6 mai 2024 | Office fédéral de la cybersécurité OFCS

Rapport semestriel 2023/II (juillet – décembre)

Sécurité de l'information

La situation en Suisse et sur le plan international

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de la défense,
de la protection de la population et des sports DDPS
Office fédéral de la cybersécurité OFCS

Table des matières

Résumé **4**

Éditorial **5**

1 Thème prioritaire: les défis de la cybersécurité **7**

1.1 Identifier les cybermenaces et informer ***7***

1.2 Sensibilisation ***8***

1.3 Donner des conseils pour se protéger et renforcer la résilience ***9***

1.4 Label cyber-safe.ch: les expériences d'une commune vaudoise ***10***

1.4.1 Vers une sensibilisation à la cybersécurité *10*

1.4.2 Processus d'obtention du label cyber-safe.ch *10*

1.4.3 Utilité, défis et chances pour les communes *10*

1.4.4 Conclusion *11*

1.5 Enregistrer les incidents et donner des recommandations aux victimes ***11***

1.6 Protéger et soutenir les infrastructures critiques ***12***

1.7 Réduire les vulnérabilités ***12***

1.8 Poursuite pénale de la cybercriminalité ***13***

2 Annonces émises par des entreprises et la population **15**

2.1 Aperçu des annonces de cyberincidents ***15***

2.2 Escroquerie ***17***

2.2.1 L'escroquerie toujours à l'origine de la plupart des signalements *17*

2.2.2 Premières tentatives d'escroquerie à l'aide de l'intelligence artificielle (IA) *18*

2.3 Signalements d'hameçonnage ***20***

2.3.1 Hameçonnage en chaîne, concernant des paquets postaux et des factures payées à double *20*

2.3.2 La réapparition de l'hameçonnage par téléphone *21*

2.4 Signalements de maliciels et de piratage ***22***

2.4.1 Rançongiciels *22*

2.4.2 Signalements de piratage *23*

2.4.3 Les hôtels dans le viseur *23*

3 Situation **24**

3.1 Accès initial à l'aide de maliciels (chevaux de Troie) ***24***

3.2 Vulnérabilités: Ivanti CVE-2023-35078 et CVE-2023-35081 ..... ***25***

3.3 Rançongiciels ***27***

3.3.1 Incidents de rançongiciels *27*

3.3.2 Suivi des variantes de rançongiciels et des acteurs *29*

3.4 Fuites de données / Gestion des données ***31***

3.4.1 Fuites de données dans le secteur de la santé (à l'international) *32*

3.4.2 Fuite de données à la ville de Baden 33
3.5 Systèmes de contrôle industriels (SCI) et technologie opérationnelle (TO) . 35
3.5.1 La plus grande agilité des acteurs étatiques dans le domaine des TO 36
3.5.2 Perturbation de l'approvisionnement en eau par des hacktivistes..... 36
3.5.3 Appareils IoT utilisés comme infrastructure d'attaque 37
3.6 Le cyber dans les conflits..... 38
3.6.1 La guerre en Ukraine..... 39
3.6.2 Conflit au Proche-Orient..... 40
3.6.3 Développements futurs..... 41

Résumé

Le Centre national pour la cybersécurité (NCSC) est devenu l'Office fédéral de la cybersécurité (OFCS) le 1er janvier 2024. L'office profite de cette transformation pour mettre l'accent sur les différents champs d'activité de la Confédération dans le domaine de la cybersécurité, avec deux articles d'invités consacrés aux défis à relever sur le plan de la poursuite pénale et de la certification de la cybersécurité dans les communes.

Hausse des signalements durant le deuxième semestre 2023

Au cours du deuxième semestre de l'année 2023, le NCSC encore appelé ainsi à l'époque a reçu 30'331 signalements de cyberincidents, ce qui représente presque un doublement des cas par rapport au second semestre en 2022 (16'951 signalements). Cette hausse est surtout due à des offres d'emploi frauduleuses et à des appels frauduleux se faisant passer pour la police.

Durant le deuxième semestre 2023, les annonces d'escroquerie figuraient également parmi les cyberincidents les plus signalés au NCSC. Les tentatives d'escroquerie signalées par les entreprises relèvent pour la plupart des catégories de «l'arnaque au président», avec 253 signalements (contre 190 annonces pour la même période en 2022), et de «la fraude à la facturation», avec 63 signalements (contre 45 en 2022). Ainsi ce type d'annonce a connu une légère augmentation. Les signalements d'attaques par rançongiciel contre des entreprises ont en revanche quant à eux reculé, passant de 54 au cours du deuxième semestre 2022 à 42 pour la même période en 2023.

Tentatives d'escroquerie par intelligence artificielle (IA)

Durant la période sous revue, le NCSC a reçu davantage de signalements de tentatives d'escroquerie impliquant l'intelligence artificielle (IA). Les annonces portaient entre autres sur des attaques de sextorsion avec des images générées par l'IA et sur des appels téléphoniques et des fraudes à l'investissement au nom de personnalités connues. Au vu du nombre relativement peu élevé d'annonces dans ce domaine, le NCSC est d'avis qu'il pourrait s'agir de premiers essais de la part des cybercriminels pour analyser comment l'IA pourrait à l'avenir être utilisés lucrativement pour des cyberattaques.

Hameçonnage toujours en vogue (deuxième place)

Par rapport à la même période de l'année précédente, les signalements d'hameçonnage ont plus que doublé au cours du deuxième semestre, passant de 2'179 à 5'536. Nous mentionnerons plus particulièrement l'«hameçonnage en chaîne», par lequel des pirates envoient des courriels à toutes les adresses enregistrées de boîtes de réception préalablement piratées. Étant donné que l'expéditeur est supposé être connu des destinataires, la probabilité est grande que ceux-ci tombent dans le piège. Ensuite, tous les contacts existants du compte courriel suivant piraté reçoivent à leur tour un courriel d'hameçonnage.

Éditorial

L'Office fédéral de la cybersécurité: pour renforcer la cybersécurité de la Suisse

Depuis le 1er janvier 2024, le Centre national pour la cybersécurité (NCSC), jusque-là rattaché au Département fédéral des finances (DFF), a été transformé en l'Office fédéral de la cybersécurité (OFCS), rattaché au Département fédéral de la défense, de la protection de la population et des sports (DDPS).

Malgré ce changement, le mandat de base de cet organe reste inchangé, à savoir protéger la Suisse de manière préventive contre les cyberrisques, fournir son appui en cas d'incidents cyber et identifier les opportunités pour la Suisse de stratégiquement bien se positionner dans le cyberespace. Le but premier est de donner aux organisations et aux personnes les moyens de comprendre les cyberrisques et d'organiser la cybersécurité en fonction des risques qu'elles sont prêtes à prendre. Pour ce faire, l'OFCS établit des mécanismes économiques et sociétaux avec ses partenaires, afin de faire d'une part baisser les risques systémiques et permettre d'autre part de maîtriser les coûts liés à la gestion des cyberrisques. La Suisse devient ainsi un endroit attrayant pour les entreprises qui se meuvent dans l'espace digital.

Parmi les défis auxquels est actuellement confrontée la cybersécurité en Suisse, nous retrouvons la grande vulnérabilité des systèmes informatiques, une capacité de réaction encore faible en cas d'incidents et de crises informatiques qui affectent le système, ainsi qu'un manque de transparence et des données lacunaires pour catégoriser et jeter un regard critique sur les déclarations d'experts et d'organisations sur la cybersécurité. Ces facteurs de risque font que les cyberattaques aboutissent bien trop souvent, ce qui se traduit à son tour par des dommages économiques importants et un risque élevé de défaillance des infrastructures critiques. Les signalements de cyberincidents impliquant des dommages augmentent en moyenne de 30% par an. Or, même si la situation peut sembler dramatique, il faut bien comprendre que ces chiffres, au vu de l'utilisation toujours plus intense de l'espace digital, sont parfaitement plausibles. En comparaison internationale, la Suisse se situe dans la moyenne. La situation doit toutefois être prise au sérieux et améliorée. Pour ce faire, l'OFCS se focalise sur quatre champs stratégiques, que sont une meilleure compréhension des cybermenaces, une mise à disposition de moyens pour empêcher les cyberattaques, une réduction des dommages causés par ces incidents ainsi qu'une amélioration de la sécurité des produits et prestations digitaux. Vous pouvez découvrir ce que cela signifie concrètement dans la stratégie de l'OFCS récemment publiée.

Un facteur central de succès réside dans les collaboratrices et collaborateurs. L'OFCS souhaite être un employeur attrayant, pour attirer plus de personnel et pour engager de nouveaux talents, qui lui permettront d'axer ses prestations et produits le plus efficacement et qualitativement possible sur les besoins de la politique, de l'économie et de la société civile. Pour y parvenir, l'OFCS doit être flexible et pouvoir rapidement adapter son organisation aux nouvelles exigences et réalités économiques. Cela n'est faisable que lorsque ses équipes peuvent agir de manière aussi autonome que possible et que les décisions peuvent être prises de manière indépendante ou être du moins influencées de manière significatives par les collaboratrices et collaborateurs qui dispose de connaissances techniques nécessaires. De telles décisions doivent souvent être prises rapidement, ce qui permet une culture de l'erreur aussi ouverte qu'objective. Je préfère ainsi que nous fassions des erreurs contrôlées tout en restant

novateurs, plutôt que de ne pas faire d'erreurs et de rester passifs, raison pour laquelle il est d'autant plus important de maintenir l'excellence opérationnelle à un niveau élevé tout en fournissant des résultats fiables et cohérents. Tout cela repose sur un personnel aussi diversifié que possible, qui ne cesse de remettre en question son propre travail ainsi que celui de la direction de l'office, de manière constructive. Bien sûr, nous n'en sommes pas encore tout à fait là, mais nous avons fait des pas importants dans cette direction, preuve en est, selon moi, l'excellent travail accompli par nos collaboratrices et collaborateurs.

