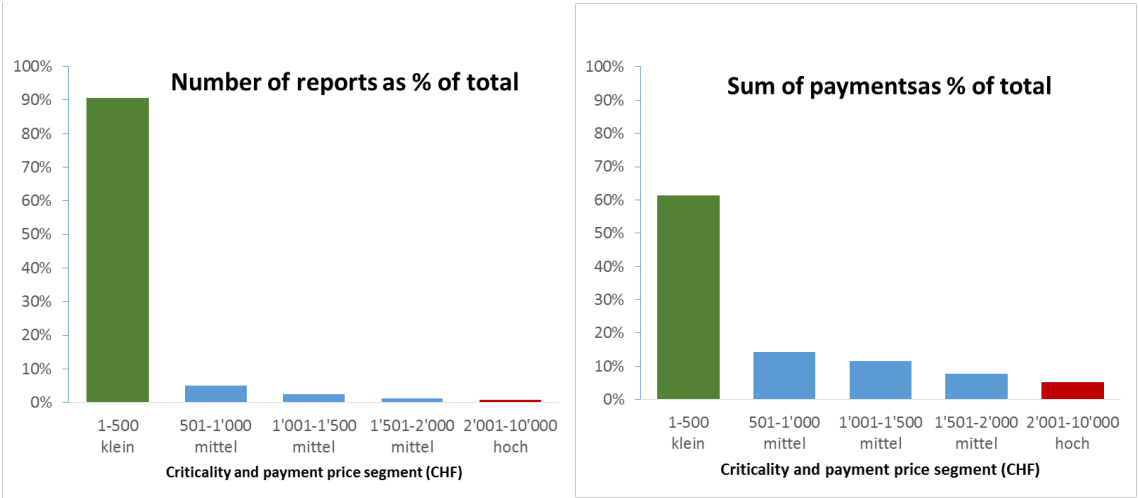

Figure 4 – Percentage of payments and number of reports per price segment

Figure 4 shows the ratio between bounty payments and the number of reports in different price segments for 2016.

> 90% of the vulnerabilities fell into the segment of less critical vulnerabilities (eligible for a bounty of between CHF 1 and CHF 500) and accounted for 60% of the total payout. The vast majority of these vulnerabilities concerned a range of different Web applications, most of which were small special applications for individual projects. The complexity of the vulnerability and the effort required for its rectification are often low (e.g. through a change to the configuration). The Bug Bounty programme has now helped us quickly identify and fix these “legacy” problems.
> A select few of the vulnerabilities fell into the critical segment (bounties of CHF 2,000 or more) and for these reports the discoverers were paid quite well. The damage potential if these vulnerabilities are misused is high to very high. A vulnerability in customers' Internet router, for instance, falls into this category.

4.5 Experience

Despite the fact that the Bug Bounty programme is still fairly new, it has swiftly yielded some valuable insights and increased the security of our infrastructure even further:

- The effectiveness of internal security initiatives becomes quantifiable:
  Software developed internally at Swisscom has a significantly lower number of vulnerabilities than purchased software. Our investments in secure software development go hand in hand with the Bug Bounty programme.
- Areas in need of improvement and those with a high security level are clearly identified.
- There is a heightened awareness of security-related issues within the company.
- Vulnerability handling processes have been streamlined.

Our experience with Swisscom's Bug Bounty programme has been extremely positive. The programme boosts the security of our infrastructure in a cost-effective way, helps get key security processes established while streamlining existing processes and increases the awareness of security-related issues at all levels and in all units. The company's decision to become the first major corporation in Switzerland to initiate a Bug Bounty programme was bold and the right move, however it also requires the full support of management. The legal environment for operating a bug bounty programme in Switzerland is anything but trivial and it is advisable for interested parties to seek out support on legal matters in this regard.
Over the past few years, bug bounty programmes have been set up in companies all around the globe and, in future, will play a key role in the portfolio of security-enhancing measures. For companies not (yet) interested in setting up their own bug bounty programmes, companies like Hackerone[13] offer this service.

