Cyber Security 2017:

Data Breaches & Bug Bounties

Autore: Swisscom Security
Questo report è stato realizzato grazie alla stretta collaborazione di Swisscom Security con altre unità operative.

Aprile 2017

Indice

1 Introduzione

Nel corso degli ultimi due decenni lo sviluppo di nuove tecnologie, e in particolare di internet, ha creato opportunità incredibili, che hanno cambiato per sempre le nostre vite e che continueranno a cambiarle. La sicurezza in internet è diventata un fattore critico e la sua importanza crescerà anche proporzionalmente all'interconnessione tra persone e dispositivi. Il settore della sicurezza in internet è caratterizzato da evoluzioni e cambiamenti rapidi che avvengono dove tecnologia, economia e società si incontrano. Negli anni scorsi differenti temi del settore Cyber-Security hanno risvegliato grande interesse. Gli esempi più eclatanti sono gli attacchi Distributed Denial of Service (DDoS) con milioni di dispostivi[1] Internet of Things (IoT), continue ondate di attacchi di Malware, che criptano tutti i dati delle vittime (privati e aziende) restituendoli solo dietro pagamento ("Ransomware"), fughe di dati con milioni di conti utente colpiti con implicazioni politiche, oltre alla persistenza delle falle nei software.

Attualmente contro molte minacce informatiche vi sono delle contromisure promettenti, di natura sia tecnica che organizzativa. Spesso le contromisure note non vengono impiegate, sia per la scarsa conoscenza della soluzione che per scarsa esperienza o incertezze nell'utilizzo dei nuovi approcci, ma anche per mancanza di comprensione delle conseguenze e dei legami tra le minacce.

In questa relazione ci concentriamo sul punto di vista di Swisscom sulle persistenti minacce informatiche dovute alle lacune nei software, alle massicce fughe di dati e alla relativa ripercussione sulla Svizzera. Vogliamo rafforzare la comprensione di queste minacce e dei loro effetti, indicare le contromisure e condividere la nostra esperienza con gli approcci innovativi alle soluzioni possibili.

Con ciò ci auguriamo di dare un contributo per far fronte insieme ai rischi informatici in Svizzera.

Con la presente pubblicazione vogliamo dare un'idea del nostro programma Bug Bounty. La nostra esperienza con il programma Bug Bounty è molto positiva e vogliamo incoraggiare altre aziende in Svizzera ad osare questo passo per incrementare la sicurezza.

2 Quadro della situazione - Radar delle minacce

Le minacce hanno origine proprio nel continuo sviluppo delle tecnologie e del relativo uso e della diffusione all'interno della società. Le potenziali minacce devono essere riconosciute precocemente e registrate sistematicamente. Per descrivere lo stato attuale delle minacce e la relativa evoluzione ci serviremo di un radar (Figura 1).

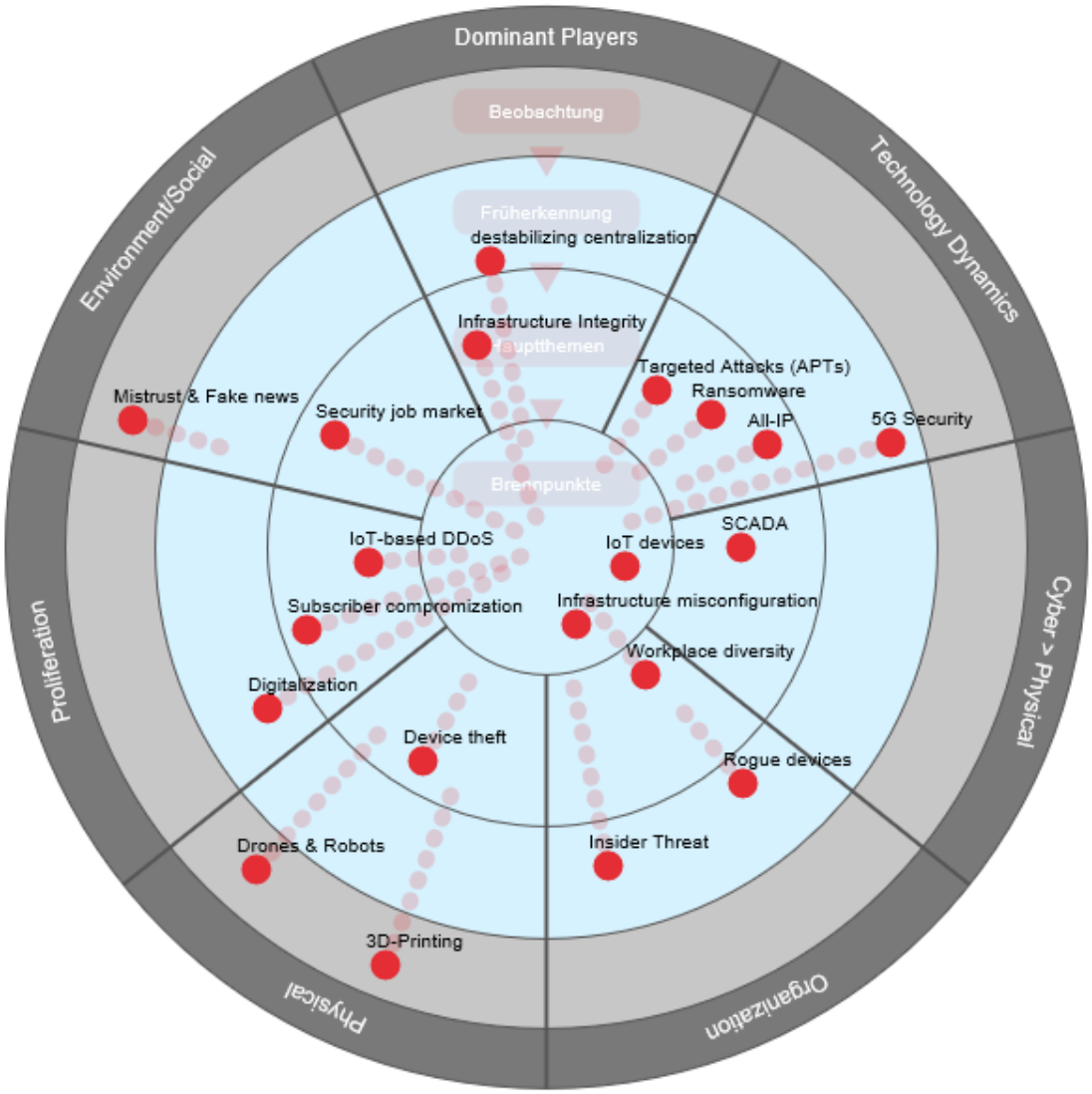

Figura 1 – Radar delle minacce

2.1 Metodologia

Il radar delle minacce è diviso in sette segmenti che delimitano i diversi domini delle minacce. In ogni segmento le relative minacce possono essere assegnate a uno dei quattro anelli concentrici. I cerchi indicano l'attualità della minaccia e quindi anche l'approssimazione della valutazione della minaccia. Più vicina al centro del cerchio si

trova la minaccia e più è concreta e tanto più importanti sono le contromisure necessarie. Definiamo gli anelli come