Chères lectrices et chers lecteurs, il est important pour nous d'avoir vos retours et aussi d'entendre vos critiques constructives dans le cas où l'OFCS devait ne pas répondre à vos attentes. Dans cette phase de développement importante de l'office, nous en avons plus que jamais besoin. Au final, nous visons l'aménagement avec vous d'un cyberespace libre et sûr pour le bien de toutes et tous.

Florian Schütz, directeur de l'Office fédéral de la cybersécurité

1 Thème prioritaire: les défis de la cybersécurité

La cybersécurité et la protection de la Suisse contre les cyberrisques sont une tâche commune de la société, l'économie et l'État. Toutes les parties prenantes sont tenues de prendre des mesures appropriées dans leur sphère de compétence et d'influence.

Comme dans de nombreux autres secteurs, le principe de la responsabilité individuelle s'applique aussi à la cybersécurité. Il y a toutefois des enjeux qui dépassent les capacités et les possibilités des individus et des organisations, dès lors l'État doit apporter son aide ou assumer certaines tâches.

Avec le Centre national pour la cybersécurité (NCSC[1]), aujourd'hui devenu l'Office fédéral de la cybersécurité (OFCS), qui joue le rôle de centre de compétences de la Confédération en matière de cybersécurité, le Conseil fédéral a créé une structure permettant de faire face à différents défis dans le domaine de la cybersécurité, sur un plan étatique.

1.1 Identifier les cybermenaces et informer

Pour savoir ce à quoi il faut faire attention et définir les mesures à prendre, il est important de connaître les phénomènes actuels. Posséder des informations sur ce qui se passe et sur les évolutions en cours aide à évaluer les risques et à prendre les décisions qui s'imposent. L'OFCS dispose d'une bonne vue d'ensemble des événements et des formes de menaces actuels grâce aux annonces reçues par la population et les entreprises (voir chap. 1.5 et 2), aux contacts qu'il entretient avec les exploitants d'infrastructures critiques (voir chap. 1.6) et au réseau national et international d'organisations partenaires.

L'OFCS traite ces informations sur la situation adéquatement en fonction des groupes cibles et fournit en conséquence à divers cercles de destinataires les informations pertinentes pour les sensibiliser (voir chap. 1.2) et les aider à prendre les mesures nécessaires à leur protection (voir chap. 1.3 et 1.5).

Recommandations

Lisez les anciens rapports semestriels et rendez-vous régulièrement sur le site de l'OFCS.

Vous trouverez également des informations utiles sur les phénomènes, menaces et mesures de protection actuels sur d'autres sites web tels que cybercrimepolice.ch (uniquement en allemand) et «eBanking – en toute sécurité!» (ebas.ch).

[1] National Cyber Security Centre, voir Finlande: NCSC-FI (kyberturvallisuuskeskus.fi); Irlande: National Cyber Security Centre (ncsc.gov.ie); Lettonie: National Cyber Security Centre (nksc.lt); Pays-Bas: National Cyber Security Centre (ncsc.nl), Norvège: Norwegian National Cyber Security Centre (nsm.no) et Royaume-Uni: National Cyber Security Centre (ncsc.gov.uk). Quelques pays ont des désignations spécifiques propres à leurs unités correspondantes, comme l'Allemagne: BSI - Bundesamt für Sicherheit in der Informationstechnik (bsi.bund.de); la France: ANSSI - Agence nationale de la sécurité des systèmes d'information (cyber.gouv.fr) ou les États-Unis: Cybersecurity & Infrastructure Security Agency – America's Cyber Defense Agency (cisa.gov). Quant à l'Australie et au Canada, ils mettent l'accent sur leur pays directement dans le titre: Australian Cyber Security Centre ACSC (cyber.gov.au) et Centre canadien pour la cybersécurité (cyber.gc.ca/fr). Voir aussi le Centre pour la cybersécurité Belgique (belgium.be) et le Cyber Security Agency of Singapore (csa.gov.sg).

1.2 Sensibilisation

Dans le domaine de la cybersécurité, les mesures de sensibilisation et de prévention revêtent une importance élémentaire, car la neutralisation d'un cyberincident est beaucoup plus fastidieuse que la mise en place de mesures préventives plus facilement applicables permettant à chacune et chacun de se mouvoir en toute sécurité dans l'espace digital. C'est la raison pour laquelle l'OFCS publie des informations sur la cybersécurité et des recommandations sur des mesures préventives contre les cyberattaques. Dans le cadre de la Cyberstratégie nationale (CSN), le NCSC a formulé des approches avec des représentants de l'économie, des autorités, de la population et des instituts de formation, afin de les informer et sensibiliser d'une part sur la thématique. En outre, des recommandations d'action ont été élaborées en fonction des groupes cibles, permettant aux personnes et aux organisations concernées de prendre elles-mêmes des mesures pour se protéger.

Pour accomplir cette tâche en fonction des besoins exprimés, l'OFCS peut s'appuyer premièrement sur ses propres constats tirés de ses activités opérationnelles. Deuxièmement, il coordonne entre autres les efforts visant à améliorer la cyberrésilience à l'échelle du pays. Il conçoit troisièmement des mesures de protection en étroite collaboration avec des partenaires externes tels que la Prévention suisse de la criminalité, la plateforme «eBanking – en toute sécurité!» de la Haute école de Lucerne, la *Swiss Internet Security Alliance* ainsi que d'autres organisations et organes existants. Ces mesures et recommandations peuvent être individuellement mises en œuvre par les différents groupes cibles définis, qui constituent le public dans leur ensemble, en fonction du degré selon lequel ils sont affectés.

C'est ainsi que des projets pilotes sont par exemple menés dans le secteur de l'économie, comme dans la branche logistique, dans l'industrie de transformation des métaux ou dans des entreprises familiales. Les constats qui en résultent sont idéalement par la suite discutés et développés avec les associations professionnelles compétentes avant d'être mis à la disposition des divers secteurs économiques. L'OFCS mène par ailleurs à travers tout le pays des campagnes destinées à la population en collaboration avec des partenaires externes. Ces campagnes visent à donner des informations sur la cybersécurité et mettent à la disposition de toute personne ayant des appareils numériques et un accès Internet des outils faciles à utiliser pour se protéger contre la cybercriminalité. Tous les efforts entrepris sont régulièrement examinés et évalués, afin qu'ils puissent être optimisés quant à leur mise en œuvre et à leur efficacité.

Recommandations

Renseignez-vous régulièrement sur les événements actuels qui peuvent menacer votre cybersécurité ou celle de votre entreprise. Sur les sites web de l'OFCS, de la Prévention suisse de la criminalité, de la plateforme «eBanking – en toute sécurité!», de la plateforme de sécurité Internet iBarry ou de la campagne de prévention s-u-p-e-r.ch, vous trouverez de nombreuses informations pour les privés, les entreprises, les autorités et les spécialistes informatiques.

Parlez de la cybersécurité, du traitement des données et de la cybercriminalité avec des collègues, des membres de votre famille et des connaissances.

1.3 Donner des conseils pour se protéger et renforcer la résilience

L'Office fédéral pour l'approvisionnement économique du pays (OFAE) a développé la norme minimale pour les TIC, en collaboration avec l'OFCS et la branche économique, afin de pouvoir mettre à la disposition des entreprises des consignes systématiques pour l'aménagement de leur cybersécurité. La norme minimale pour les TIC regroupe différentes normes internationalement reconnues et doit contribuer à l'amélioration de la résilience TIC. La norme en tant que telle et l'outil d'évaluation associé sont régulièrement actualisés.

Des normes sectorielles ont été élaborées et publiées en collaboration avec les associations professionnelles et des représentants desdits secteurs pour différents secteurs critiques, afin de mieux prendre en compte les exigences spécifiques à ces derniers. Ces normes revêtent en principe aussi le caractère de recommandations.

Cependant dans certains secteurs, des aspects des normes TIC minimales ont été qualifiées de contraignantes. L'Office fédéral de l'énergie (OFEN) a par exemple décidé que les normes TIC minimales pour l'approvisionnement en énergie et en gaz étaient contraignantes. Pour le secteur de l'électricité, cette obligation s'applique depuis 2024 et s'appliquera dès 2025 pour celui du gaz. En plus, l'Office fédéral des transports (OFT) a publié à l'automne 2023 la directive sur la cybersécurité ferroviaire (RL CySec-Rail). La nouvelle directive décrit les exigences minimales d'un système de management de la sécurité de l'information (ISMS) que les entreprises ferroviaires doivent mettre en place et gérer. La directive CySec-Rail, qui entrera en vigueur le 1er juillet 2024, se réfère à la "norme minimale pour les TIC destinée aux entreprises de transport public", publiée en 2020.[2]

L'OFCS apporte pour sa part son aide avec des consignes et des recommandations sur différents thèmes, tels que la sécurité des sites web,[3] la protection des systèmes de contrôle industriels[4] et des appareils liés à l'Internet des objets[5] ou la collaboration avec des prestataires de services informatiques.[6]

Conclusion / Recommandation

Vous trouverez de nombreuses informations utiles sur la cybersécurité sur le site web de l'OFCS.

