Cyber Security 2017:

Data Breaches & Bug Bounties

Auteur: Swisscom Security
Ce rapport a été réalisé dans le cadre d'un partenariat étroit de Swisscom Security et d'autres unités opérationnelles.

Avril 2017

Table des matières

1 Introduction

Au cours des deux dernières décennies, le développement de nouvelles technologies, en particulier celles liées à Internet, a créé d'incroyables possibilités qui ont modifié durablement notre vie privée et professionnelle et qui continueront de le faire. La sécurité Internet est donc devenue un facteur critique et verra son importance croître dans la mesure où les personnes et les appareils sont de plus en plus reliés. L'environnement de la sécurité Internet est marqué par des évolutions fulgurantes ainsi que des modifications de l'interface entre la technologie, l'économie et la société. Différents thèmes dans le domaine de la cyber-sécurité ont suscité à nouveau une forte attention. Les exemples les plus parlants sont les attaques par Distributed Denial of Service (DDoS) avec des millions d'appareils Internet of Things (IoT)[1], des vagues d'attaques soutenues de malwares, chiffrant toutes les données (privées et d'entreprise) et ne les libérant que contre paiement («Ransomware»), les fuites de données avec des millions de comptes utilisateurs concernés et des implications politiques , ainsi que le flux continu de failles logicielles.

De nombreuses cyber-attaques ont déjà des contre-mesures prometteuses, soit de nature technique soit de nature organisationnelle. Il n'est pas rare que des approches de solution connues ne soient pas utilisées, soit par ignorance de la solution, par hésitation ou par manque d'expérience des nouvelles approches, soit par manque de compréhension des effets et d'un contexte de la menace.

Nous expliquons dans ce rapport partant du point de vue de Swisscom les cyber-menaces continues résultant de failles logicielles ainsi que par des fuites de données massives et leurs conséquences sur la Suisse. Nous voulons améliorer la compréhension de ces menaces et de leurs conséquences, montrer les contre-mesures et partager nos propres expériences avec des approches de solutions innovantes. Nous espérons ainsi pouvoir apporter une contribution à la maîtrise commune des cyber-risques en Suisse.

Nous souhaitons en outre que cette publication apporte un éclairage sur notre programme Bug-Bounty. Nos expériences avec Bug Bounty sont très positives et nous souhaitons encourager d'autres entreprises en suisse à faire le pas pour améliorer la sécurité.

2 Situation – radar des menaces

Les menaces trouvent leur origine dans le développement constant de nouvelles technologies et de leur application et diffusion au sein de la société. Les menaces potentielles doivent être détectées de façon précoce et systématiquement répertoriées. Pour représenter l'état des menaces et leur évolution, nous utilisons un radar (figure 1).

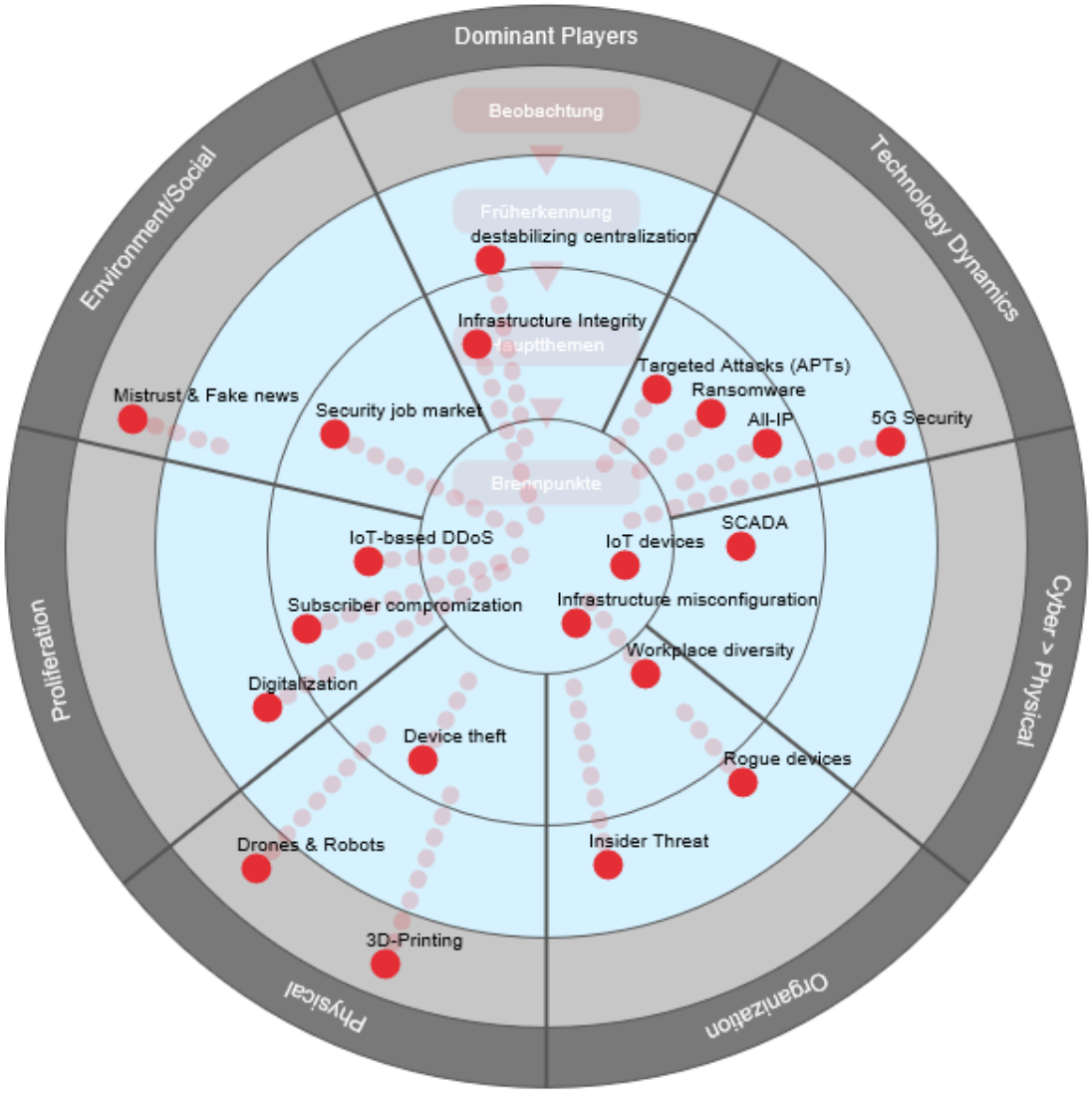

Figure 1 – Radar des menaces

2.1 Méthodologie

Le radar des menaces se compose de sept segments, délimitant les différents domaines des menaces. Il est possible de rattacher à chaque segment les menaces associées dans l'un des quatre anneaux concentriques. Les cercles présentent l'actualité de la menace et donc le manque de précision lié à la menace. Plus la

menace est proche du centre du cercle plus elle est concrète et plus les contre-mesures sont importantes. Nous considérons les anneaux comme des