- **Emergenze** per minacce già reali e controllate con un impiego relativamente importante di risorse.
- **Temi principali** per minacce che sono già comparse occasionalmente e controllate con un impiego normale di risorse. Spesso sussistono processi regolati per contrastare in modo efficiente queste minacce.
- **Allerta precoce** per minacce non ancora comparse o che attualmente mostrano solo un'azione ridotta. Sono stati avviati dei progetti per contrastare tempestivamente una futura crescente importanza di tali minacce.
- **Osservazione** per minacce che compariranno solo tra qualche anno. Non vi sono misure concrete per gestire queste minacce.

Inoltre le minacce contrassegnate dai punti citati mostrano una tendenza. Questa può essere in aumento, in diminuzione o stabile nella propria criticità. La lunghezza del raggio della tendenza indica la velocità di trasformazione attesa della criticità della minaccia.

2.2 Minacce

2.2.1 Dominant players

Minacce derivanti da interdipendenze di produttori, servizi o protocolli dominanti.

Temi principali	**Infrastructure Integrity:** i componenti fondamentali di infrastrutture critiche possono aver installato per negligenza o volutamente delle falle che minacciano la sicurezza del sistema.
Allerta precoce	**Destabilizing Centralization:** la forte centralizzazione nella struttura di internet comporta un rischio di accumulazione. L'interruzione di un servizio può avere effetti a livello mondiale, come ad esempio l'interruzione di Amazon Web Services (AWS).

2.2.2 Technology dynamics

Le minacce derivanti dalla rapidissima innovazione tecnologica da un lato forniscono nuove opportunità agli hacker e dall'altro creano nuove minacce dovute allo sviluppo stesso.

Temi principali	**Targeted attacks (APTs):** le persone chiave sono identificate e aggredite in modo mirato per ottenere informazioni rilevanti o per creare il massimo danno possibile. **Ransomware:** i dati critici vengono cifrati su vasta scala e decifrati (eventualmente) in cambio di un riscatto.

	All IP: durante il lancio con copertura capillare di All IP aumentano i rischi in relazione alla tecnologia VoIP.
Allerta precoce	**5G Security:** 5G è una tecnologia ancora giovane, l'introduzione porterà con sé oltre alle numerose opportunità anche delle minacce ancora sconosciute.

2.2.3 Cyber goes physical

Gli attacchi tramite le infrastrutture nel Cyberspace provocheranno sempre più danni nel mondo fisico.

Emergenza	**IoT Devices:** i dispositivi con una protezione debole possono essere compromessi e sabotati. Potranno così essere limitati nella propria funzione, ad esempio in fatto di disponibilità o integrità dei dati.
Temi principali	**SCADA:** esistono sempre ancora dei sistemi di controllo protetti male o non protetti per gli impianti delle infrastrutture critiche.

2.2.4 Organization

Minacce che si basano sulle modifiche nelle organizzazioni o sfruttano i punti deboli nelle organizzazioni.

Emergenza	**Infrastructure misconfiguration:** sfruttamento di componenti mal configurati delle infrastrutture e/o falle identificate ed eliminate tardivamente.
Temi principali	**Workplace diversity:** oltre alle numerose opportunità che i nuovi modelli di lavoro portano con sé, l'impiego incontrollato di tali modelli, come ad es. «Bring your own Device» (BYOD) oppure il maggiore impiego di postazioni di lavoro remote comporta una maggiore esposizione al rischio.
Allerta precoce	**Rogue devices:** dispositivi sconosciuti nella rete aziendale possono effettuare attacchi diretti oppure essere utilizzati per gli attacchi a causa della scarsa protezione. **Insider threat:** partner o collaboratori manipolano, usano in modo illecito o vendono per negligenza o intenzionalmente le informazioni.

2.2.5 Physical

Minacce derivanti da un ambiente fisico e di regola orientate verso obiettivi fisici.

Temi principali	**Device theft:** il furto in particolare di componenti dell'infrastruttura critica o in futuro anche di apparecchi IoT

	può comportare la perdita di dati o compromettere la disponibilità dei servizi.
Allerta precoce	**Drones and Robots:** lo spionaggio o gli attacchi da grande distanza diventano più semplici ed economici. **3D-Printing:** la produzione ad esempio di chiavi o di altri dispositivi fisici diventa più economica e semplice con la migliore qualità delle stampanti 3D.

2.2.6 Proliferation

Minacce che profittano della sempre più semplice ed economica disponibilità di media IT e know-how. Da un lato perché la diffusione comporta un maggior numero di potenziali bersagli di attacchi e dall'altro perché incrementa la disponibilità di strumenti di attacco.

Temi principali	**IoT-based DDoS:** la grande diffusione di dispositivi IoT con una scarsa protezione porta a un maggior numero di «candidati di trasmissione» per botnet. **Subscriber compromization:** il software dannoso attacca i dati privati degli utenti mobile o viene utilizzato per attacchi all'infrastruttura IT o delle telecomunicazioni.
Allerta precoce	**Digitalization:** una messa in rete sempre maggiore del mondo reale e virtuale e della vita privata e commerciale comporta un maggior numero di vie di attacco.

2.2.7 Environmental / Social

Minacce che originano da cambiamenti socio-politici o che diventano più semplici o vantaggiosi per gli hacker a causa di tali cambiamenti.

Temi principali	**Security job market:** la richiesta di Security-Professionals viene soddisfatta con molta difficoltà, comportando un minore know-how nell'attività contro attacchi sempre più complessi e intelligenti.
Allerta precoce	**Mistrust & fake news:** la sempre più scarsa fiducia verso gli uffici statali o sociali può portare a una riduzione dello scambio di informazioni per l'identificazione e la difesa contro potenziali attacchi.