La norme minimale pour les TIC et les normes minimales par secteur élaborées par l'OFAE en collaboration avec le secteur de l'économie sont des recommandations qui servent de points d'orientation pour se protéger contre les menaces liées aux cyberrisques.

2 Directive en matière de cybersécurité (bav.admin.ch)

3 Mesures de protection pour les systèmes de gestion des contenus (ncsc.admin.ch); mesures contre les attaques DDoS (ncsc.admin.ch)

4 Mesures de protection pour les systèmes de contrôle industriels (SCI) (ncsc.admin.ch)

5 Sécurité de l'Internet des objets (ncsc.admin.ch)

6 Collaborer avec des prestataires externes de services informatiques (ncsc.admin.ch)

1.4 Label cyber-safe.ch: les expériences d'une commune vaudoise

Contribution de Kilian Cuche, conseiller communal à Pomy/VD

La commune de Pomy (900 habitants), sise dans le district du Jura-Nord vaudois, a obtenu à la fin 2023 le label suisse de cybersécurité cyber-safe.ch, après deux ans et demi de travail. Cet article vise à présenter le processus allant du relevé de l'état actuel aux avantages de la mise en œuvre et à mettre en lumière les défis et les opportunités que cela représente pour les communes.

1.4.1 Vers une sensibilisation à la cybersécurité

En 2021, après un événement de l'Union des communes vaudoises (UCV) sur le thème de la cybersécurité, l'idée a émergé de procéder à un état des lieux de la question pour la commune de Pomy et d'apporter des améliorations. Lors de la conférence, le label cyber-safe.ch a été présenté, ce qui nous a servi de point de départ. Bien sûr, il a d'abord fallu convaincre l'entièreté du Conseil communal de la nécessité d'investir dans la cybersécurité. Pour ce faire, l'association cyber-safe.ch nous a montré, sur la base d'un premier questionnaire, les coûts qui pourraient être causés par une cyberattaque, en fonction de la taille de notre infrastructure et de l'étendue de nos données. Ce rapport nous a été très utile, car il a clairement mis en évidence le rapport entre les coûts et l'utilité inhérents à un investissement dans la cybersécurité. La commune de Pomy a très vite été convaincue de la nécessité d'investir dans ce sens et a démarré au printemps 2021 le processus en vue de l'obtention du label susmentionné. La cyberattaque dirigée contre la commune de Rolle, intervenue quelques mois plus tard à peine, nous a ensuite encore confortés dans notre volonté d'améliorer la cybersécurité de la commune.

1.4.2 Processus d'obtention du label cyber-safe.ch

La première étape menant à l'obtention du label cyber-safe.ch a consisté en l'établissement d'un rapport sur la base de questionnaires, de tests d'hameçonnage et d'une analyse de notre structure informatique (telle que l'examen de détection des failles de sécurité). Grâce à ce rapport, un état des lieux a été fait sur la cybersécurité de la commune, permettant ensuite d'identifier des mesures prioritaires, lesquelles ont dû être mises en œuvre en guise de prérequis à l'obtention du label. En d'autres termes, nous avons reçu une liste des points remplis et non remplis, sur la base de laquelle nous avons pu établir un plan d'action pour la préparation de la certification. C'est ensuite qu'est intervenue la partie la plus importante du travail, à savoir la mise en œuvre des mesures correctives. De l'administration des mises à jour jusqu'à la sécurisation physique de notre infrastructure en passant par le contrôle des sauvegardes et la formation des utilisatrices et utilisateurs, tous les éléments essentiels de la cybersécurité ont été passés sous la loupe, vérifiés, adaptés et corrigés. Deux ans plus tard, nous avons effectué un premier audit, au cours duquel il a été constaté que quelques non-conformités étaient encore présentes. Nous avons ensuite travaillé à les éliminer et avons finalement reçu la certification cyber-safe.ch après un deuxième audit.

1.4.3 Utilité, défis et chances pour les communes

Le label cyber-safe.ch a été pour nous un instrument idéal pour améliorer notre cybersécurité. Un regard indépendant de notre administration et de notre prestataire informatique porté sur

notre infrastructure a permis d'identifier le potentiel d'amélioration de manière étendue et intégrale. Nous avons été accompagnés dans le processus avec professionnalisme et aussi avec une grande compréhension pour les défis auxquels font face les petites communes. Parmi ces derniers, je pense notamment au fait que notre Conseil communal est exclusivement composé de politiciens de milice, qui ont tous leurs limites pour ce qui est du temps disponible, des compétences mais aussi des connaissances dans le domaine de la cybersécurité. Tous ces paramètres ont été pris en compte et une solution adaptée à notre contexte a pu être trouvée. Il est aussi réjouissant de constater que plusieurs cantons mettent de plus en plus d'argent à la disposition des communes afin de les soutenir dans l'amélioration de la cybersécurité. Ces efforts devraient être consolidés et coordonnés au niveau suisse.

1.4.4 Conclusion

Bien que notre infrastructure, dotée de deux places de travail, d'un serveur et de quelques périphériques BYOD,[7] soit très petite, il ne faut pas sous-estimer la charge de travail en vue de l'obtention d'un label de cybersécurité tel que cyber-safe.ch. La plus grande partie des mesures sont en effet indépendantes de la taille de l'infrastructure. Les responsables du label nous ont toutefois accompagnés de manière pragmatique, en s'adaptant à la fois à nos besoins et aux différentes réalités rencontrées sur place. Obtenir le label n'a donc rien d'une mission impossible. Avec un bon accompagnement, une bonne gestion du changement vis-à-vis du personnel et un soutien adéquat par le prestataire informatique, une amélioration de la cybersécurité est possible pour toutes les communes suisses et devrait faire partie de chaque planification informatique communale. Au final, il en va en effet de la sécurité des données de nos citoyennes et citoyens et de la protection des infrastructures critiques qui sont sous la responsabilité des communes.

1.5 Enregistrer les incidents et donner des recommandations aux victimes

L'OFCS est doté d'un service de guichet qui reçoit les annonces de cyberincidents et de cybermenaces. Celui-ci catégorise les annonces entrantes et procède à une première analyse, sur la base de laquelle des mesures peuvent être prises et des examens plus approfondis peuvent être effectués. Il convient d'aider les auteurs des signalements aussi rapidement, pragmatiquement et professionnellement que possible, leurs questions doivent donc recevoir des réponses directes. Ces personnes reçoivent par ailleurs des recommandations pour la marche à suivre et/ou sont renvoyées aux organes compétents. En sa qualité de guichet national centralisé pour les signalements et les questions dans le domaine cyber, l'OFCS travaille étroitement avec des autorités de la Confédération, des cantons et de la poursuite pénale, mais également avec des organisations et partenaires internationaux ainsi que des partenaires privés tels que des prestataires de service. L'OFCS veille en outre à ce que les informations frauduleuses telles que des sites web, adresses électroniques, numéros de téléphone, etc. soient transmis aux organes compétents, afin que ceux-ci puissent à leur tour prendre les mesures qui s'imposent.

[7] BYOD signifie "bring your own device", cf. Bring your own device (wikipedia.org)

Grâce à ces signalements entrants, l'OFCS peut identifier de nouvelles tendances et modes opératoires dans le domaine cyber. L'ensemble des cas ainsi obtenu à l'aide des signalements complète la vue d'ensemble de la situation cyber actuelle (voir chap. 1.1). L'évolution de ces phénomènes est analysée en continu, afin que la population et les entreprises puissent être averties en cas d'aggravation de la menace. Les chiffres relevés constituent une base importante pour la prévention et la sensibilisation du public en lien avec la gestion des cyberrisques (voir chap. 1.2). Les informations ainsi obtenues permettent parfois de prévenir de futures infractions et d'éviter de nouvelles victimes.

Recommandations

Aidez-nous à identifier les dangers sur Internet et annoncez les incidents et les cybermenaces à l'OFCS via le formulaire en ligne: NCSC Report (ncsc.admin.ch).

1.6 Protéger et soutenir les infrastructures critiques

Les infrastructures critiques sont des processus, systèmes et installations essentiels au bon fonctionnement de l'économie et le bien-être de la population. L'OFCS vient en aide aux exploitants d'infrastructures critiques en Suisse afin de les aider à se protéger contre les cybermenaces et ainsi minimiser les cyberrisques. Il gère pour ce faire une équipe d'intervention en cas d'incident informatique urgent (Computer Emergency Response Team [CERT]), qui agit comme un service spécialisé à l'échelle nationale pour gérer techniquement les cyberincidents et procéder à l'analyse technique des cybermenaces.

L'OFCS met à la disposition des exploitants d'infrastructures critiques des outils et des données qui permettent d'améliorer la cybersécurité de l'infrastructure et de ses utilisatrices et utilisateurs. Les informations techniques sur les infrastructures informatiques susceptibles d'être utilisées abusivement pour diffuser de maliciels ou gérer de sites web d'hameçonnage en sont un exemple.

1.7 Réduire les vulnérabilités

Les logiciels et/ou les configurations de systèmes peuvent comporter des vulnérabilités dont les attaquants peuvent se servir pour y accéder de manière non autorisée. Afin de diminuer les surfaces d'attaque et prévenir les incidents, de telles vulnérabilités doivent être identifiées et rapidement éliminées.