5 What is Swisscom doing?

As Switzerland's largest Internet Service Provider (ISP) with several million Internet access points and e-mail accounts, Swisscom is directly confronted with copious numbers of data breaches, phishing campaigns, malware attacks, etc. on a daily basis that target us and our customers. Our main task is to ensure that our customers have high-performance, secure, barrier-free Internet access. On the one hand, we cannot prevent customer systems from being compromised or their user data from being misused in connection with external data breaches. On the other, we have to ensure that the unknown misuse of customer access or user accounts does not cause any collateral damage that could interfere with the operation of our infrastructure or harm other customers. Measures devised to overcome these challenges can be broken down into three categories: *prevention, detection* and *reaction*.

While prevention is aimed at warding off attacks, detection and reaction come into play after an attack has already taken place. Intelligent detection can help initiate reactive measures that prevent the attacks from spreading further (lateral movement) or intensifying and also fend them off. Detection and reaction are therefore closely linked to one another. Reactive measures have to be efficient and work without monitoring the content of a customer's transmissions.

5.1 Detection

Individual aspects of detection measures that protect both private Internet access and mobile customers include spam traps, our proprietary *Phishing Inspector* tool and *reports from customers*.

Spam traps	Spam traps are e-mail addresses without users created for the purpose of identifying illegitimate e-mails. Since these mailboxes have no real user behind them, any incoming e-mails have to be illegitimate e-mails including spam, phishing and malware attacks. Swisscom operates thousands of these e-mail accounts, whose contents are automatically analysed and incorporated into the protective filters.
Phishing Inspector	Phishing Inspector analyses the websites of suspicious addresses/URLs in order to reliably identify phishing sites. The addresses of the phishing sites are fed into the protective filters.
Customer reports	Customers can use the spamreport@bluewin.ch mailbox to notify Swisscom directly of any phishing e-mails they receive. This channel has proven extremely effective in efforts to combat phishing. Once the content of the e-mail is checked, the information is incorporated into the protective filters.

Peer collaboration	Swisscom engages in an active, direct exchange of security-relevant information with other providers and public authorities. Many Internet providers, including Swisscom, use the service operated by MELANI, www.antiphishing.ch, to share the latest information about phishing attacks and update their protective filters in a timely manner.
Blacklists	Blacklists are lists of domain names, IP or e-mail addresses that have been flagged in the past, e.g. because they were used for sending large volumes of spam or malware or were actively involved in attempted attacks. Several different security organisations compile special blacklists. When establishing a connection, ISPs and general e-mail server operators check whether the counterparty's address is entered on one of the blacklists. If so, this generally causes the e-mail to be rejected, delayed, given special treatment or flagged as spam. Swisscom also uses multiple blacklists to protect its customers.

5.2 Machine learning in action - Phishing Inspector

Phishing Inspector automatically analyses the websites of suspicious addresses/URLs so that machine learning tools can reliably identify phishing sites on the basis of more than 100 characteristics. Suspicious Web addresses from the proxy logs of the Swisscom mobile phone network are automatically anonymised and sent to Phishing Inspector.

Swisscom developed Phishing Inspector which it then rolled out in the first quarter of 2016. Since then, it has proven itself to be a robust, extremely efficient security solution. The automatic classification function achieves an accuracy level of over 97%. This helps Swisscom identify a large number of phishing attacks promptly, reliably and with very few resources. Between 80% and 90% of the attacks detected by Phishing Inspector are not blocked when checked by Google SafeBrowsing.

Every day, between 10,000 and 20,000 URLs are inspected and 50 to 100 phishing pages are identified. The top ten organisations most frequently targeted by phishing attacks are *Apple, PayPal, UBS, Google, Swisscom, MasterCard, Amazon, Cembra, Facebook* and *PostFinance*.

Phishing Inspector is currently blocking 2,652 domains of phishing sites. Our phishing warning page (see Figure 5) is called up nearly 35,000 times every day by customers from the mobile and fixed networks.