2.3 Conclusione

Il nostro quadro della situazione mostra la sempre maggiore complessità della situazione delle minacce. Gli hacker profittano del crescente valore degli asset degni di particolare protezione, accrescendo la motivazione per un attacco mirato e

intelligente. Inoltre le innovazioni tecnologiche e la convergenza del mondo fisico con quello virtuale creano nuove opportunità di attacco. I cambiamenti sociali hanno un effetto sulla fiducia reciproca e sul modo in cui si collabora. Tutti fattori che gli hacker possono utilizzare per i loro scopi.

Anche le funzioni di sicurezza preposte alla protezione di persone, dati e impianti possono utilizzare questi cambiamenti sociali e tecnologici per impedire in modo efficiente e mirato questi attacchi.

Swisscom Security interpreta il quadro della situazione come impegnativo con sfide sempre nuove, che possono essere padroneggiate tramite misure adeguate.

3 Furto di dati („Data Breaches“)

Tramite la crescente digitalizzazione della nostra società ed economia, nelle aziende, presso le autorità e i privati si accumula un sempre maggiore quantitativo di dati di ogni genere. Non sorprende il fatto che nell’anno 2016 la serie di furti massicci di dati (di seguito “Data Breach”), che perdura da anni, è incrementata in modo impressionante. In passato i Data Breaches erano visti semplicemente come un problema dell’azienda colpita e dei rispettivi clienti. Lo scorso anno si sono evidenziati gli effetti sullo sviluppo sociale e politico. Qui di seguito prendiamo in considerazione i rischi derivanti dai Data Breaches dal punto di vista della società, di Swisscom e degli utenti, per valutare gli effetti sulle aziende e sugli utenti svizzeri. Questa ponderazione dei rischi si basa sull’analisi dei dati attuali derivanti da sette grandi Data Breaches con più di 890 milioni di conti utente colpiti. Il più noto servizio di Data Breach Monitoring haveibeenpwned.com (HIBP) elenca attualmente più di 2 miliardi di conti utente rubati in 187 Data Breaches confermati degli ultimi anni.[2]

3.1 Conti svizzeri in Data Breaches

Per esemplificare il rischio per gli utenti svizzeri abbiamo analizzato i dati liberamente disponibili di sette importanti Data Breaches recenti. La tabella in figura 2 mostra per differenti settori industriali e autorità svizzere il numero di conti utente esposti dai Data Breaches di *Adobe, Ashley-Madison, Badoo, Dropbox, Gawker, Linkedin* e *MySpace*. Tramite questi sette Data Breaches sono stati esposti 890 milioni di conti utente.

Categoria	Totale	Adobe	Ashley-Madison	Badoo	Dropbox	Gawker	LinkedIn	Myspace	Breach multiplo
Data attacco		Ott. 2013	Lugl. 2015	Giu. 2013	Lugl. 2012	Dic. 2010	Mag. 2012	Lugl. 2008	
Data pubblicazione		Dic. 2013	Ag. 2015	Lugl. 2016	Ag. 2016	Dic. 2013	Mag. 2016	Mag. 2016	
Totale conti utente (milioni)		**152.4**	**30.8**	**112.0**	**68.6**	**1.2**	**164.6**	**359.4**	
Indice della ditta									
Fortune 500 (internazionale)	2'958'767	441'355	46'143	999'781	200'325	1'039	743'295	616'274	3%
Consulenza (Big 6, internaziona	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%
Settori industriali - Svizzera									
Banche	18'565	2'792	53	512	1'100	22	13'831	677	2%
Assicurazioni	5'921	936	44	671	584	1	3'595	309	4%
Imprese settore energia	6'107	1'622	34	466	2'061	1	2'214	213	8%
Farmaceutica/Chimica	2'988	519	18	174	351	1	1'917	127	4%
Media - Svizzera									
Stampa	599	193	10	36	216	0	118	84	10%
Televisione, radio	93	23	2	18	28	0	22	14	16%
Amministrazione Svizzera									
Amministrazione federale	3'070	907	28	532	545	1	1'123	89	5%
Amministrazione cantonale	7'963	2'276	45	1'622	2'453	0	1'867	188	6%
Aziende federali	4'680	1'222	42	832	1'384	0	1'385	124	7%
Università e Scuole universitari	66'124	16'794	153	2'937	43'708	6	6'905	2'431	11%
Mailprovider - Svizzera									
Servizi di posta elettronica	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%

Figura 2 – Numero di conti utente esposti tramite Data Breaches per differenti settori industriali in Svizzera

Per questa analisi sono stati confrontati i nomi di dominio dei conti utente dei Data Breaches con i nomi di dominio delle organizzazioni dei differenti settori. L'ultima colonna in figura 2 mostra inoltre il numero di conti utente compromessi durante più di un Data Breach. Queste cifre rappresentano una stima minima poiché abbiamo analizzato solamente i dati di sette Data Breaches, mentre HIBP elenca attualmente 187 Data Breaches importanti.

L'analisi mostra che anche autorità e amministrazioni sono state interessate da questi Data Breaches, come grandi aziende, fornitori critici di infrastrutture, università o utenti privati. Il settore «Mailprovider Svizzera» comprende i conti utente dei dodici maggiori Internet Service Provider svizzeri e dei noti portali freemail hotmail.ch, gmx.ch e gmail.ch. Questo settore rappresenta la maggioranza degli account di posta elettronica privati svizzeri, e di questi almeno 800'000 sono stati interessati da Data Breaches.

3.2 I rischi della funzione «Non ricordi la password?»

Si potrebbe argomentare che i danni dai Data Breaches su LinkedIn e MySpace sono limitati per gli interessati – si tratta in fondo di portali di social media sui quali si pubblicano volontariamente i propri dati. Per Dropbox come soluzione di memoria basata sul cloud è decisamente diverso. In ogni caso questa semplice considerazione è troppo limitata, considerando che la maggior parte degli utenti utilizza la stessa password per differenti servizi internet. La situazione diventa critica quando le password vengono riutilizzate anche per gli account e-mail. Se questo account e-mail è stato riportato come contatto per altri servizi internet, tramite la funzione «Non ricordi la password?» viene inviata una nuova password direttamente all'indirizzo e-mail e quindi giunge nelle mani dell'hacker. Di conseguenza l'hacker non ha accesso solo all'account e-mail della vittima, ma può anche trovare l'accesso ad altri servizi del cliente. Il lungo intervallo di tempo tra il furto effettivo e la pubblicazione è fatale: gli effetti sono globali, anche per gli utenti in Svizzera.
L'esempio seguente illustra la grave concretezza di questo rischio. Verso la fine dell'agosto 2016 nella Security Community si sono moltiplicate le voci sul fatto che i dati di Dropbox venivano commercializzati clandestinamente in alcuni forum. Poco dopo i dati erano liberamente disponibili in internet. L'8 settembre, in un unico giorno, Swisscom registra sui server mail di Bluewin più di 10'000 login sospetti, ma di successo, da parte di un unico indirizzo IP estero. La Figura 3 mostra in modo impressionante questa attività di quella giornata.