L'OFCS reçoit quotidiennement des indications sur des vulnérabilités dans le domaine des systèmes informatiques de la part de partenaires et de différentes sources internes et externes. Il examine ces informations avec soin et analyse les différents signalements pour en déduire les mesures qui s'imposent pour les systèmes propres à la Confédération et pour les organes externes. L'OFCS peut avertir les exploitants d'infrastructures critiques de certaines failles de sécurité au moyen de sa propre plateforme d'information par exemple et également publier des consignes de sécurité en la matière.

Souvent, l'OFCS informe par ailleurs aussi directement les entreprises concernées par courriel, téléphone ou par lettre recommandée. Dans de nombreux cas, cette manière de procéder permet de résoudre les vulnérabilités à temps, en collaboration avec les entreprises concernées.

L'OFCS est également le point de contact officiel pour l'annonce de failles de sécurité en Suisse et est reconnu par MITRE[8] comme organe d'autorisation pour l'attribution de numéros CVE. En cette qualité, l'OFCS assure la publication coordonnée des vulnérabilités qui lui sont signalées et contribue ainsi de manière importante à éviter, dans la mesure du possible, l'exploitation de vulnérabilités.[9]

Les mesures de sensibilisation contribuent également à réduire les surfaces d'attaque. L'OFCS encourage les entreprises, organisations et administrations en Suisse à par exemple mettre en œuvre la norme de sécurité *security.txt,*[10] fournissant ainsi une contribution essentielle à la cybersécurité.

Afin d'améliorer la cybersécurité de l'infrastructure informatique appartenant à la Confédération et de réduire les cyberrisques, l'OFCS est également responsable de l'exploitation de son propre programme de primes aux bogues. Ce complément aux autres mesures de sécurité, sert à identifier les éventuelles vulnérabilités dans les systèmes informatiques et autres applications, en collaboration avec des pirates éthiques, ainsi qu'à documenter et éliminer ces failles.

Recommandations

Actualisez vos applications et programmes installés dès que des mises à jour sont disponibles. Activez si possible la fonction de mise à jour automatique.

Tenez compte du cycle de vie des appareils et des logiciels et remplacez-les lorsque leurs fabricants ne fournissent plus de mises à jour de sécurité.

Pour les entreprises: tenez un inventaire actuel des appareils et des logiciels installés et veillez à obtenir les informations sur les vulnérabilités et les mises à jour.

1.8 Poursuite pénale de la cybercriminalité

Contribution de Serdar Günal Rütsche, responsable du Réseau national de soutien aux enquêtes dans la lutte contre la criminalité informatique (NEDIK)

Les rançongiciels constituent de loin actuellement la principale menace dans le domaine de la cybercriminalité en Suisse. Bien que nous soyons dans les faits très bien protégés en Suisse, toutes les entreprises et personnes qui utilisent des services web constituent des cibles potentielles pour de telles attaques. La numérisation offre à l'économie de nouvelles chances de croissance et opportunités de travail. Elle exige en même temps de nouveaux processus et mène à une plus grande dépendance aux technologies de l'information et de la communication opérationnelle. Les criminels peuvent également profiter de ces dépendances pour obtenir un

8 Solving Problems for a Safer World (mitre.org)

9 Le NCSC fait désormais partie du réseau mondial gérant les vulnérabilités des systèmes informatiques (ncsc.admin.ch)

10 Security.txt - Enregistrez un contact de sécurité sur votre site Internet (ncsc.admin.ch)

accès à des réseaux, dérober des données ou neutraliser des systèmes entiers. Leurs méthodes deviennent toujours plus raffinées. Ainsi, de la petite entreprise artisanale à la grande entreprise, une cyberattaque peut devenir une menace existentielle pour les entreprises.

Le nombre d'infractions signalées dans le domaine de la cybercriminalité a fortement augmenté en 2023. C'est avant tout le secteur de la cybercriminalité économique qui est concerné par cette croissance significative. Les menaces dans le cyberespace font partie des dangers les plus importants pour les entreprises, les autorités, les particuliers et les infrastructures critiques. Le progrès technologique dans le domaine de l'intelligence artificielle ouvre aux criminels de nouveaux vecteurs d'attaque, qui peuvent être utilisés dans de nombreuses constellations et faciliter ainsi leurs actions. Le Réseau national de soutien aux enquêtes dans la lutte contre la criminalité informatique (NEDIK), est un regroupement des corps de police qui lutte de manière concertée contre la criminalité numérique et la cybercriminalité. Il coordonne le traitement des enquêtes, il échange des informations en temps réel, établit des vues d'ensemble actuelles et nationales des cyberincidents, transmet des connaissances, élabore des projets intercantonaux et coopère pour ce faire avec des partenaires compétents à l'échelle nationale et internationale. Tous les corps de police y contribuent. Grâce à la mise en place d'une telle plateforme interdisciplinaire, les phénomènes et menaces peuvent être identifiés et contrés suffisamment tôt. La collaboration active, l'établissement de nouveaux partenariats de coopération et le travail opérationnel de prévention visent à endiguer la criminalité dans l'espace numérique et à protéger la population suisse. En 2023, NEDIK a ainsi soutenu des projets dans des domaines prioritaires tels que la fraude à l'investissement en ligne, la pédocriminalité et le renforcement de la collaboration avec des leaders du marché civil.

Dans les années à venir, le domaine de la cybercriminalité va beaucoup évoluer. Les rançongiciels vont rester une menace majeure pour la Suisse, raison pour laquelle nous devons continuer à sensibiliser la population. L'intelligence artificielle va modifier l'état de la menace de manière significative. Grâce à de nouvelles opportunités d'attaque telles que le clonage de la voix ou les *deepfakes*, l'intelligence artificielle va massivement améliorer les capacités des cybercriminels. Une intelligence artificielle ne peut certes pas générer seule une cybermenace entièrement nouvelle à partir d'un maliciel existant, mais cela est possible avec un regard et un contrôle humain. Grâce à l'intelligence artificielle, les escroqueries deviennent également plus raffinées et taillées sur mesure. Afin de nous protéger de ces menaces, nous devons continuer à miser sur des équipes de sécurité hautement spécialisées et sur un traitement responsable des données. Pour ce faire, il faut mettre à disposition les budgets nécessaires, créer des places de formation en Suisse et améliorer le cadre juridique. La sécurité informatique n'est pas qu'une question de technologie, mais une tâche commune impliquant des coopérations contraignantes.

2 Annonces émises par des entreprises et la population

2.1 Aperçu des annonces de cyberincidents

En 2023, le nombre total de signalements enregistrés par le NCSC (devenu ensuite OFCS) a encore une fois augmenté. Avec 49'380 signalements, ce chiffre a augmenté de manière significative par rapport à l'année précédente (34'527 signalements). La hausse observée durant le second semestre 2023 est même encore plus nette par rapport à la même période l'année précédente, passant de 16'951 signalements à 30'331. Ce quasi doublement est avant tout dû à la hausse d'annonce dans deux phénomènes que sont les «offres d'emploi frauduleuses»[11] et les «faux appels au nom de la police».[12]

Le ratio entre les signalements effectués par la population (88%) et ceux émis par des entreprises, des sociétés et les autorités (12%) est resté stable. L'arnaque au président[13] et le piratage d'une messagerie professionnelle[14] font partie des escroqueries typiquement signalées par les entreprises. Nous observons ici une légère hausse durant le deuxième semestre. Pour ce qui est de l'arnaque au président, le nombre de cas signalés au cours du deuxième semestre 2023 est passé à 253, contre 190 pour la même période en 2022, alors que pour le piratage d'une messagerie professionnelle, les signalements sont passés de 45 à 63. Quant au nombre de signalements d'attaques au rançongiciel[15] contre des entreprises, il a légèrement diminué au cours du dernier semestre. Alors qu'au deuxième semestre 2022 le NCSC avait encore reçu 54 signalements, il n'en a plus reçu que 42 au cours de la période sous revue. Les signalements d'attaques par rançongiciel visant des particuliers ont pour leur part fortement diminué. Au deuxième semestre 2023, il n'y a eu que 3 signalements, contre 22 au semestre précédent.