- **Points délicats** pour les menaces, qui sont déjà réelles et qui sont gérées avec une mobilisation relativement importante de ressources.
- **Thèmes principaux** pour les menaces déjà survenues individuellement et gérées avec une mobilisation de ressources normale. On applique souvent des processus réguliers pour traiter efficacement de telles menaces.
- **Reconnaissance précoce** pour les menaces qui ne sont pas encore survenues ou qui montrent actuellement très peu d'effet. Des projets ont été lancés afin de pouvoir rapidement faire face à l'avenir à l'importance croissante de ces menaces.
- **Observation** pour les menaces qui ne surviendront que dans quelques années. Il n'y a pas de mesures concrètes pour la gestion de ces menaces.

Par ailleurs, les différentes menaces identifiées par ces points présentent une tendance. Celle-ci peut avoir une criticité en progression, en recul ou stable. La longueur du faisceau de tendance indique la rapidité escomptée de l'évolution de la criticité de la menace.

2.2 Menaces

2.2.1 Dominant players

Menaces résultant des dépendances aux éditeurs, services ou protocoles dominants.

Thèmes principaux	**Infrastructure Integrity:** Les principaux composants des infrastructures critiques peuvent injecter par négligence ou sciemment des failles mettant en péril la sécurité du système.
Détection précoce	**Destabilizing Centralization:** La centralisation forte dans la structure d'Internet crée des risques de masses compactes. La défaillance d'un service peut avoir des conséquences mondiales, comme cela s'est produit lors d'une défaillance de Amazon Web Services (AWS).

2.2.2 Technology dynamics

Menaces résultant de l'accélération de l'innovation technologique et donnant ainsi d'une part de nouvelles possibilités aux assaillants, et créant d'autre part de nouvelles menaces suite au développement.

Thèmes principaux	**Targeted attacks (APTs):** Les personnes-clé sont identifiées et attaquées de manière ciblée afin d'obtenir des informations pertinentes ou d'occasionner un maximum de dégâts.

	Ransomware: Les données sont largement chiffrées et sont à ensuite déchiffrées (éventuellement) contre le versement d'une rançon. **All-IP:** Dans la contexte de la mise en place de la technologie tout IP à couverture globale, les risques augmentent dans le contexte de la technologie VoIP.
Détection précoce	**5G Security:** La 5G est une technologie encore jeune dont la mise en place comporte de nombreuses chances ainsi que des risques encore inconnus.

2.2.3 Cyber goes physical

Les attaques utilisant les infrastructures dans le cyberespace provoqueront de plus en plus de dommages dans le monde physique.

Point délicat	**IoT Devices:** Les appareils insuffisamment protégés peuvent être compromis et sabotés. Ils peuvent ainsi voir leurs propres fonctions, par exemple leur disponibilité ou l'intégrité des données, restreintes.
Thèmes principaux	**SCADA:** Il continue à y avoir des systèmes de contrôle insuffisamment ou pas du tout protégés pour les installations des infrastructures critiques.

2.2.4 Organisation

Menaces résultant des changements dans l'organisation ou exploitant les failles qui y sont présentes.

Point délicat	**Infrastructure misconfiguration:** Exploitation des composants d'infrastructures mal configurés et/ou des failles identifiées et corrigées tardivement.
Thèmes principaux	**Workplace diversity:** Outre les nombreuses chances accompagnant les nouveaux modèles de travail, l'utilisation incontrôlée de ces modèles comme «Bring your own Device» (BYOD) ou l'utilisation accrue des postes de travail distants entraîne une exposition accrue aux risques.
Détection précoce	**Rogue devices:** Les appareils inconnus dans le réseau d'entreprise peuvent participer à des attaques directes ou être exposés à des attaques en raison d'une protection insuffisante. **Insider threat:** Manipulation, exploitation abusive ou vente d'informations de partenaires ou de collaborateur, par négligence ou de manière préméditée.

2.2.5 Physical

Menaces émanant de l'environnement physique et visant généralement des objectifs physiques.

Thèmes principaux	**Device theft:** Le vol, notamment de composant des infrastructures critiques ou, à l'avenir de plus en plus d'appareils IoT, peut donner lieu à des pertes de données ou perturber la disponibilité des services.
Détection précoce	**Drones and Robots:** La reconnaissance ou les attaques à de grandes distances deviennent plus simples et favorables. **3D-Printing:** La fabrication de clés par exemple ou d'autres appareils physiques est plus avantageuse et plus simple grâce à l'amélioration de la qualité des imprimantes 3D.

2.2.6 Proliferation

Menaces résultant des progrès en matière de disponibilité et d'accessibilité des médias informatiques et de l'expertise. D'une part parce que l'élargissement augmente les surfaces d'attaque et d'autre part parce que la disponibilité des outils d'attaque augmente.

Thèmes principaux	**IoT-based DDoS:** Une croissance forte associée à une faible protection des appareils IoT augmente le nombre des «candidats à la prise de contrôle» pour les botnets. **Subscriber compromization:** Les logiciels malveillants attaquent les données des utilisateurs ou sont utilisés pour les attaques contre les infrastructures de télécommunications ou informatiques.
Détection précoce	**Digitalization:** La mise en réseau de plus en plus importante des mondes virtuel et réel et de la vie privée et professionnelle multiplie les vecteurs d'attaque.

2.2.7 Environmental / Social

Menaces résultant des changements politiques et sociaux ou devenant plus aisées ou plus payantes grâce à ces changements.

Thèmes principaux	**Security job market:** Les besoins en professionnels de sécurité peuvent difficilement être couverts, ce qui se traduit par une pénurie d'expertise dans les interventions contre les attaques qui deviennent de plus en plus complexes et intelligentes.
Détection précoce	**Mistrust & fake news:** La perte de confiance à l'encontre des instances étatiques ou sociales peut contribuer à réduire les échanges d'informations pour l'identification et la défense contre des attaques potentielles.