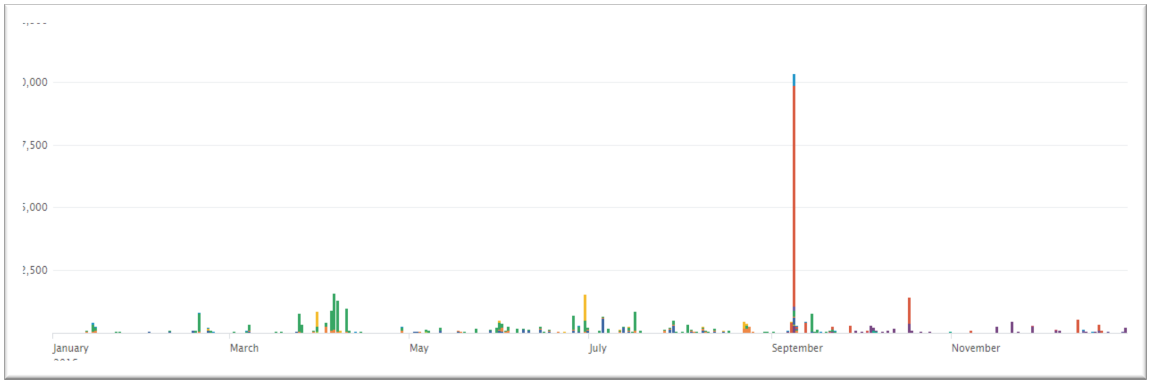

Figura 3 – Numero di accessi sospetti sul server mail di bluewin nel 2016

Gli indirizzi IP dai quali sono partiti questi accessi sono stati immediatamente bloccati, i 10'000 account di posta elettronica interessati sono stati bloccati e gli utenti sono stati informati.
Swisscom, tra marzo e dicembre 2016 ha effettuato in totale 83'928 blocchi (inclusi blocchi multipli) di 74'602 indirizzi mail differenti. Circa la metà, o 34'892 di questi indirizzi mail sono stati esposti da uno o più Data Breaches.
Questo episodio documenta l'azione sistematica e rapida dei criminali dopo un Data Breach, come anche l'abilità nel craccare le password (o la difficoltà degli utenti di scegliere password forti e differenti).
La protezione efficace delle password tramite hashing dipende prevalentemente dai seguenti criteri controllati dall'utente o dal gestore:

Utente	> Lunghezza della password > Caratteri alfanumerici per formare la password > Imprevedibilità della password
Gestore	> Scelta della funzione hash impiegata > Caratteri alfanumerici ammessi per formare la password > Lunghezza minima e/o massima della password > Implementazione sicura

Purtroppo differenti analisi delle password dai maggiori Data Breaches del passato mostrano sempre lo stesso quadro[3]:

> La maggior parte delle password è troppo corta, troppo semplice e quindi prevedibile. Nel tempo le password più frequenti sono sempre le stesse: «123456», «password», «12345», «12345678», «qwerty» sono i Top 5.
> Gli utenti utilizzano un piccolo numero di password per un grande numero di servizi differenti. In media si utilizzano sei password diverse per 24 servizi.

3.3 Le tappe dei dati rubati

Dopo un attacco con successo i dati seguono differenti tappe secondo l'hacker. In prima linea i dati vengono visualizzati, analizzati e utilizzati dagli hacker stessi, senza alcun tipo di pubblicità. Se la compromissione mantiene l'obiettivo l'hacker ha un grande interesse a mantenere segreto il Data Breach per più tempo possibile per non compromettere l'accesso alla vittima. Per ottimizzare il profitto vi sono le opzioni seguenti:

- i dati vengono offerti in vendita in un mercato clandestino
- l'azienda colpita viene ricattata, viene minacciata della pubblicazione dei dati
- i dati vengono pubblicati liberamente accessibili in internet

Queste opzioni sono scelte se l'hacker non può o non vuole utilizzare direttamente i dati, se l'analisi è terminata e se l'obiettivo primario è stato raggiunto, o se l'attacco è stato scoperto da terzi o dall'organizzazione interessata.
Gli attori statali analizzano direttamente i dati, oppure in un preciso momento li pubblicano tramite canali adatti per trarne un profitto politico. Tipicamente passa un lungo periodo di tempo tra l'attacco e il momento in cui gli interessati (l'azienda o i clienti) hanno notizia del Data Breach.
Spesso, in qualche momento, i dati di numerosi Data Breaches vengono resi disponibili in internet e accessibili da chiunque, a volte anche accompagnati da molta pubblicità. Contemporaneamente diverse organizzazioni offrono servizi che informano i clienti se i loro dati vengono resi disponibili in internet o in ambienti clandestini[4]. Organizzazioni meno serie offrono per il download l'insieme dei dati di un Data Breach come un cosiddetto "Data Dump" a qualsiasi cliente pagante – comprese le password craccate. Il periodo di tempo tra l'attacco effettivo e la prima pubblicazione del fatto (ad esempio la comunicazione del Data Breach da parte della ditta colpita, o da parte di terzi) può anche essere qualche anno.