11 Offres d'emploi frauduleuses (ncsc.admin.ch)
12 Appels au nom de fausses autorités (police, douanes) (ncsc.admin.ch)
13 Arnaque au président (ncsc.admin.ch)
14 Piratage d'une messagerie professionnelle (ncsc.admin.ch)
15 Rançongiciels (ncsc.admin.ch)

Annonces parvenues au NCSC durant le deuxième semestre 2023 (par semaine)

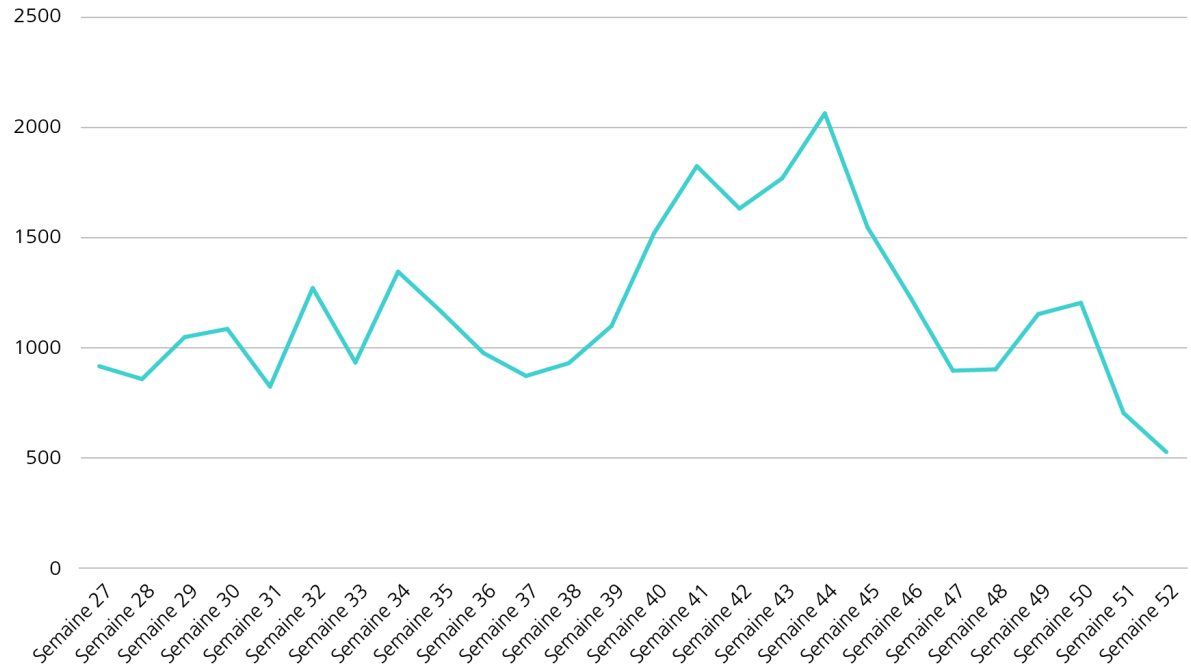

Fig. 1: nombre d'annonces par semaine au NCSC, de juillet à décembre 2023, voir aussi chiffres actuels (ncsc.admin.ch).

Annonces parvenues au NCSC durant le deuxième semestre 2023 (selon la catégorie)

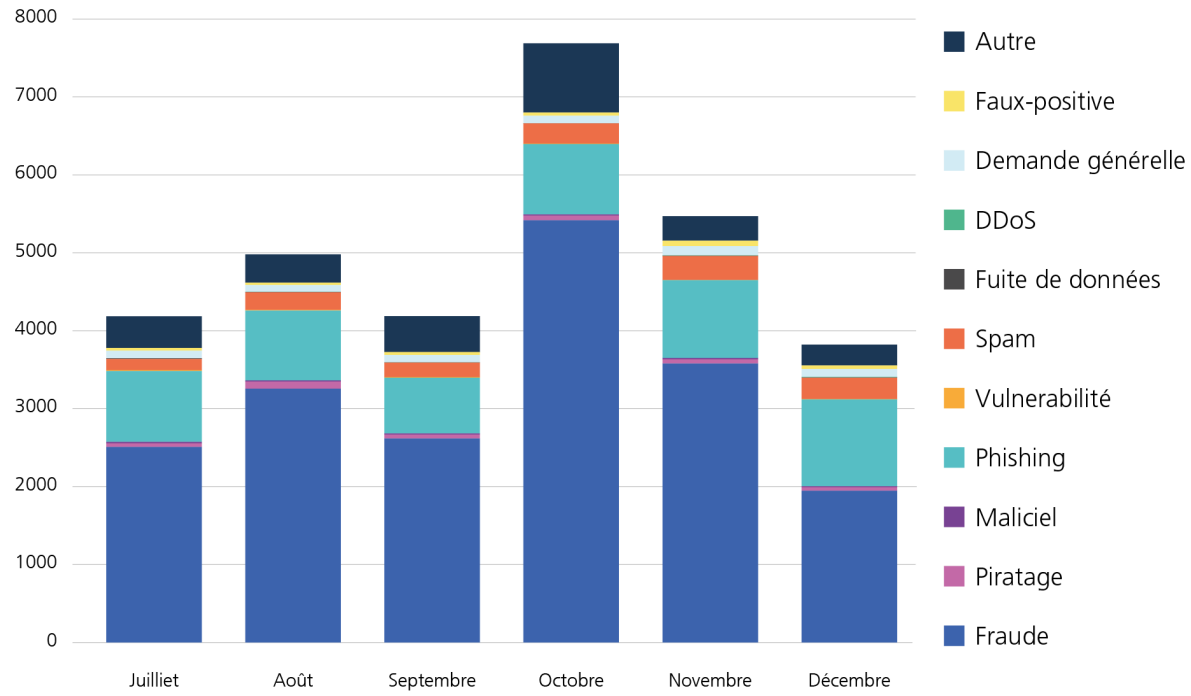

Fig. 2: annonces parvenues au NCSC durant le deuxième semestre 2023, selon la catégorie, voir aussi chiffres actuels (ncsc.admin.ch).

2.2 Escroquerie

2.2.1 L'escroquerie toujours à l'origine de la plupart des signalements

En 2023, avec plus de 30'000 signalements, l'escroquerie a encore largement été le phénomène avec le plus haut nombre d'annonces. La hausse est particulièrement marquante durant le deuxième semestre. Par rapport au deuxième semestre de l'année 2022, le nombre de signalements d'escroquerie a doublé, passant de 10'503 à 19'323. Parmi ces derniers, à l'instar de l'an dernier, une grande partie ont été des courriels de menace au nom d'autorités de poursuite pénale. 4'461 signalements ont ainsi été enregistrés à ce sujet au cours du deuxième semestre 2023. Dans ces courriels de menace, les auteurs prétendent que le destinataire a eu un comportement pénalement répréhensible (le plus souvent en lien avec de la pédopornographie) et que la plainte s'y rapportant ne peut être retirée que contre le versement d'une importante somme d'argent.[16]

Durant le deuxième semestre, une nouvelle manière de procéder a été observée, provoquant ainsi une hausse du nombre de cas. Cela commence par un appel téléphonique d'une supposée autorité de police. Une voix générée par ordinateur informe alors les personnes concernées que leurs coordonnées bancaires personnelles sont par exemple apparu en lien avec une infraction. Les personnes sont ensuite invitées à presser la touche 1 pour davantage d'informations. Si la victime presse le 1, elle est mise en relation avec un prétendu collaborateur et invitée à télécharger un outil d'accès à distance pour permettre en vérité à l'agresseur d'accéder à l'ordinateur ou au téléphone mobile. Les agresseurs essaient ainsi d'obtenir un accès au compte eBanking de la victime et déclenchent des paiements en arrière-plan, via l'outil d'accès à distance. Les signalements liés à ce phénomène ont considérablement augmenté durant le deuxième semestre 2023. Un pic a été atteint durant la semaine 44, durant laquelle le NCSC a reçu record de signalements avec un total de 2'059. La moitié, à savoir 914 signalements, concernaient des appels de menace.[17]

Durant le deuxième semestre, les signalements d'offres d'emploi frauduleuses se sont aussi multipliés, surtout les offres de prétendus bureaux de placement envoyées par WhatsApp. Les candidates et candidats sont attirés par des promesses d'avantages hors du commun. Pour ce faire, le/la futur/e «collaborateur/collaboratrice» reçoit par exemple à travers une plateforme en ligne une liste de tâches à effectuer, telles que par exemple des évaluations en ligne. Pour chaque évaluation, il y a ensuite une indemnité qui est crédité sur le compte de la collaboratrice ou du collaborateur via la plateforme. Le nombre de tâches disponibles passe toutefois rapidement à zéro. Afin d'accélérer la procédure et de ne pas devoir attendre d'obtenir de nouvelles tâches, la plateforme offre la possibilité, d'en recevoir rapidement des nouvelles en échange d'une certaine somme. C'est ainsi qu'il est possible, pour quelques dollars seulement, d'acquérir 50 nouvelles tâches d'évaluation. Le prétendu gain des victimes, qui est censé être crédité sur la plateforme, dépasse rapidement les frais dépensé pour l'obtention de nouvelles tâches. Ainsi, la personne lésée a le sentiment que ce modèle est rentable. La mauvaise surprise intervient ensuite lorsque la victime veut se faire verser ses gains. Pour pouvoir toucher

16 Prétendus courriels de menace émanant des autorités (ncsc.admin.ch)

17 Semaine 43: des escrocs proposant une pseudo-assistance œuvrent au sein de structures similaires à des entreprises (ncsc.admin.ch)

sa paie, les exploitants de la plateforme exigent des frais, et ce jusqu'à ce que la victime se rende compte qu'il s'agit d'une escroquerie.[18]

2.2.2 Premières tentatives d'escroquerie à l'aide de l'intelligence artificielle (IA)

L'IA est devenue l'an dernier un thème d'actualité auprès du grand public, surtout grâce à ChatGPT. Comme toute technologie, elle peut avoir des effets bénéfiques, mais elle peut aussi provoquer des dégâts. Il n'est dès lors pas étonnant de constater que les cybercriminels essaient aussi d'utiliser l'IA pour leurs propres desseins. À l'appui des cas signalés, l'OFCS part toutefois du principe que l'IA n'est pas encore utilisée de manière systématique par les cybercriminels. Il s'agit plutôt d'un expérimentation, par lequel les escrocs cherchent à identifier ce que l'IA rend possible et rentable.[19]

2.2.2.1 Sextorsion avec des images générées par l'IA

La sextorsion désigne une méthode de chantage par laquelle une personne est confrontée à du matériel photographique et à des vidéos qui la montrent en plein acte sexuel et/ou dénudée. Les victimes sont au préalable contactées par une femme séduisante ou un homme séduisant via les réseaux sociaux puis incitées à se déshabiller devant la caméra. Leurs actes sont secrètement enregistrées. Les auteurs menacent ensuite de publier les enregistrements sur YouTube, tout en indiquant le nom de la victime, ou de les envoyer par courriel à des membres de leur famille, des amis ou à leur employeur.[20]

L'OFCS a aussi connaissance de quelques cas où les escrocs créent des photos ou des vidéos compromettantes à l'aide de l'IA pour faire chanter leurs victimes. Pour ce faire, il suffit que les auteurs soient en possession d'une vidéo ou d'une photo anodine qu'ils ont prise eux-mêmes ou qu'ils ont trouvée en libre accès sur Internet. L'IA fabrique ensuite des vidéos pornographiques ou des images de personnes nues à partir de ces vidéos anodines. Le résultat est impressionnant comme l'a montré l'incident du *Deep Fake Porno* impliquant la chanteuse Taylor Swift.[21] L'OFCS part du principe que cette forme de chantage va fortement augmenter dans les années à venir. Outre ces sombres perspectives, il y a toutefois aussi des aspects positifs. Comme de telles vidéos falsifiées peuvent être fabriquées par presque n'importe quelle personne sur Internet, cela pourrait conduire à un désintérêt généralisé, éliminant de fait aussi tout levier de menace sur les personnes pour lesquelles il existe effectivement des vidéos compromettantes.