2.3 Conclusion

Notre situation montre que l'état des menaces devient de plus en plus complexe. Les attaquants profitent de la valeur croissante des actifs à protéger, ce qui augmente la motivation pour une attaque ciblée et intelligente. Par ailleurs, les innovations techniques et le rapprochement des mondes physique et virtuel créent de nouvelles possibilités d'attaques. Les changements sociaux se répercutent sur la confiance et sur la manière dont nous travaillons ensemble. Les attaquants peuvent exploiter ces deux facteurs pour leurs besoins.

Les fonctions de sécurité chargées de la protection des personnes, des données et des installations peuvent utiliser ces changements technologiques et sociaux pour parer de manière ciblée et efficace les attaques.

Swisscom Security considère que la situation reste exigeante et comporte toujours de nouveaux défis, mais qui peuvent être maîtrisés grâce à des mesures appropriées.

3 Vol de données („Data Breaches“)

La numérisation croissante de notre société et de notre économie donnent lieu à une accumulation de données de toutes sortes, plus volumineuses et critiques, dans les entreprises, les administrations et chez les particuliers. La série de vols de données, qui s’est poursuivie depuis des années (ci-après désignées «Data Breach») s’est considérablement renforcée en 2016. Auparavant, les Data Breaches étaient considérés uniquement comme un problème de l’entreprise concernée et de ses clients. L’an passé, les effets sur le développement social et politique ont toutefois été clairement démontrés. Nous examinons ci-après les risques issus des Data Breaches du point de vue de la société, de Swisscom et de l’utilisateur, afin d’évaluer les effets sur les utilisateurs et les entreprises suisses. Nous soumettons l’examen de ces risques à une analyse de données actuelles à partir de sept importants Data Breaches ayant visé plus de 890 millions de comptes utilisateurs.
Le service de Data Breach Monitoring le plus connu haveibeenpwned.com (HIBP) a établi à plus de 2 milliards le nombre de comptes utilisateurs volés dans 187 Data Breaches confirmés intervenus ces dernières années.[2]

3.1 Des comptes suisses dans les Data Breaches

Pour illustrer le risque auquel les utilisateurs suisses sont exposés, nous avons évalué les données librement disponibles de sept Data Breaches importants survenus dernièrement. Le tableau de la figure 2 montre pour différents secteurs industriels et administrations de Suisse le nombre de comptes utilisateurs exposés par les Data Breaches d’*Adobe, Ashley-Madison, Badoo, Dropbox, Gawker, Linkedin* et *MySpace*. Dans l’ensemble, ces sept Data Breaches ont exposé 890 millions de comptes utilisateurs.

Catégorie	Total	Adobe	Ashley-Madison	Badoo	Dropbox	Gawker	LinkedIn	MySpace	Breach multiples
Date de l'intrusion		Oct 2013	Juil 2015	Juin 2013	Juil 2012	Déc 2010	Mai 2012	Juil 2008	
Date de la publication		Déc 2013	Août 2015	Juil 2016	Août 2016	Déc 2013	Mai 2016	Mai 2016	
Total comptes utilisateurs (mio)		**152.4**	**30.8**	**112.0**	**68.6**	**1.2**	**164.6**	**359.4**	
Index de l'entreprise									
Fortune 500 (International)	**2'958'767**	441'355	46'143	999'781	200'325	1'039	743'295	616'274	3%
Conseil (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 industrielles - Suisse									
Banques	**18'565**	2'792	53	512	1'100	22	13'831	677	2%
Assurances	**5'921**	936	44	671	584	1	3'595	309	4%
Entreprises de l'énergie	**6'107**	1'622	34	466	2'061	1	2'214	213	8%
Pharma/Chimie	**2'988**	519	18	174	351	1	1'917	127	4%
Médias- Suisse									
Imprimés	**599**	193	10	36	216	0	118	84	10%
Télévision & radio	**93**	23	2	18	28	0	22	14	16%
Administration - Suisse									
Administration fédérale	**3'070**	907	28	532	545	1	1'123	89	5%
Administration cantonale	**7'963**	2'276	45	1'622	2'453	0	1'867	188	6%
Entreprises fédérales	**4'680**	1'222	42	832	1'384	0	1'385	124	7%
Hautes écoles et hautes écoles	**66'124**	16'794	153	2'937	43'708	6	6'905	2'431	11%
Fournisseurs de messagerie - Suisse									
Services de messagerie	**291'277**	84'242	28'875	110'834	56'317	42	12'769	43'458	16%
Fournisseurs Internet (ISP)	**547'796**	241'725	19'234	148'319	118'277	66	54'290	54'731	17%

Figure 2 – Nombre de comptes utilisateurs exposés par des Data Breaches pour différents secteurs industriels en Suisse

Les noms de domaine des comptes utilisateurs de ces Data Breaches ont été comparés avec les noms de domaine des organisations des différents secteurs pour conduire cette analyse. La dernière colonne de la figure 2 indique par ailleurs combien de comptes utilisateur ont été compromis dans plus d'un Data Breach. Ces chiffres sont une estimation minimum, car nous n'avons analysé que les données de sept Data Breaches tandis que HIBP a actuellement une liste de 187 Data Breaches importants.

L'analyse montre par ailleurs que les autorités et les administrations sont tout autant concernées par ces Data Breaches que les grandes entreprises, les fournisseurs d'infrastructure, les hautes écoles ou les utilisateurs privés. Le secteur «Fournisseurs de messagerie Suisse» regroupe les comptes utilisateur des douze plus grands fournisseurs d'accès à Internet suisses et des portails de messagerie gratuite connus hotmail.ch, gmx.ch et gmail.ch. Ce secteur représente ainsi la majorité des comptes de messagerie suisses privés, dont au moins 800 000 sont concernés par des Data Breaches.