3.4 Effetti sulla società e sull'economia

Oltre alla vendita dei dati rubati a scopo di spionaggio e furto di identità ai danni degli interessati, i Data Breaches del 2016 mostrano una nuova dimensione del rischio. Gli eventi seguenti hanno dimostrato chiaramente gli effetti dei Data Breaches sul corso della storia e sullo sviluppo della società:

Panama Leaks / Mossack Fonseca

Più di 11.5 milioni di documenti confidenziali degli anni tra il 1970 e il 2015 dello studio legale Fonseca sono stati consegnati ai media nell'aprile 2016[5]. Secondo l'esame dei media coinvolti i documenti confermano le strategie legali di elusione fiscale, ma anche reati di riciclaggio di denaro e reati fiscali, evasione di sanzioni ONU e altri reati di clienti di Mossack Fonseca. Tra i clienti identificati nel Data Breach vi sono numerosi personaggi importanti di tutto il mondo, tra cui 143 politici, capi di stato e di governo del passato e ancora in carica. La fuga di dati da Mossack Fonesca

ha avuto vaste conseguenze per alcuni clienti, l'esempio più celebre sono le dimissioni del primo ministro islandese dopo le proteste di massa a seguito della pubblicazione tramite i Panama Papers.

Campagna elettorale negli USA

Durante la campagna elettorale negli USA la società viene inondata di informazioni dal leak della rete del Democratic National Committee (DNC) e di e-mail interne del direttore della campagna elettorale John Podesta[6]. Le informazioni documentano i molteplici intrecci tra politica, Wall Street e gruppi di interesse nel partito democratico, con una potenziale influenza sulle elezioni.

Tramite l'utilizzo indebito di documenti confidenziali è possibile influenzare apertamente o in modo occulto la persona interessata, manipolarla o anche ricattarla. Se si influenzano in questo modo le decisioni e le azioni di personaggi pubblici, di leader economici o di politici, le conseguenze per l'economia o la società sono potenzialmente molto vaste. La manipolazione è difficilmente dimostrabile e avviene in modo occulto. L'attacco da Mossack Fonseca è stato banale a causa della scarsissima sicurezza dei sistemi tecnologici, mentre dietro l'attacco alla rete DNC si suppone esservi l'opera complessa dei servizi segreti russi.

Di conseguenza dobbiamo supporre che sia i servizi segreti che i criminali informatici sono in possesso da molto tempo (e anche attualmente) di dati critici di molte organizzazioni e che li utilizzano in modo occulto per i propri scopi, compresa la manipolazione di decisori e di politici.

La protezione contro tali rischi è impegnativa e comporta molta disciplina, sia nella costruzione e nella gestione dell'infrastruttura IT che nel lavoro quotidiano dei collaboratori. L'analisi costi-benefici tra sicurezza e comfort di lavoro deve essere effettuata con molta cura e deve essere ben comunicata e compresa. Si evidenzia sempre nuovamente che gli utenti, spesso per evidente interesse personale, sono molto creativi nell'impiego di protezioni e misure di sicurezza tecniche.

4 Programma Bug-Bounty

Negli ultimi decenni i software sono diventati un elemento critico e fondamentale nella nostra economia e anche nella società. Tramite il progresso della interconnessione in internet, i software comunicano ininterrottamente in utti i tipi di apparecchi con persone e macchine, permettendo così una società digitale. Malgrado gli enormi investimenti dell'industria e della ricerca per uno sviluppo di software sicuri, le lacune o falle nella sicurezza sono un problema costante. Un hacker può sfruttare le falle nei software per compromettere, manipolare, controllare, spiare o sabotare i sistemi o servizi colpiti. Inoltre la storia di internet mostra inequivocabilmente che la scoperta delle lacune nella sicurezza dei software non può essere impedita o bloccata da parte del produttore, dell'utente o anche da parte dello Stato. Non sorprende che l'interesse verso le lacune critiche dei software è aumentato in modo considerevole negli ultimi anni, in particolare da parte della criminalità (profitto) o da parte di attori statali (spionaggio, sabotaggio). Di conseguenza è nato un mercato che offre prezzi elevati per le lacune critiche dei software.[7] Ad esempio la ditta Zerodium offre più di un milione di USD per una lacuna che consente di compromettere i dispositivi mobile Apple[8].

4.1 Limiti dell'altruismo

Fortunatamente molti scopritori di falle si comportano in modo etico e seguono il cosiddetto processo «Coordinated Disclosure»[9]. Lo scopritore comunica la falla al produttore dandogli il tempo necessario allo sviluppo di una Security Patch, prima di pubblicare la falla. Ciò implica però che lo scopritore rinuncia al profitto derivante dalla vendita della falla. Alla luce dello sviluppo rapidissmo del mercato delle falle dei software, con prezzi sempre più elevati, questo modello è messo sempre più sotto pressione. Inoltre è preoccupante che la sicurezza informatica della società sia in misura sempre maggiore dipendente dal comportamento altruistico degli scopritori.

Nell'industria si è diffusa progressivamente l'opinione che la scoperta delle falle dovesse essere ricompensata per il comportamento etico. Nei cosiddetti programmi Bug-Bounty, le aziende offrono agli scopritori dei premi, i cosiddetti (Bug) Bounties, in cambio della comunicazione delle falle nei prodotti o nei servizi. I grandi sviluppatori di software sono molto avanzati con questo modello. Come dimostra uno studio esteso dei programmi Bug Bounty di Google e Mozilla, le esperienze con i Bug Bounties sono positive, sia dal punto di vista della sicurezza che da quello economico[10]. Lentamente, ma con sicurezza i programmi Bug Bounty si stanno sviluppando da eccezione a norma – la "The Bug Bounty List" di BugCrowd lo dimostra in modo impressionante con circa 500 aziende registrate in un programma Bug Bounty[11].

4.2 Il programma Bug Bounty Swisscom

Dal settembre 2015 Swisscom, come prima grande azienda in Svizzera, gestisce un programma Bug Bounty proprio sotto la responsabilità del nostro «Computer Security Incident Response Team» (CSIRT)[12]. Il programma Bug Bounty è stato avviato con i seguenti obiettivi:

- creare un interlocutore centrale per la comunicazione delle falle
- creare lo stimolo a comunicarci direttamente le falle scoperte
- creare dei processi ottimizzati per il trattamento delle falle (processi interni ed esterni)
- trasparenza in relazione alle falle nella sicurezza riguardanti la nostra infrastruttura (Reality Check)
- supporto al costante processo di consolidamento della nostra infrastruttura

Con il programma Bug Bounty vogliamo ricompensare gli scopritori per il loro impegno in relazione al resoconto e alla documentazione della falla. Tutte le attività in relazione alla scoperta della falla devono svolgersi all'interno della legalità e non devono compromettere le operazioni della nostra infrastruttura critica.