2.2.2.2 Appels téléphoniques

La plupart des tentatives d'escroquerie s'effectuent toujours par la voie écrite, des courriels ou des services de messagerie. Seule une petite partie se fait par téléphone, pour une raison évidente. Alors que les auteurs peuvent prendre le temps d'écrire, traduire leurs phrases dans la langue souhaitée à l'aide de DeepL ou d'un autre outil, en revanche à l'oral, ils doivent

---

18 Semaine 35: offres d'emploi fictives 2.0 (ncsc.admin.ch)

19 Semaine 49: l'intelligence artificielle, une nouvelle arme dans les tentatives d'escroquerie (ncsc.admin.ch)

20 Sextortion (ncsc.admin.ch); Prévention suisse de la criminalité | Sextorsion (skppsc.ch)

21 Deepfake-Pornos: Ein manipuliertes Video kann ein Leben ruinieren (srf.ch)

maîtriser la langue de la victime et pouvoir réagir instantanément à leur interlocuteur. À l'avenir, l'IA pourrait jouer son rôle ici aussi, en permettant de traduire simultanément les conversations téléphoniques à l'aide d'une voix et d'une langue prédéfinies. Il existe d'ailleurs déjà des premiers signaux d'utilisation de l'IA dans le cadre de conversations téléphoniques. Plusieurs entreprises ont ainsi déjà annoncé à l'OFCS des cas où des prétendus collaborateurs dont la voix correspondait auxdites personnes les auraient appelées, afin de se renseigner sur des questions internes à l'entreprise ou pour déclencher des paiements. Le réel collaborateur n'avait toutefois aucune idée de ces abus de leur propre voix, sans doute générée à l'aide de *deepfakes*. Des voix très similaires à celles de leurs enfants sont aussi utilisées pour des appels visant à provoquer un choc auprès des parents, en prétendant que ceux-ci ont eu un accident. On ne sait toutefois pas dans quelle mesure l'IA joue déjà un rôle dans ce type d'incident.

2.2.2.3 Communication en suisse allemand

Des courriels d'hameçonnage font sporadiquement aussi surface en suisse-allemand. Le NCSC en faisait déjà état durant le dernier semestre.[22] L'IA pourrait jouer un rôle dans leur élaboration, même si le procédé est surprenant. En effet dans la majorité des affaires, l'allemand est la règle. Un courriel prétendument officiel d'une banque en dialecte suisse-allemand devrait plutôt susciter la méfiance, plutôt que de convaincre la cible de cliquer sur le lien correspondant. Il pourrait donc s'agir encore une fois d'expérimentations des agresseurs. Il existe toutefois un autre domaine où le dialecte est courant dans la communication, à savoir les petites annonces. Le NCSC a ainsi observé quelques cas d'escroquerie dans ce secteur le semestre dernier, où la communication s'est faite en dialecte. Cela met la victime en confiance, puisque le vendeur et l'acheteur semblent venir de la même région (linguistique). Il faut partir du principe que l'IA est également utilisée dans ces cas-là.

2.2.2.4 Fraude à l'investissement avec des personnes connues

Lors de fraudes à l'investissement en ligne, les criminels utilisent souvent des images de personnes connues pour donner une impression de sérieux aux offres douteuses. Pour ce faire, ils n'utilisent pas seulement des images ou des vidéos en libre accès mais génèrent aussi des vidéos de type *deepfake*. La vidéo *deepfake* d'Elon Musk lors du lancement de la fusée Starship en est un exemple: Des fraudeurs avaient profité du lancement de la fusée de l'entreprise SpaceX pour faire de la publicité pour une escroquerie relative à un prétendu cadeau. Sur un site web, Elon Musk promet dans une vidéo de doubler et reverser les montants qui lui seront versés en cryptomonnaies.[23]

Conclusion / Recommandations

À l'aide de l'IA, des cyberacteurs peuvent créer des contenus pour des courriels et des messages courts semblant crédibles, qui ressemblent à s'y méprendre à un courrier légitime, tant du point de vue de la langue que de la présentation. Ces contenus ne peuvent à peine être

22 Semaine 14: Courriel d'hameçonnage en suisse allemand et facture de la «Garde routière suisse de sauvetage» (admin.ch)

23 Semaine 17: vidéo de promotion truquée pour une fausse action «give away» (ncsc.admin.ch)

différenciés de ce qu'une personne polyglotte pourrait produire. Il est ainsi plus difficile pour les destinataires de tels contenus de les identifier comme des tentatives d'escroquerie.

L'utilisation de l'IA permet par ailleurs de fabriquer des photos, des vidéos et des voix qui ressemblent à s'y méprendre à des vraies (aussi appelées *deepfakes*). Elles peuvent être ensuite utilisées pour des attaques d'ingénierie sociale. Les imitations de voix peuvent par exemple convaincre la personne ciblée qu'elle parle avec une personne qu'elle connaît et la victime sera dès lors plus encline à lui verser de l'argent.

Les auteurs d'escroqueries se montrent toujours très créatifs, à imaginner de nouveaux scénarios pour inciter les victimes à réagir sans prendre la peine de réfléchir. Les contenus générés par l'IA accentue cette tendance. Ne vous laissez dès lors pas déborder et subermerger, mais prenez le temps de réfléchir et, en cas de doute, adressez-vous à d'autres personnes ou à l'OFCS, pour obtenir leur avis sur la question.

2.3 Signalements d'hameçonnage

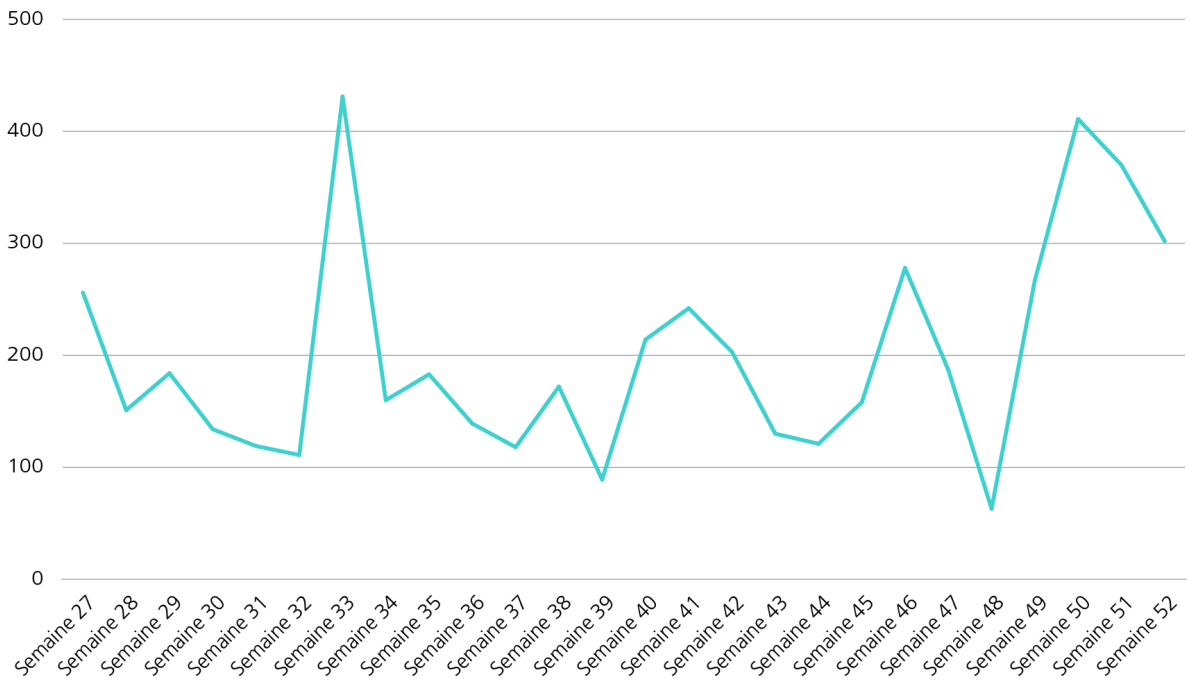

Fig. 3: nombre d'URL à phishing vérifiées et confirmées par le NCSC par semaine au cours du deuxième semestre 2023.