3.2 Les risques de la fonction «Oubli de mot de passe»

On pourrait argumenter que le dommage résultant des Data Breaches de LinkedIn et MySpace pour les personnes concernées est limité – dans la mesure où il s'agit de

portails de médias sociaux auxquels on confie volontairement des données. Dans le cas de Dropbox comme solution de stockage dans le Cloud, la situation est très différente. Dans tous les cas, cet examen simple est trop limité lorsque l'on tient compte du fait qu'une grande part des utilisateurs utilisent le même mot de passe pour différents services Internet. La situation devient critique lorsque les mots de passe sont également utilisés pour les comptes de messagerie. Si un de ces comptes e-mail est utilisé en guise de contact pour d'autres services Internet, la fonction «Mot de passe oublié» permet d'envoyer un nouveau mot de passe directement à cette adresse e-mail et elle tombe ainsi entre les mains de l'attaquant. Par la suite, l'attaquant a non seulement accès au compte de messagerie de la victime mais il peut aussi accéder à d'autres services du client. Le délai important entre l'intrusion effective et sa divulgation est fatal – les conséquences sont globales, y compris pour les utilisateurs en Suisse.
L'exemple ci-après illustre le caractère extrêmement concret de ce risque. Vers la fin août 2016, des voix se sont élevées dans la Security Community, informant que les données de Dropbox étaient négociées dans les forums Underground de référence . Peu de temps après, les données étaient disponibles librement sur Internet. Le 8 septembre, Swisscom enregistrait le même jour sur les serveurs de messagerie de Bluewin plus de 10 000 logins suspects et réussis depuis une adresse IP unique située à l'étranger. La figure 3 montre clairement cette activité pendant cette journée.

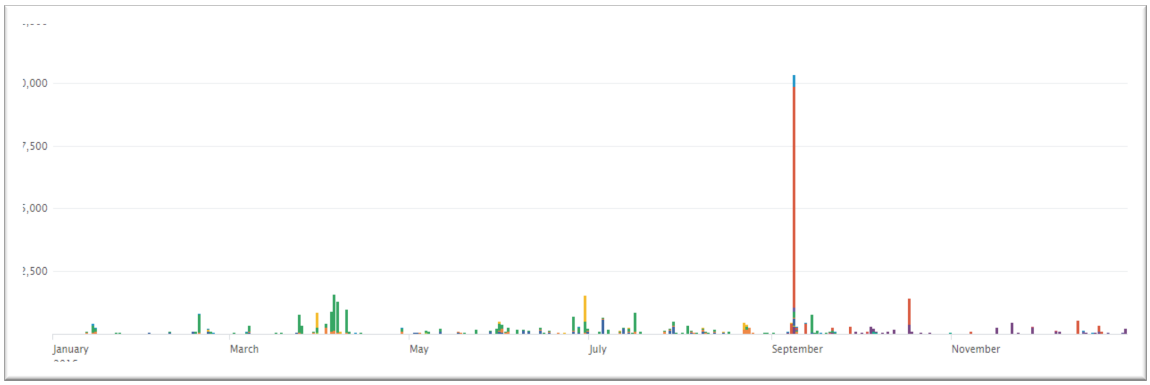

Figure 3 – Nombre d'inscriptions suspectes sur les serveurs de messagerie de bluewin en 2016

L'adresse IP à partir de laquelle les inscriptions émanaient a été immédiatement bloquée et les 10 000 comptes de messagerie déjà touchés ont été bloqués et leurs utilisateurs informés.
Swisscom a procédé dans la période comprise entre mars et décembre 2016 à un total de 83 928 blocages (y compris les blocages multiples) de 74 602 adresses de messagerie différentes. Près de la moitié, soit 34 892 de ces adresses de messagerie, ont été exposées par un ou plusieurs Data Breaches.
Ce résultat documente la démarche systématique et rapide des criminels après un Data Breach, ainsi que leur capacité à casser des mots de passe (ou la difficulté que rencontrent les utilisateurs pour choisir des mots de passe forts et multiples).

La protection effective des mots de passe par le hachage dépend dans une large mesure des critères ci-après contrôlés par l'utilisateur ou l'exploitant:

Utilisateurs	> Longueur du mot de passe > Caractères utilisables pour créer un mot de passe > Impossibilité de prévoir le mot de passe
Exploitant	> Choix de la fonction de hachage utilisée > Caractères autorisés pour créer un mot de passe > Longueur minimum et/ou maximum du mot de passe > Sécurité de l'implémentation

Différentes analyses de mots de passe à partir des plus importants Data Breaches du passé montrent malheureusement toujours la même situation[3]:

> La plupart des mots de passe sont trop courts, trop simples et sont ainsi prévisibles. La liste des mots de passe le plus souvent choisis n'évolue pas au fil des ans: Les 5 les plus courants sont «123456», «password», «12345», «12345678», «qwerty».
> Les utilisateurs utilisent un nombre restreint de mots de passe pour un nombre important de services différents. Ils utilisent en moyenne six mots de passe différents pour 24 services.

3.3 Parcours des données volées

En fonction de l'attaquant, les données ont un parcours variable après une intrusion. Dans un premier temps, les données sont examinées, évaluées et exploitées par les attaquants – sans publicité en direction de l'extérieur. Si la compromission de la cible est maintenue, l'attaquant a tout intérêt à garder le secret sur le Data Breach afin de ne pas menacer l'accès à la victime. Différentes options peuvent être envisagées pour tirer un profit maximum:

> les données sont proposées à la vente sur un marché Underground
> l'entreprise victime est rançonnée avec la menace de publier les données
> les données sont publiées sur Internet et sont ainsi librement accessibles.

Ces options sont appliquées dans le cas où l'attaquant ne peut pas ou ne veut pas utiliser lui-même les données, qu'il a terminé l'évaluation et que l'objectif initial a été atteint ou que l'intrusion a été détectée par des tiers ou par l'organisation affectée.
Les acteurs étatiques peuvent soit évaluer les données par eux-mêmes soit les publier à une date donnée sur les canaux appropriés pour en tirer un profit politique.
Il y de manière typique un délai important entre l'intrusion et le moment auquel les parties concernées (l'entreprise ou les clients) sont informées d'un Data Breach.
Il arrive souvent que les données de plusieurs Data Breaches soient disponibles librement sur Internet et accessibles pour quiconque à un moment donné, en partie

avec beaucoup de publicité. Entretemps, plusieurs organisations proposent des services alertant les clients lorsque leurs données sont publiées sur Internet ou dans l'Underground[4]. Des organisations moins sérieuses peuvent aussi proposer l'ensemble des données d'un Data Breach, sous forme de «Data Dump» à tout client prêt à payer pour cela, afin de les télécharger – y compris les mots de passe cassés. Le délai entre l'intrusion effective et la première publication de l'intrusion (par ex. la publication du Data Breach par l'entreprise visée elle-même ou par des tiers) peut se compter en années.