4.3 Valutazione di una falla

L'ammontare dei Bounty (premio in denaro) dipende dal rischio dato dalla falla, e non dal tipo o dalla complessità in senso tecnico della falla. Ad esempio una falla «SQL Injection» viene pagata maggiormente se attraverso di essa vengono esposti dei dati sensibili rispetto a dei dati non critici. La fascia di prezzo del nostro programma Bug Bounty è tra 150 CHF e 10'000 CHF per falla.

4.4 Comunicazioni Bug Bounty

Grazie al programma Bug Bounty Swisscom nel 2016 sono arrivate 281 comunicazioni da parte di 54 scopritori relative a prodotti o servizi utilizzati da Swisscom. Di queste sinora più della metà (157) delle falle si sono qualificate per un Bounty. La maggior parte delle falle, circa il 75%, riguarda diverse applicazioni web. La tabella seguente mostra la distribuzione delle falle comunicate in base alla criticità.

Criticità	Quantità	Tipo ed effetti
Alto	1	> Falle critiche in terminali per i clienti ampiamente diffusi > Falle critiche in funzioni di autenticazione > Remote Code Execution
Medio	14	> Falle limitatamente utilizzabili in terminali per i clienti > SQL Injection senza esposizione di dati sensibili > Cross Site Scripting (XSS) su pagine web altamente frequentate
Basso	142	> Cross-Site-Scripting (XSS) in applicazioni non critiche > Esposizione di dati non sensibili

Durante lo scorso anno, all'interno del programma Bug Bounty, sono stati versati ca. 50'000 CHF agli scopritori di undici nazioni differenti di quattro continenti.

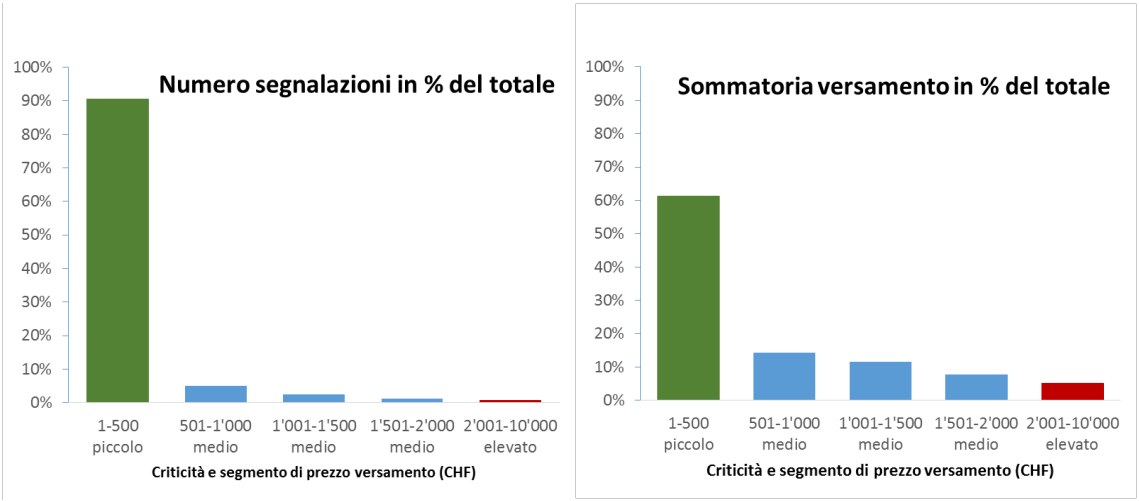

Figura 4 – Percentuale dei pagamenti e numero di segnalazioni per segmento di prezzo

Per l'anno 2016 la Figura 4 mostra l'andamento dei pagamenti di Bounty e del numero di segnalazioni in differenti segmenti di prezzo.

> Nel segmento delle falle con criticità minore (Bounty tra 1 fino a 500 CHF) si trova il 90% delle falle per il quale è stato versato il 60% della somma complessiva. La stragrande maggioranza di queste falle riguarda diverse applicazioni web, prevalentemente piccole applicazioni speciali per progetti individuali. Spesso la complessità delle falle e la loro eliminazione non è importante (ad es. eliminazione tramite una modifica della configurazione). Grazie al programma Bug-Bounty questi «rifiuti del passato» vengono ora rapidamente identificati ed eliminati.

> Nel segmento delle falle critiche (Bounty da 2'000 CHF) se ne trova un paio, ma le segnalazioni sono state ben pagate agli scopritori. Il potenziale di danno in caso di abuso della falla è alto fino a molto alto. In questa categoria troviamo tra l'altro una falla nel router internet dei clienti.

4.5 Esperienze

Grazie al programma Bug Bounty, ancora molto giovane, sono state acquisite conoscenze importanti in breve tempo e la sicurezza della nostra infrastruttura è stata ulteriormente incrementata:

> L'efficacia delle iniziative interne di Security è misurabile:
> *i software sviluppati internamente a Swisscom mostrano decisamente meno falle rispetto ai software acquistati. I nostri investimenti in uno sviluppo sicuro di software vanno mano nella mano con il programma Bug Bounty.*
> Si riconoscono con chiarezza i settori che richiedono una revisione e quelli con un alto livello di sicurezza.
> La consapevolezza della sicurezza nell'azienda viene rafforzata.
> I processi per il trattamento delle falle sono stati razionalizzati.

La nostra esperienza con il programma Bug Bounty Swisscom è decisamente positiva. Il programma incrementa la sicurezza della nostra infrastruttura con efficienza in termini di costi, aiuta a definire processi importanti per la Security, a razionalizzare i processi esistenti ed incrementa la consapevolezza legata alla sicurezza a tutti i livelli e in tutti i settori. La decisione di instaurare un programma Bug Bounty come prima grande azienda in Svizzera è stata coraggiosa e corretta, sottintende comunque il totale supporto del Management. L'ambiente legale per la conduzione di un programma Bug Bounty in Svizzera non è semplice, un sostegno da parte della legislazione sarebbe opportuno.
Negli ultimi anni i programmi Bug Bounty si sono affermati nell'industria in tutto il mondo e in futuro avranno un ruolo importante nel portfolio delle misure per l'incremento della sicurezza. Per le aziende che non vogliono (ancora) costruire un proprio programma Bug-Bounty, vi sono aziende che offrono questo tipo di servizio come ad es. Hackerone[13].