5.3 Prevention

Based on information obtained through the various detection mechanisms, domain names are extracted and rerouted to a warning page based on the name resolution of our DNS name server. That means that the DNS name server does not respond

with the IP address of the attacker's domain, rather with an IP address that leads to a Swisscom page containing a warning.
This method helps provide effective, timely protection against attacks to the users of private networks, mobile phone networks, and public WLAN hotspots that use our DNS name servers.

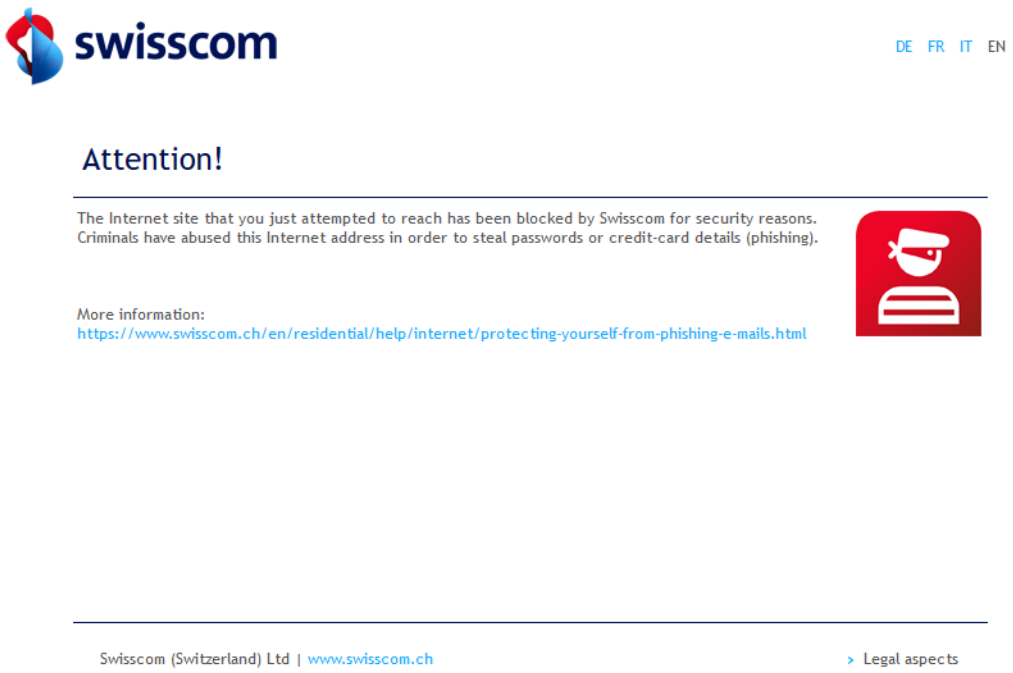

Figure 5 - *Warning page that appears when a user attempts to access a phishing site*

5.4 Reaction

We have to assume that a portion of our customers has already been compromised or that a data breach has violated the confidentiality of passwords to mailboxes or the Swisscom login. In cases involving a compromise, we differentiate as follows:

Compromised customer

One or more of a customer's devices has been compromised and the customer's Internet access is being misused.

Compromised mailbox or Swisscom login

If the confidentiality of access details is no longer intact, the attacker has access to the victim's mailboxes and could potentially compromise the accounts of other services used by the victim by using the "Password forgotten" function. The attacker

can use the access details of the Swisscom Login to misuse the victim's Swisscom services, including Internet access.

Typically, the individuals affected are not aware of the fact that they have been compromised. As far as they can see, their systems are behaving normally because attackers keep a low profile for as long as possible in order to maximise the profit generated through an attack. This not only means a direct, sustained threat to the customer but misuse of the customer's Internet connection and system also endangers other Internet users and services including:

- through the large-scale sending of malware or spam,
- through attempted breaches of other online systems launched from the customer's Internet connection,
- through participation in Distributed Denial of Service (DDoS) attacks against third parties.

If misuse of this nature occurs, there is a chance that Swisscom e-mail servers, systems and networks could be blacklisted. This would significantly impair other customers and uninvolved third parties since systems and networks on the blacklist are largely prevented from communicating with the outside world. For an Internet Service Provider, the challenge lies in protecting the compromised customer with minimal interference while also preventing any negative impact on the infrastructure and other customers.