3.4 Conséquences pour la société et l'économie

Outre l'exploitation primaire des données pour l'espionnage et le vol de données afin de nuire aux victimes directes, les Data Breaches de 2016 montrent que le risque a pris une nouvelle dimension. Les résultats ci-après ont montré clairement les effets des Data Breaches sur le cours de l'histoire et sur l'évolution de la société.

Panama Leaks / Mossack Fonseca

Plus de 11,5 millions de documents confidentiels du cabinet d'avocats Mossack Fonseca couvrant la période 1970 à 2015 ont été communiqués aux médias en avril 2016[5]. Selon des estimations des médias concernés, les documents apportent la preuve de stratégies légales de contournement fiscal, mais aussi de délits fiscaux et de blanchiment d'argent, d'infractions aux sanctions des Nations Unies ou encore d'autres délits commis par les clients de Mossack Fonseca. Parmi les clients identifiés par le Data Breach figurent de nombreuses personnalités dans le monde entier, dont 143 hommes politiques, des chefs d'État et de gouvernement encore en fonctions ou pas. La fuite de données auprès de Mossack Fonesca a eu d'importantes conséquences pour certains clients, l'exemple le plus frappant étant la démission du premier ministre islandais après une vague de protestations suite aux révélations par les Panama Papers.

Campagne électorale aux États-Unis

Pendant la campagne électorale américaine, la société a été submergée de documents internes issus de la fuite du réseau du Democratic National Committee (DNC) et d'e-mails internes du directeur de campagne John Podesta[6]. Les informations révèlent les nombreux liens entre les milieux politiques, Wall Street et les clans internes au sein du parti démocrate – avec une influence potentielle sur les élections.

L'exploitation abusive de documents confidentiels peut contribuer à influencer, manipuler voire rançonner secrètement une personne visée. Lorsque des personnes de premier plan, des leaders du monde de l'économie ou des hommes politiques sont ainsi influencés dans leurs décisions et leurs actions, les conséquences pour l'économie ou la société sont potentiellement considérables. La manipulation est difficile à prouver et est dissimulée. L'intrusion au sein de Mossack Fonseca était

triviale, en raison d'une sécurité largement défaillante des système techniques, alors que les services secrets russes sont suspectés être à l'origine de l'intrusion dans le réseau DNC.

Nous devons désormais partir du principe que tant les services secrets que les cybercriminels sont depuis longtemps (et également aujourd'hui) en possession de données critiques d'autres organisations et qu'ils les exploitent discrètement pour leurs fins, y compris la manipulation de décideurs et de responsables politiques.

La protection contre de tels risques est une lourde tâche et exige beaucoup de discipline, tant dans la mise en place de l'infrastructure IT que dans le travail quotidien des collaborateurs. L'arbitrage entre la sécurité et le confort de travail doit être réalisé soigneusement et doit donner lieu à une communication solide, et être bien compris. On ne cesse d'observer que les utilisateurs, sont souvent très créatifs, généralement dans leur propre intérêt, pour contourner les contraintes et les mesures de protection techniques.

4 Programme Bug Bounty

Au cours des dernières décennies, les logiciels sont devenus un élément critique pour notre économie et notre société. L'interconnexion croissante au sein du réseau Internet conduit les logiciels à communiquer sans interruptions dans toutes sortes d'appareils avec les personnes et les machines – ce qui permet la mise en place de la société numérique. En dépit d'investissements énormes de l'industrie et de la recherche dans le développement de logiciels sécurisés, les faiblesses ou les failles de sécurité constituent un problème récurrent. L'exploitation des faiblesses des logiciels permet à un attaquant de compromettre, manipuler, contrôler, espionner ou saboter les systèmes ou les services concernés. Par ailleurs, l'histoire d'Internet montre sans conteste que la découverte de failles de sécurité logicielles ne peut pas être empêchée ou bloquée ni par le constructeur, l'utilisateur ou encore l'État. L'intérêt pour les failles logicielles critiques a considérablement augmenté ces dernières années, en particulier pour les criminels (profit) ou les acteurs étatiques (espionnage, sabotage). Cette situation s'est accompagnée par l'apparition d'un marché appliquant des tarifs élevés pour les failles logicielles critiques.[7] La société Zerodium offre par exemple plus d'un million de dollars pour une faille logicielle permettant de compromettre des appareils mobiles Apple[8].

4.1 Les limites de l'altruisme

Heureusement, de nombreux découvreurs de failles ont une attitude éthique et suivent le processus appelé «Coordinated Disclosure»[9]. Le développeur signale la faille au fabricant et lui laisse le temps de développer un patch de sécurité avant de publier la faille. Ceci implique toutefois que le développeur renonce à tirer profit de la vente de la faille. Ce modèle est toutefois de plus en plus remis en question face au développement extrêmement rapide du marché des failles logicielles dont les prix ne cessent de croître. En outre, on peut se poser des questions sur le fait que la cyber-sécurité de la société dépende de plus en plus dans une large mesure du comportement altruiste de découvreurs.

L'industrie commence à accepter l'idée que les découvreurs de failles soient récompensés pour leur comportement éthique. Les entreprises offrent lors de programmes «Bug Bounty» des récompenses (appelées Bug Bounties) pour le signalement de failles dans les produits ou les services. De grands éditeurs de logiciels les ont précédés avec ce modèle. Les expériences avec les Bug Bounties sont positives, tant financièrement que du point de vue de la sécurité, comme l'a montré une étude exhaustive des programmes Bug Bounty de Google et de Mozilla[10]. Les programmes Bug Bounty, qui étaient au départ l'exception, deviennent lentement mais sûrement, la norme – comme le prouve clairement la «The Bug Bounty List» de BugCrowd, qui regroupe actuellement près de 500 entreprises enregistrées avec un programme Bug Bounty[11].

4.2 Le programme Bug Bounty de Swisscom

Swisscom gère depuis septembre 2015 – et est d'ailleurs la première entreprise en Suisse à le faire – un programme Bug Bounty placé sous la responsabilité de notre «Computer Security Incident Response Team» (CSIRT)[12]. Le programme Bug Bounty a été lancé avec les objectifs suivants:

- Créer un interlocuteur central pour les signalements de failles
- Créer des incitations pour nous signaler directement les failles.
- Créer des processus optimisés pour le traitement des failles (processus internes et externes)
- Transparence sur les failles de sécurité concernant notre infrastructure (Realty Check)
- Assistance pour le processus de durcissement continu de notre infrastructure

L'objectif de notre programme Bug Bounty est de récompenser les découvreurs pour leurs efforts sur le rapport et la documentation de la faille. Toutes les activités associées à la découverte de la faille doivent se dérouler dans un cadre légal et ne doivent pas perturber le fonctionnement de notre infrastructure critique.