5 Che cosa fa Swisscom?

Come importante Internet Service Provider (ISP) svizzero con diversi milioni di accessi internet e conti e-mail, Swisscom si confronta ogni giorno direttamente e in grande misura con Data Breaches, campagne di phishing, attacchi Malware e simili contro di noi e contro i nostri clienti. Il nostro compito principale è garantire un accesso internet performante, sicuro e senza barriere per i nostri clienti. Da un lato non possiamo evitare che i sistemi dei clienti vengano compromessi o che i loro dati utente vengano utilizzati per scopi illeciti tramite Data Breaches esterni. Dall'altro lato dobbiamo garantire che dall'uso illecito ignoto degli accessi clienti o conti utente non derivino danni collaterali che compromettono l'esercizio dell'infrastruttura o danneggiano altri clienti. Le misure per padroneggiare tali sfide si suddividono in tre settori *Prevenzione*, *Rilevamento* e *Reazione*.

Mentre la prevenzione ha come obiettivo la difesa dagli attacchi, il rilevamento e la reazione intervengono quando gli attacchi hanno già luogo. Tramite un rilevamento intelligente è possibile introdurre delle misure reattive che impediscono l'ulteriore diffusione («*lateral movement*») e il rafforzamento degli attacchi e che possono contrastarli. Di conseguenza rilevamento e reazione sono strettamente correlati. Le misure reattive devono essere efficienti e funzionare senza la sorveglianza dei contenuti del traffico del cliente.

5.1 Rilevamento

Singoli aspetti del rilevamento per la protezione degli accessi internet privati e dei clienti di telefonia mobile sono *Spam Traps*, il nostro sviluppo proprietario *Phishing Inspector* e *Segnalazioni dei clienti*.

Spam Traps	Spam Traps sono indirizzi e-mail senza utente, creati per identificare e-mail illegittime. Poiché non esiste un utente reale dietro queste Mailbox, in caso di e-mail in ingresso si tratta esclusivamente di messaggi illegittimi come spam, phishing o attacchi Malware. Swisscom gestisce migliaia di questi conti e-mail il cui contenuto viene analizzato automaticamente per confluire nei filtri di protezione.
Phishing Inspector	Phishing Inspector analizza i siti web di indirizzi/URL sospetti per identificare con certezza le pagine di phishing. Gli indirizzi delle pagine di phishing confluiscono nei filtri di protezione.
Segnalazioni dei clienti	Tramite la Mailbox spamreport@bluewin.ch i clienti possono comunicare direttamente a Swisscom le e-mail di phishing. Questo canale si è dimostrato molto efficace nella lotta al phishing. Dopo un'analisi del contenuto l'informazione confluisce nei filtri di protezione.
Scambio con peers	Swisscom ha uno scambio vivace di informazioni rilevanti per la sicurezza direttamente con altri provider e con le autorità.

	Molti provider internet, e anche Swisscom, utilizzano il servizio gestito da MELANI www.antiphishing.ch, per informarsi reciprocamente in tempi brevi sugli attacchi di phishing e per aggiornare rapidamente i filtri di protezione.
Blacklists	Le blacklists sono elenchi di nomi di dominio, indirizzi IP o e-mail che in passato si sono fatti notare in senso negativo, ad esempio per l'invio di massa di spam o Malware o per tentativi attivi di attacco. Diverse organizzazioni di Security hanno speciali blacklists. Durante lo stabilimento della comunicazione ISPs e in generale i gestori di E-Mail-Server controllano se l'indirizzo della controparte è inserita in una blacklist. In questo caso ciò comporta un diniego, un ritardo, un trattamento speciale o un contrassegno come spam. Anche Swisscom utilizza diverse blacklists a difesa dei clienti.

5.2 Uso di Machine Learning - Phishing Inspector

Phishing Inspector analizza automaticamente le pagine web di indirizzi/URL sospetti per identificare in modo affidabile le pagine di phishing tramite Machine Learning a partire da più di 100 caratteristiche. Gli indirizzi web sospetti dai proxy-logs della rete mobile Swisscom vengono inviati automaticamente e in modo anonimo al Phishing Inspector.
Phishing Inspector è stato sviluppato da Swisscom e introdotto nel primo trimestre del 2016, da allora si è dimostrato una soluzione molto efficiente e valida per la sicurezza. La precisione della classificazione automatica è superiore al 97%. Ciò consente a Swisscom di identificare un grande numero di attacchi phishing in modo rapido, affidabile e con un ridotto impiego di risorse. Tra l'80% e il 90% degli attacchi rilevati dal Phishing Inspector al momento del riconoscimento non vengono bloccati da Google SafeBrowsing.
Ogni giorno vengono esaminati tra 10'000 e 20'000 URL ed identificati da 50 a 100 pagine di phishing. La Top 10 delle organizzazioni più frequentemente colpite dal phishing sono *Apple, PayPal, UBS, Google, Swisscom, MasterCard, Amazon, Cembra, Facebook* e *PostFinance*.
Attualmente vi sono 2'652 domini di pagine phishing bloccate dal Phishing Inspector. Ogni giorno si registrano 35'000 visualizzazioni da parte dei clienti di rete di telefonia fissa e mobile della nostra pagina di avvertenza di phishing (vedi Figura 5).

5.3 Prevenzione

Dalle informazioni dei diversi meccanismi di rilevamento si estraggono i nomi dei domini per deviarli a una pagina di avvertenza tramite la risoluzione dei nomi dei nostri name server DNS. O meglio: il name server DNS non risponde con l'indirizzo IP del dominio dell'hacker, ma con l'indirizzo IP che porta alla pagina Swisscom con l'avvertenza.

Grazie a questo meccanismo le reti mobili e private e gli hotspot WLAN pubblici che utilizzano i nostri name server DNS sono protetti in modo efficace e rapido dagli attacchi.

Figura 5 - *Pagina di avvertenza durante un tentativo di accesso a una pagina di phishing*

5.4 Reazione

Dobbiamo supporre che a causa di un Data Breach una parte dei nostri clienti è già stata compromessa e che la confidenzialità delle password per le Mailbox o il Swisscom Login non è più garantita. Distinguiamo i seguenti casi di compromissione:

Compromissione del cliente

Uno o più dispositivi del cliente sono compromessi e l'accesso internet del cliente è utilizzato illecitamente.