We have two measures at our disposal for protecting customers and preventing collateral damage. These are triggered either automatically or manually once misuse or a compromise is detected:

Case (A) – Network quarantine

Over the years, Swisscom has built up a multi-step quarantine process for compromised Internet connections. If we determine that an Internet connection has been compromised (or is intentionally being misused), this connection is terminated in an isolated quarantine network. Apart from a few exceptions, that blocks all Internet connections. When attempting to connect to the Internet, they are shown an information page explaining what was done and why, and also providing additional information and tips on how they can rectify the situation themselves. This block does not affect Swisscom TV or telephony. Other connections the customer needs to rectify the problem are also still enabled, such as antivirus programmes, software updates, etc.
Once the customer has rectified the problem, he or she can reactivate the Internet connection with the help of the information page. If the connection is blocked three or more times within a specified period of time, this block can only be lifted by calling the call centre.

Case (B) – Blocked account

If a mailbox is compromised or misused, it is blocked.
This prevents the attacker from reading the contents of the mailbox or using it to obtain passwords for other services. Customers can then use their Swisscom Login to set a new password. If the Swisscom Login is compromised, it is blocked. The block is only lifted and a new password set once the authorised customer has been clearly identified.

On average, around 200 blocks of this nature are performed every day. The majority of these blocks are lifted by the customers themselves once they have rectified the problem. Figure 6 shows the number of blocks performed every day for part of 2016.

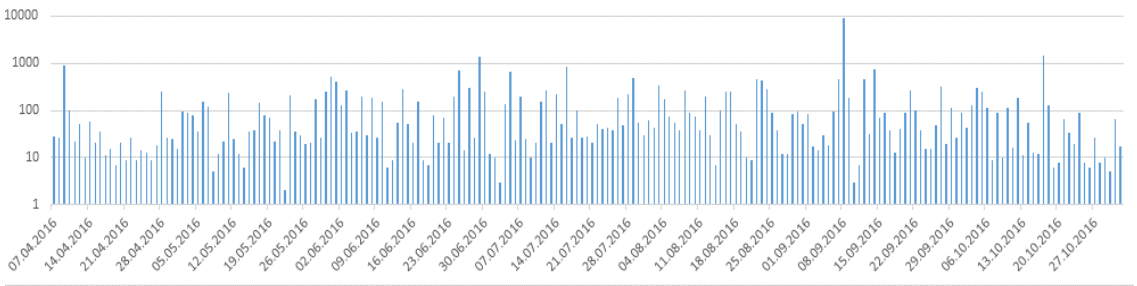

Figure 6 – Accounts blocked per day between April and October 2016 (logarithmic scale)

6 Summary

The Internet has brought about disruptive changes. As a society and as an economy, we are still in the early stages of adapting these possibilities. Naturally, these developments also give rise to new threats and dangers. The goal is to identify these threats and actively initiate effective countermeasures.
We have to presume that both undisclosed software vulnerabilities and extensive amounts of data from as-yet-undisclosed data breaches are in circulation, both now and in future. While the causes of many cyber threats are often technical in nature, effective countermeasures should also be sought outside the technical sphere. Bug bounty programmes do not prevent vulnerabilities however they permit a coordinated, efficient and fair discussion (and compensation) about security between the parties involved and also achieve effective, measurable increases in security. Ideally, companies should take a serious look at the topic of a bug bounty and introduce a bug bounty programme where necessary while legislators clear up any uncertainties on the matter.
Armed with knowledge about the situation and a bit of discipline, each and every user can greatly minimise the repercussions of unavoidable future data breaches by choosing and using his or her passwords correctly.
To do this, lessons have to be learned from the wealth of knowledge that has already been gleaned from past events. Avoid known mistakes that are preventable.
In this report we looked at the topics of data breaches and software vulnerabilities, shared our experiences and outlined some possible solutions.

We hope that this report will help us in our efforts to jointly tackle cyber threats in Switzerland.

---

[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/en/about/company/portrait/network/security/bug-bounty.html
[13] https://www.hackerone.com/about