4.3 Evaluation d'une faille

Le montant du Bounty (récompense) se mesure au risque résultant de la faille et non pas à la nature technique ou à la complexité de la faille. Ainsi, une faille par «SQL Injection» donne lieu à une récompense plus importante si elle expose des données sensibles que pour des données non critiques. La fourchette de prix de notre programme Bug Bounty se situe entre 150 CHF et 10 000 CHF par faille.

4.4 Informations Bug Bounty

En 2016, le programme Bug Bounty de Swisscom a enregistré 281 annonces de la part de 54 découvreurs, concernant des produits ou des services utilisés par Swisscom. Sur ces annonces, plus de la moitié (157) des failles ont été qualifiées pour un Bounty. La majeure partie des failles, soit près de 75%, concernent différentes applications Web. Le tableau ci-après montre la distribution par criticité des différentes failles enregistrées.

Criticité	Nombre	Nature et conséquence
Élevé	1	> Failles critiques dans les appareils largement diffusés des clients > Failles critiques dans les fonctions d'authentification > Remote Code Execution
Moyenne	14	> Failles exploitables sous certaines conditions dans les appareils des clients > SQL Injection sans exposition des données sensibles > Cross Site Scripting (XSS) sur des sites Web extrêmement fréquentés
Faible	142	> Cross-Site-Scripting (XSS) dans des applications non critiques > Exposition de données non sensibles

L'an passé, près de 50 000 CHF ont été versés dans le cadre du programme Bug Bounty aux découvreurs de onze pays différents répartis sur quatre continents.

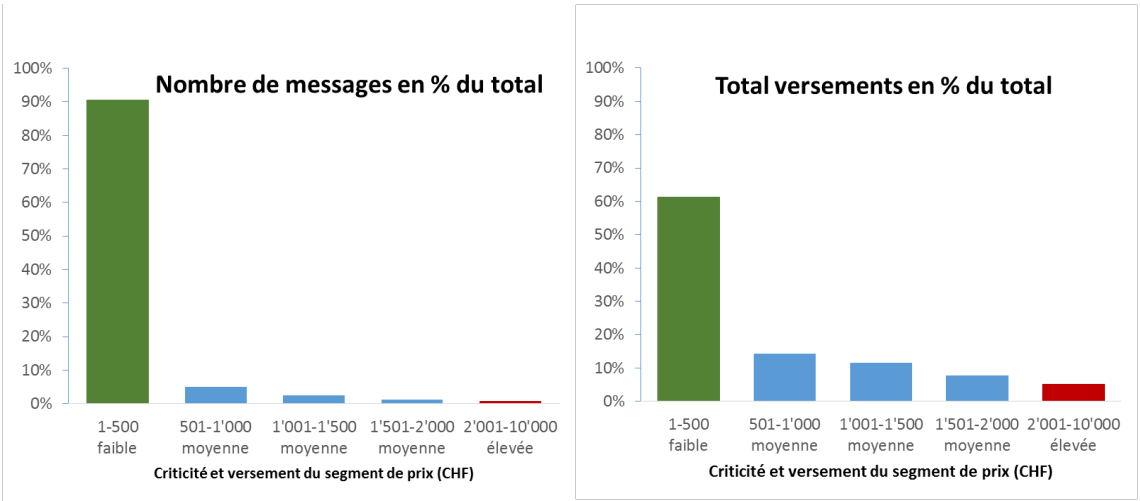

Figure 4 – Pourcentage de versements et nombre d'annonces par segment de prix

Pour l'année 2016, la figure 4 présente le rapport entre les versements de Bounty et le nombre d'annonces dans différents segments de prix.

> On trouve dans le segment des failles les moins critiques (Bounty entre 1 et 500 CHF) 90% des failles pour lesquelles 60% du montant total a été dépensé. La très grande majorité de ces failles concerne diverses applications Web, généralement de petites applications spéciales pour des projets individuels. La complexité de la faille et de sa correction est généralement peu élevée (par ex. correction par un changement de configuration). Le programme Bug Bounty permet désormais d'identifier et de corriger rapidement ces «problème anciens».

> Il y a, dans le segment des failles critiques (Bounty dès 2°000 CHF) un petit nombre d'annonces de failles mais donnant lieu au versement de montants importants pour les découvreurs. Le potentiel de dommages en cas d'exploitation abusive de la faille va de élevé à très élevé. Cette catégorie concerne notamment une faille dans le routeur Internet des clients.

4.5 Expériences

Le programme Bug Bounty, encore jeune, a permis de gagner en peu de temps des enseignements importants et de continuer à améliorer la sécurité de notre infrastructure.

> L'efficacité des initiatives en faveur de la sécurité interne est mesurable:
Les logiciels développés en interne par Swisscom présentent moins de failles que les logiciels achetés. Nos investissements dans le développement de logiciels sécurisés sont cohérents avec le programme Bug Bounty.
> Les domaines avec un besoin de rattrapage et ceux avec un niveau de sécurité élevé sont clairement reconnus.
> La conscience de la sécurité dans l'entrepris est renforcée.
> Les processus de traitement des failles ont été rationalisés.

Nos expériences avec le programme Bug Bounty sont extrêmement positives. Le programme constitue une amélioration rentable de la sécurité de notre infrastructure, contribue à établir des processus de Security importants et de rationaliser ceux qui existent, tout en améliorant la prise de conscience de la sécurité à touts les niveaux et dans tous les domaines. La décision d'être la première entreprise en Suisse à créer un programme Bug Bounty était courageuse et judicieuse, mais elle passe par le plein soutien du management. L'environnement juridique pour la gestion d'un programme Bug Bounty en Suisse n'est pas trivial, et il est souhaitable d'obtenir en la matière un soutien sur le plan de la législation.
Ces dernières années, les programmes Bug Bounty se sont généralisés dans le monde entier dans l'industrie et auront à l'avenir un rôle important dans le portefeuille des mesures visant à améliorer la sécurité. Pour les entreprises ne souhaitant pas (encore) mettre en place leur propre programme Bug Bounty, des entreprises comme Hackerzone[13] proposent ce service.