2.3.1 Hameçonnage en chaîne, concernant des paquets postaux et des factures payées à double

Après l'escroquerie, l'hameçonnage se place en deuxième position des phénomènes les plus fréquemment signalés via le formulaire d'annonce. Par rapport à la même période de l'année précédente, le nombre de cas signalés a plus que doublé. Au cours du deuxième semestre 2023, le nombre de signalements est passé de 2'179 à 5'536. Pour l'ensemble de l'année, le NCSC a reçu par ce biais au total 9'415 signalements d'hameçonnage. Le NCSC (aujourd'hui

OFCS) reçoit aussi des signalements d'hameçonnage via la plateforme antiphishing.ch, qui sont ensuite traités de manière partiellement automatisée.[24]

Pour la plus grande partie des attaques d'hameçonnage, il s'agit d'attaques à la chaîne, diffusées à large échelle. Celles-ci contiennent des erreurs et sont envoyées assez facilement. Un signe typique d'une telle attaque reste par exemple une formule de politesse impersonnelle, comme «Cher client» ou simplement l'adresse courriel comme formule.

Les annonces d'envoi de paquets falsifiées sont toujours envoyées par milliers[25] et font cette fois encore partie des tentatives d'hameçonnage les plus fréquemment signalées, comme ce fut le cas l'an dernier. Les prétendus courriels de remboursement au nom de fournisseurs, des CFF et aussi de l'administration fiscale font toujours partie du répertoire standard des hameçonneurs.[26] Les agresseurs misent ici avant tout sur la probabilité élevée de voir une personne effectivement attendre un paquet ou avoir effectivement payé une facture auprès d'un fournisseur. Cela confère une plus grande plausibilité au courriel en question.

L'OFCS observe par ailleurs une hausse des attaques d'hameçonnage contre des entreprises. Les attaques visent avant tout sur les données d'accès aux courriels d'entreprise et en particulier aux comptes Office365. On observe de plus en plus de tentatives d'hameçonnage fonctionnant selon le principe dit de la boule de neige, au cours desquelles un compte courriel d'entreprise est piraté de manière à envoyer ensuite au nom de la victime un courriel d'hameçonnage à tous les contacts trouvés par les agresseurs dans le compte piraté. Cela permet de récupérer plusieurs milliers de contacts surtout des collaborateurs et collaboratrices étant en contact avec la clientèle. Étant donné que, dans ces cas, l'expéditeur est connu du destinataire, la probabilité est plus grande que ce dernier tombe dans le piège de la tentative d'hameçonnage. Dès lors, le jeu recommence depuis le début et les contacts de la nouvelle victime reçoivent à leur tour un même courriel d'hameçonnage. Ce procédé est aussi appelé «hameçonnage en chaîne».

2.3.2 La réapparition de l'hameçonnage par téléphone

L'hameçonnage par téléphone ne représente toujours qu'une petite partie des signalements d'hameçonnage. Étant donné que les appels sont très ciblés et que l'appelant interagit aussi avec la victime, les chances de succès pourraient ici être bien plus grandes. C'est certainement aussi la raison pour laquelle les hameçonneurs sont prêts à fournir des efforts supplémentaires.

Vers la fin de l'année 2023, les signalements d'appels de prétendus employés de banque se sont multipliés, les appelants indiquant vouloir interrompre un paiement frauduleux. Dans certains cas, le numéro de téléphone affiché correspondait même au numéro officiel de la banque. Celui-ci est ce qu'on appelle «spoofé» par les fraudeurs, c'est-à-dire falsifié, afin de paraître crédible. Dans de nombreux cas, par exemple, les fraudeurs ont prétendu qu'un virement avait

---

[24] Voir aussi le rapport anti-phishing 2023 (ncsc.admin.ch).

[25] Pièges d'abonnement aux paquets (ncsc.admin.ch); semaine 23: quand une tentative d'hameçonnage débouche sur un abonnement piège (ncsc.admin.ch); voir aussi le rapport anti-phishing 2023 (ncsc.admin.ch)

[26] Semaine 46: courriels d'hameçonnage faisant miroiter un droit au remboursement de l'impôt et hameçonnage de portefeuilles de cryptomonnaie (ncsc.admin.ch);
Semaine 41: diverses tentatives d'hameçonnage des données Office 365 et CFF (ncsc.admin.ch)

été effectué pour un écran plat dans un magasin spécialisé en électronique et qu'il fallait tout de suite prévenir la section anti-fraude de la police cantonale. L'appelant fournit même immédiatement le numéro de téléphone correspondant de la police. Bien évidemment, ce numéro appartient aussi aux hameçonneurs.

Or, ce qui semble plausible au premier abord n'est toutefois tout simplement pas possible, car, même si la banque voit bel et bien les montants comptabilisés dans son système, elle ne sait pas quels produits ou quelles prestations le client a achetés. Une banque ne peut donc par principe pas du tout savoir ce qui a été acheté par un client.

En règle générale, les appelants se font passer pour des collaborateurs ou collaboratrices d'une grande banque. En effet, la probabilité que la personne appelée ait un compte auprès d'une des banques les plus répandues de Suisse est assez élevée. Lorsque les auteurs ne devinent pas correctement le nom de la banque, ils adoptent la solution suivante: Ils essaient de découvrir le nom de la banque de la victime au cours de la conversation téléphonique pour ensuite rappeler peu de temps après, cette fois-ci au nom de la banque en question.

Comme le montrent les signalements reçus par l'OFCS, les fraudeurs utilisent également des informations librement accessibles. C'est ainsi qu'une victime a dans un cas de figure reçu un appel d'un prétendu collaborateur d'une banque, qui lui a demandé si elle avait effectivement transféré une grosse somme d'argent au cours des derniers jours. Étonnamment, le prétendu bénéficiaire était connu de la victime en raison d'une fonction antérieure. Une recherche sur Internet effectuée par l'OFCS a révélé que le nom et le numéro de téléphone de la victime et du prétendu destinataire figuraient tous deux sur une présentation publique commune passée. Cela montre que les fraudeurs scannent systématiquement Internet à la recherche de telles informations, qu'ils peuvent ensuite utiliser pour des attaques ciblées d'ingénierie sociale. Jusqu'à présent, ce procédé avait avant tout été observé en lien avec l'arnaque au président et semble désormais s'être étendu au phénomène de l'hameçonnage par téléphone.

2.4 Signalements de maliciels et de piratage

2.4.1 Rançongiciels

Une hausse n'a pas été observée pour tous les phénomènes. Pour la catégorie des rançongiciels, par rapport à 2022, le nombre de cas a nettement reculé. Avec 109 signalements, il y a eu près de 40 cas de moins que l'année précédente. Ce recul concerne toutefois avant tout des particuliers et non des entreprises. C'est ainsi que seuls 11 cas ont été signalés en 2023 portant sur des particuliers, alors que ce chiffre s'élevait encore à 56 l'an dernier. Les systèmes NAS (stockage en réseau) domestiques, particulièrement visés par les particuliers, ne sont attaqués plus que de manière isolée. Cela est dû d'une part au fait qu'il n'y a pas eu de vulnérabilité sérieuse cette année, et d'autre part, au fait que les attaques n'ont certainement pas dû être suffisamment lucratives.

Si l'on considère désormais le nombre de signalements de rançongiciels au sein des entreprises, la tendance à la baisse est nettement plus modérée et le nombre de signalements se stabilise pratiquement au niveau de l'année précédente, avec 98 cas au lieu de 103. L'OFCS constate en revanche, que les attaques entraînent désormais presque toujours une fuite de données, ce qui provoque des dégâts plus étendus (concernant les rançongiciels, voir aussi chap. 3.23.3).

Le rançongiciel LockBit est resté particulièrement actif. Les autres familles de rançongiciels signalées au NCSC furent Play, MedusaLocker, BlackCat/ALPHV, Phobos, BlackByte, Black-Basta, Babuk, ECh0raix et Akira.

Recommandations

Sur le site web de l'OFCS, vous trouverez une liste de mesures préventives pour se protéger des rançongiciels et des consignes à suivre en cas d'incident.

2.4.2 Signalements de piratage

Une hausse a également été observée en 2023 pour ce qui concerne les cas de piratage. Par rapport au deuxième semestre 2022, les signalements ont augmenté durant la période sous revue, passant de 276 à 351. Ce sont surtout les comptes de réseaux sociaux qui sont sous pression ici, puisque le NCSC a reçu 186 signalements (+78) se rapportant à cette catégorie. Les agresseurs se concentrent ici de plus en plus sur les comptes commerciaux, qui sont associés à une carte de crédit. À travers un tel compte, ils peuvent activer de la publicité aux frais de la victime, par exemple pour des offres douteuses. Outre le dommage provoqué par la perte du compte de réseau social, les dégâts financiers peuvent eux se chiffrer à plusieurs milliers de francs.

2.4.3 Les hôtels dans le viseur

Au cours du deuxième semestre de l'année 2023, les hôtels et leur clientèle se sont retrouvés dans le viseur des criminels, tout particulièrement la plateforme booking.com. Au début de l'année 2023 déjà, le NCSC a alerté le secteur sur des incidents lors desquels un faux réceptionniste a contacté un client pour obtenir ses données de carte de crédit.[27] Les fraudeurs connaissaient tous les détails de la réservation et ont utilisé ces informations pour convaincre leur interlocuteur qu'il avait réellement affaire à un hôtel. Il est possible alors que les pirates aient pu accéder au compte «booking.com» de l'hôtel.