Compromissione di Mailbox o del Swisscom Login

Se la confidenzialità delle informazioni di accesso non è più garantita, l'hacker ha accesso alle Mailbox della vittima e può eventualmente compromettere gli account della vittima presso altri servizi tramite la funzione «Non ricordi la password?». Con le informazioni di accesso del Swisscom Login l'hacker può utilizzare illecitamente i servizi Swisscom della vittima, compreso l'accesso internet.

Tipicamente la persona interessata non sa nulla della compromissione. Dal suo punto di vista i suoi sistemi si comportano in modo normale, poiché gli hacker usano la massima discrezione per massimizzare i vantaggi dell'attacco. Ciò comporta da un lato un rischio diretto e persistente per il cliente. Dall'altro lato, tramite l'uso illecito del collegamento internet e dei sistemi del cliente, vengono messi a rischio altri utenti internet e altri servizi, ad esempio tramite:

- l'invio di massa di Malware o spam,
- tentativi di accesso illecito ad altri sistemi in internet provenienti dal collegamento internet del cliente,
- la partecipazione ad attacchi Distributed Denial of Service (DDoS) contro terzi.

Se un tale uso illecito ha luogo sussiste il rischio che mail server, sistemi o reti di Swisscom vengano iscritte in cosiddette blacklist. Di conseguenza altri clienti e terzi estranei vengono fortemente danneggiati, dato che sistemi e reti iscritte nella blacklist non possono praticamente comunicare con il mondo esterno. La sfida per un Internet Service Provider sta nel proteggere al meglio il cliente compromesso con un danno minimo ed evitare effetti negativi sull'infrastruttura e su altri clienti.

Per la protezione del cliente e per evitare danni collaterali abbiamo a disposizione due misure. Queste vengono avviate automaticamente oppure manualmente dopo l'accertamento di un abuso o una compromissione:

Caso (A) – Quarantena della rete

Swisscom ha definito nel corso degli anni un processo di quarantena a più livelli per collegamenti internet compromessi. Quando accertiamo che sussiste una compromissione (o un abuso volontario) di un collegamento internet, questo collegamento viene terminato in una rete di quarantena isolata. Salvo poche eccezioni, con ciò tutti i collegamenti a internet sono bloccati. Il cliente, quando tenta di collegarsi, visualizza una pagina informativa che gli comunica la misura e il motivo e gli fornisce ulteriori informazioni per risolvere autonomamente il problema. Non sono interessati dal blocco la Swisscom TV e la telefonia. Inoltre sono possibili connessioni che aiutano il cliente a risolvere il problema, ad esempio tramite programmi antivirus, aggiornamenti di software ecc.
Quando il cliente ha risolto il problema può sbloccare autonomamente l'accesso a internet seguendo le indicazioni della pagina informativa. A partire dal terzo blocco entro un termine definito, il blocco può essere eliminato solo dopo una telefonata al callcenter.

Caso (B) – Blocco del conto

In caso di compromissione o di uso illecito di una Mailbox questa viene bloccata.

Con ciò si evita che l'hacker possa leggere la Mailbox o ottenerne le password per altri servizi. Il cliente può impostare una nuova password attraverso il Swisscom Login. In caso di compromissione di un Swisscom Login questo viene bloccato. Solo dopo una inequivocabile identificazione del cliente autorizzato si elimina il blocco e viene impostata una nuova password.

In media ogni giorno avvengono 200 di questi blocchi. La maggior parte di questi blocchi viene risolta direttamente dai clienti dopo l'eliminazione del problema. La figura 6 mostra il numero di blocchi al giorno per un periodo del 2016.

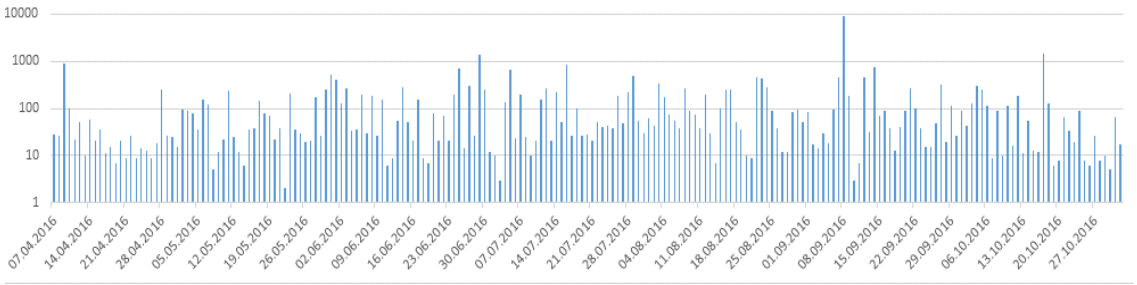

Figura 6 – Blocchi conto per giorno tra aprile e ottobre 2016 (scala logaritmica)

6 Riepilogo

Internet ha scatenato cambiamenti dirompenti. A livello sociale ed economico stiamo attraversando la fase iniziale dell'adattamento di queste opportunità. Ovviamente tali sviluppi comportano anche nuovi pericoli e minacce. Si tratta di riconoscere queste minacce e di introdurre attivamente delle contromisure efficaci.
Dobbiamo partire dal fatto che oggi, e anche in futuro, vi sono in circolazione falle di software non pubblicate e anche una grande quantità di dati derivanti da Data Breaches non ancora resi noti. Le cause di molte minacce informatiche sono spesso di natura tecnica, le contromisure efficaci non sono tuttavia da ricercare solo negli approcci tecnici. I programmi Bug-Bounty non evitano le falle, ma consentono una comunicazione coordinata, efficiente e leale sulla sicurezza tra i partecipanti (e un compenso) e portano a un incremento efficace e misurabile della sicurezza. Sarebbe opportuno che le aziende controllassero seriamente l'argomento Bug Bounty e che lo introducessero, mentre il legislatore dovrebbe eliminare le incertezze dall'argomento.
Grazie alla conoscenza sulle correlazioni e con un poco di disciplina nella scelta e nell'utilizzo delle proprie password ogni utente può contribuire a ridurre al minimo gli effetti di inevitabili Data Breaches futuri.
Si tratta di imparare dalle vaste conoscenze del passato. Gli errori noti ed evitabili devono essere evitati.
Nel presente report abbiamo analizzato gli argomenti Data Breaches e falle nei software, condiviso la nostra esperienza e abbozzato alcuni possibili approcci di soluzione.

Con ciò vogliamo dare un contributo per far fronte insieme ai rischi informatici in Svizzera.

---

[1] «Mirai: Router Telekom solo vittime collaterali», 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