5 Que fait Swisscom?

Swisscom, en tant que grand fournisseur d'accès à Internet (FAI) comptant plusieurs millions d'accès Internet et de compte d'e-mail, est massivement et directement confronté aux Data Breaches, aux campagnes de Phishing, aux attaques de malwares et autres contre nous et nos clients. Notre principal objectif est d'assurer un accès Internet performant, sécurisé et sans barrière pour nos clients. D'une part, nous ne pouvons pas éviter que des systèmes clients soient compromis ou que leur données utilisateur soient exploitées de manière abusive par des Data Breaches externes. D'autre part, nous devons garantir que l'exploitation involontaire des accès clients ou des comptes utilisateurs créent des dommages collatéraux, affectant l'exploitation de l'infrastructure ou d'autres clients. Les mesures visant à maîtriser ce défi se décomposent en trois domaines *Prévention*, *Détection* et *Réaction*.

Alors que l'objectif de la prévention est dé parer les attaques, la détection et la réaction interviennent lorsque les attaques ont déjà eu lieu. La détection intelligente permet de prendre des mesures intelligentes de manière à éviter une plus grande extension («*lateral movement*») et un renforcement des attaques et à les contrer. La détection et la réaction sont ainsi étroitement associées. Les mesures de réaction doivent être efficaces et fonctionner sans avoir à surveiller le contenu du trafic du client.

5.1 Détection

Parmi les aspects de la détection pour la protection des accès Internet privés ainsi que les clients mobiles figurent notamment les *Spam Traps*, notre développement interne *Phishing Inspector* ainsi que les *Annonces des clients*.

Spam Traps	Les Spam Traps sont des adresses e-mail sans utilisateur, qui ont été créées pour identifier les e-mails non légitimes. Comme ces boîtes de messagerie n'ont pas d'utilisateur, les e-mails reçus sont exclusivement des envois illégitimes comme le spam, le Phishing ou les attaques de malware. Swisscom gère des milliers de comptes de messageries de ce type, dont le contenu est analysé et qui sont intégrés aux filtres de protection.
Phishing Inspector	Phishing Inspector analyse les pages Web d'adresses/URL suspectes afin d'identifier de manière fiable les sites de phishing. Les adresse des sites de phishing sont intégrées aux filtres de protection.
Annonces des clients	La boîte de messagerie spamreport@bluewin.ch permet aux clients de signaler directement les e-mails de phishing à Swisscom. Ce canal s'est avéré très efficace dans la lutte contre le phishing. Après un contrôle du contenu, cette information est intégrée aux filtres de protection.

Échange avec des pairs	Swisscom assure de nombreux échanges d'informations de sécurité pertinentes directement avec d'autres fournisseurs et les administrations. De nombreux fournisseurs Internet comme Swisscom utilisent le service www.antiphishing.ch géré par MELANI pour échanger mutuellement des informations en temps réel sur les attaques par hameçonnage et pour actualiser leurs filtres de protection.
Blacklists	Les blacklists sont des listes de noms de domaine, d'adresses IP ou d'e-mails qui ont eu un signalement négatif dans le passé, par exemple, par l'envoi en masse de spam ou de malwares ou par des tentatives d'attaques actives. Différentes organisations de Security constituent des blacklists spéciales. Les FAI et généralement les exploitants de serveurs de messagerie contrôlent lors de l'établissement de la communication si l'adresse de l'autre partie est enregistrée sur une blacklist. Le cas échéant, ceci donne généralement lieu à un refus, un délai, à un traitement spécial ou à un marquage comme spam. Swisscom utilise également plusieurs blacklists pour la protection des clients.

5.2 Utilisation du Machine Learning - Phishing Inspector

Phishing Inspector analyse de manière automatisée les pages Web d'adresses/URL suspectes, afin d'identifier de manière fiable par Machine Learning les pages de phishing à partir de plus de 100 propriétés. Les adresses Web suspectes des logs de Proxy du réseau mobile Swisscom sont transmises de manière automatique et anonyme à Phishing Inspector.

Phishing Inspector a été développé par Swisscom, a été mis en service au premier trimestre 2016 et constitue depuis une solution de sécurité robuste et très efficace. La précision de la classification automatique est supérieure à 97%. Ceci permet à Swisscom d'identifier un nombre important d'attaques par hameçonnage en temps réel, de manière fiable et avec des ressources réduites. Entre 80% et 90% des attaques détectées par Phishing Inspector ne sont pas bloquées lors de la détection par Google SafeBrowsing.

Entre 10 000 et 20 000 URL sont examinées quotidiennement et de 50 à 100 sites de phishing sont identifiés. Le top 10 des organisations le plus souvent visées par les attaques par hameçonnage sont *Apple, PayPal, UBS, Google, Swisscom, MasterCard, Amazon, Cembra, Facebook* et *PostFinance*.

Phishing Inspector bloque actuellement 2 652 domaines de sites de phishing. Près de 35 000 appels de clients des réseaux fixes et mobile sont enregistrés quotidiennement sur notre page d'alerte Phishing (voir figure 5).

5.3 Prévention

Les noms de domaines sont extraits des informations des différents mécanismes de détection et sont redirigés vers une page de mise en garde par la résolution des noms de nos serveurs de noms de domaine DNS. Ainsi, le serveur de noms de domaine DNS ne répond pas par l'adresse IP du domaine de l'attaquant mais par l'adresse IP aboutissant à une page Swisscom avec un message d'avertissement.
Ce mécanisme protège efficacement et en temps réel contre les attaques les réseaux privés et mobiles ainsi que les hotspots WLAN publics utilisant nos serveurs de noms de domaines DNS.

Figure 5 - *Page d'avertissement lors d'une tentative d'accès à une page de Phishing*

5.4 Réaction

Nous devons partir du principe qu'une partie de nos clients a déjà été compromise ou que la confidentialité des mots de passe des mailbox ou du login Swisscom n'est plus assurée, suite à un Data Breach. Nous distinguons à cet égard différents cas de compromission:

Compromission du client

Un ou plusieurs appareils du client sont compromis et l'accès Internet du client est exploité de manière abusive.

Compromission de la mailbox ou du login Swisscom

Si la confidentialité des informations d'accès n'est plus assurée, l'attaquant peut accéder aux mailbox de la victime et peut le cas échéant utiliser la fonction «Mot de

passe oublié» pour compromettre les comptes de la victime sur d'autres services. Les informations d'accès du login Swisscom permettent à l'attaquant d'exploiter de manière abusive les services Swisscom de la victime, y compris l'accès Internet.

La victime ignore habituellement qu'il y a eu compromission. De son point de vue, ses systèmes se comportent normalement. Ceci signifie d'une part un risque direct et durable pour le client. D'autre part, l'exploitation abusive du raccordement Internet et des systèmes du client met en danger d'autres utilisateurs Internet et services, par exemple:

> par l'envoi en masse de malwares ou de spam,
> par des tentatives d'intrusion sur d'autres systèmes sur Internet à partir du raccordement Internet du client,
> par la participation à des attaques par Distributed Denial of Service (DDoS) contre des tiers..

Lorsqu'une telle exploitation abusive a lieu, le risque est que le serveur de messagerie, les systèmes ou les réseaux de Swisscom soient enregistrés dans des blacklists. Les autres clients et les tiers non concernés sont alors fortement pénalisés, car les systèmes et les réseaux de la blacklist sont largement bloqués. Le défi pour un fournisseur d'accès à Internet est de protéger le mieux possible le client compromis avec une gêne minimale et en évitant les conséquences négatives sur l'infrastructure et les autres clients.

Nous disposons de deux mesures afin de protéger le client et d'éviter les dommages collatéraux. Elles sont déclenchées soient automatiquement soit manuellement après avoir constaté une exploitation abusive ou une compromission:

Cas (A) – Quarantaine du réseau

Swisscom a mis en place au fil des ans un processus de quarantaine sur plusieurs niveaux pour les raccordements Internet compromis. Lorsque nous constatons une compromission (ou une exploitation abusive volontaire) d'un raccordement Internet, celui-ci est terminé dans un réseau isolé en quarantaine. À quelques exceptions près, toutes les connexions Internet sont ainsi bloquées. Lorsqu'il essaie de se connecter, le client obtient une page d'information sur la mesure et sa raison ainsi que des informations d'assistance supplémentaires. Swisscom TV et la téléphonie ne sont pas concernés par le blocage. Il reste possible d'avoir des connexions assistant le client à résoudre le problème, par exemple à l'aide de logiciels antivirus, de mises à jour logicielles, etc.
Lorsque le client a résolu le problème, il peut réactiver lui-même l'accès Internet à l'aide de la page d'informations. À partir du troisième blocage dans un délai prédéfini, le blocage ne peut être désactivé qu'en appelant le Callcenter.

Cas (B) – Blocage du compte

Lors d'une compromission ou d'une exploitation abusive d'une mailbox, celle-ci est bloquée.
L'objectif est d'éviter que l'attaquant puisse lire la mailbox ou l'utiliser pour obtenir les mots de passe d'autres services. Le Swisscom Login permet au client de définir un nouveau mot de passe. Lors d'une compromission du Swisscom Login, celui-ci est bloqué. Ce n'est qu'après avoir identifié clairement le client autorisé que le blocage est annulé et qu'un nouveau mot de passe est défini.

On compte en moyenne 200 blocages de ce type chaque jour. La majorité de ces blocages est annulée par le client lui-même après avoir résolu le problème. La figure 6 montre le nombre de blocages quotidiens pour un période au cours de l'année 2016.

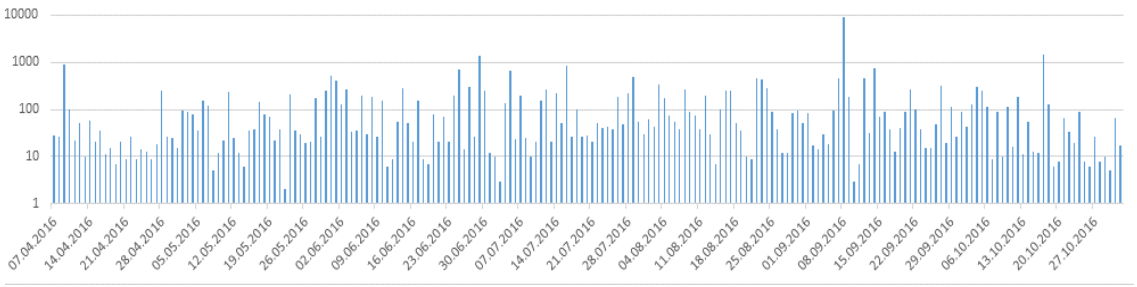

Figure 6 – Blocage de compte par jour entre avril et octobre 2016 (échelle logarithmique)

6 Résumé

Le réseau Internet a déclenché des bouleversements disruptifs. Du point de vue de la société comme de l'économie, nous sommes toujours dans la phase précoce de l'adaptation de ces possibilités. Bien entendu, ces développements donnent également lieu à de nouvelles menaces et à de nouveaux dangers. Il importe d'identifier ces menaces et de mettre en place activement des contre-mesures efficaces. Nous devons partir du principe qu'il y a actuellement et qu'il continuera à y avoir en circulation des failles logicielles non publiées ainsi que des données considérables issues de Data Breaches qui n'ont pas encore été publiés. Les causes de nombreuses cyber-menaces sont souvent techniques, mais les contre-mesures efficaces ne doivent pas être recherchées uniquement dans les approches techniques. Les programmes Bug Bounty n'empêchent pas les failles mais ils permettent toutefois une communication (et une compensation) coordonnée, efficace et équitable sur la sécurité entre les participants et contribuent à améliorer la sécurité de manière effective et mesurable. Il apparaît souhaitable que les entreprises examinent sérieusement le thème Bug Bounty et le mettent en place pendant que le législateur écarte les incertitudes sur ce thème.

Chaque utilisateur peut, grâce à la connaissance du contexte et à un peu de discipline, réduire sensiblement les effets des Data Breaches à venir en choisissant et en utilisant ses mots de passe.

Il convient de tirer les enseignements des nombreuses connaissances recueillies par le passé. Il importe d'éviter les erreurs connues et évitables.

Dans ce rapport, nous avons abordé le thème des Data Breaches et des failles logicielles, nous avons partagé nos expériences et nous avons esquissé des approches de solutions possibles.

Nous voulons ainsi apporter une contribution à la maîtrise commune des cyber-risques en Suisse.

---

[1] «Mirai: Telekom-Router nur Kollateralopfer» |Mirai: le routeur télécom, une victime collatérale], 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://fr.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