Durant le deuxième semestre, il y a ensuite eu d'autres indices quant au mode opératoire des agresseurs pour parvenir à accéder aux données d'accès de portails tels que booking.com. Diverses méthodes d'ingénierie sociale sont utilisées dans ce cadre pour inciter le personnel hôtelier à cliquer sur un lien et installer un maliciel.

Dans l'une des variantes, le fraudeur prétend qu'un client fait actuellement l'objet d'un chantage aux images pornographiques, qui ont prétendument été prises dans la chambre de l'hôtel. Il donne deux jours à l'hôtel pour clarifier les faits et trouver l'auteur, sans quoi l'hôtel sera considéré comme complice. Toute la documentation relative à l'affaire aurait été archivée à titre de preuve et le fichier concerné pourrait être téléchargé via le lien indiqué. En cliquant sur le lien, la victime télécharge un maliciel, qui enregistre toutes les données d'accès introduites

[27] Semaine 4: intrus à l'hôtel, un logiciel malveillant détourne les données fournies par les clients lors de leur réservation (ncsc.admin.ch)

et les transmet aux fraudeurs. Ces derniers peuvent ainsi accéder aux réservations actuelles de l'hôtel effectuées sur des plateformes telles que booking.com.[28]

Outre des courriels avec des maliciels en pièces jointes, de purs courriels d'hameçonnage, directement adressés au personnel de l'hôtel, circulent également. Ici aussi, on essaie d'inciter le collaborateur ou la collaboratrice concerné à révéler ses données d'accès à booking.com.

Recommandations

Les hôtels doivent ouvrir de nombreux documents transmis par des clients. Il ne faut toutefois en aucun cas ouvrir des fichiers exécutables. Réfléchissez à une stratégie où les ordinateurs utilisés pour la communication avec la clientèle sont séparés du reste du réseau (segmentation du réseau). Et gardez toujours vos systèmes à jour.

3 Situation

3.1 Accès initial à l'aide de maliciels (chevaux de Troie)

Les chevaux de Troie appartiennent à la catégorie des maliciels qui permettent d'accéder au système d'une victime en y insérant une porte dérobée. Ils sont souvent installés après que les utilisateurs aient été trompés, par exemple en intégrant le code malveillant dans un autre programme ou en le cachant d'une autre manière. Ce type de maliciel est régulièrement diffusé par courriel, soit sous forme de pièce jointe ou via un lien. Le contexte du courriel est aussi utilisé pour inciter l'utilisateur à exécuter inconsciemment le code malveillant. Afin de renforcer la légitimité du courriel malveillant, certains agresseurs utilisent une ancienne correspondance par courriel qu'ils ont obtenue de manière frauduleuse. Ce mode opératoire a notamment été observé chez les exploitants de Qakbot, un maliciel dont la première infection a régulièrement conduit à des infections par rançongiciel. Les activités de type Qakbot ont toutefois drastiquement diminué durant le deuxième semestre 2023, après qu'une opération multinationale ait été menée contre les systèmes infectés par Qakbot et contre l'infrastructure utilisée par les exploitants du maliciel.[29] Malgré cela, les acteurs criminels qui se cachaient derrière cette campagne ont pu poursuivre leurs activités sous une forme différente. Ainsi, après la dissolution de Qakbot, un nombre croissant de campagnes de diffusion des maliciels PikaBot et DarkGate a été observé, présentant plusieurs similitudes avec les activités de Qakbot, tel que l'utilisation d'une correspondance électronique antérieure ou l'utilisation de certaines infrastructures identiques.[30] De nouvelles voies de diffusion sont toutefois également venues s'ajou-

28 Semaine 47: les hôtels dans la ligne de mire des cybercriminels (ncsc.admin.ch)

29 Qakbot Malware Disrupted in International Cyber Takedown (justice.gov)

30 Semaine 42: Dynamite phishing: après Emotet et Qakbot, voici DarkGate (ncsc.admin.ch) ; Are DarkGate and PikaBot the New QakBot? (cofense.com)

ter à la liste des moyens de distribution, comme par exemple les logiciels de messagerie instantanée à des fins professionnelles (notamment Microsoft Teams et Skype) ou la publicité frauduleuse sur les moteurs de recherche (*malvertising*).[31]

Conclusion / Recommandation

Ne cliquez pas sur les liens dans les courriels suspects et n'ouvrez aucun fichier joint. En cas de doute, demandez à l'expéditeur supposé si le courriel en question a effectivement été envoyé par ses soins.

Lorsque vous recherchez des logiciels sur Internet, vérifiez avant de les télécharger que vous vous trouvez sur le site du fabricant ou sur un autre site de confiance (p. ex. un magazine informatique connu).

Soyez prudent à chaque fois qu'une fenêtre de téléchargement s'ouvre.

Laissez si possible les programmes s'actualiser automatiquement ou alors utilisez toujours la fonction de mise à jour intégrée ou téléchargez la dernière version en date directement chez le fabricant.

Ne connectez aucun appareil USB inconnu ou trouvé à votre ordinateur.

3.2 Vulnérabilités: Ivanti CVE-2023-35078 et CVE-2023-35081

Ivanti est un fournisseur de solutions *Unified Endpoint Management* ainsi que de solutions de sécurité et de gestion des services *Zero-Trust*. Il offre ainsi aux entreprises un pilotage centralisé pour protéger leurs appareils et en assurer la maintenance. Mondialement, plus de 40'000 entreprises font ainsi confiance aux produits de ce fabricant.

Une vulnérabilité a été détectée à l'été 2023 dans le *Ivanti Endpoint Manager Mobile (EPMM)*, autrefois connu sous le nom de *MobileIron Core*. Le fabricant en a averti ses clients le 24 juillet 2023 et a mis un correctif à disposition pour l'installation,[32] La faille de sécurité est connue sous le numéro CVE-2023-35078 et concernait toutes les versions du produit supportées à l'époque (11.10, 11.9 et 11.8). Des versions anciennes, qui ne sont plus supportées depuis longtemps, étaient par ailleurs également concernées.

Cette faille de sécurité critique, avec un score CVSS[33] maximal de 10.0, permet à un attaquant non authentifié d'accéder à certains chemins de l'API[34] depuis Internet. Cela peut permettre d'accéder à des informations personnellement identifiables (IPI) telles que les noms, les numéros de téléphone et d'autres détails sur les appareils mobiles. L'attaquant peut par ailleurs aussi procéder à des changements de configuration et ouvrir un compte d'administrateur

---

31 PikaBot distributed via malicious search ads (malwarebytes.com) ;
Microsoft Teams used to deliver DarkGate Loader malware (malwarebytes.com)

32 CVE-2023-35078 - New Ivanti EPMM Vulnerability (ivanti.com)

33 Le *Common Vulnerability Scoring System* (CVSS, en français: «système d'évaluation standardisé de la criticité des vulnérabilités») est une norme industrielle servant à évaluer la criticité des failles de sécurité possibles ou effectives des systèmes informatiques. Voir CVSS (wikipedia.org).

34 Une API (*application programming interface*, littéralement «interface de programmation d'application») est une partie de programme mise à la disposition, par un système logiciel, d'autres programmes pour la connexion au système. Voir Interface de programmation (wikipedia.org).

EPMM. Cela offre à son tour à un intrus d'autres possibilités d'actions de manipulation plus sérieuses dans un système vulnérable.

Au moment de la publication des détails de la vulnérabilité, celle-ci avait déjà été exploitée, comme c'est souvent le cas pour de nombreuses vulnérabilités. L'autorité nationale de sécurité de la Norvège a par exemple informé le public le 24 juillet 2023[35] qu'il avait été prouvé que la vulnérabilité avait été exploitée dans le but de mener une attaque contre des ministères norvégiens. Le fabricant Ivanti mentionne quant à lui dans son avis qu'il a connaissance d'un nombre limité de clients ayant déjà été victimes d'une telle attaque.

Alors que de nombreuses entreprises concernées étaient encore occupées à corriger CVE-2023-35078, une nouvelle faille de sécurité a été annoncée dans *Ivanti Endpoint Manager Mobile (EPMM)* quelques jours plus tard, le 28 juillet 2023, avec l'identifiant CVE-2023-35081.[36] Celle-ci a pu être identifiée dans le cadre des examens portant sur la CVE-2023-35078. Dans ce cas aussi, le fabricant a mis à disposition des informations et des correctifs, afin d'éliminer la faille de sécurité.

Évaluée à 7.2, la deuxième vulnérabilité a été considérée comme moins critique que la précédente. Néanmoins, la faille de sécurité permettait à un administrateur authentifié d'installer des fichiers malveillants sur les serveurs EPMM (Arbitrary File Write). Si cette vulnérabilité est utilisée en lien avec la CVE-2023-35078, l'authentification d'administrateur et les restrictions ACL[37] peuvent être intégralement contournées.

Comme pour la première vulnérabilité découverte, toutes les versions du produit prises en charge au moment de la publication étaient concernées, ainsi que les versions plus anciennes qui ne sont plus prises en charge depuis longtemps.

Le fabricant Ivanti a par ailleurs confirmé sur son site web que CVE-2023-35081 réduisait de manière avérée la complexité de l'attaque pour un intrus, si l'exploitant de système n'avait pas encore corrigé la première vulnérabilité publiée (CVE-2023-35078) sur un système affecté.

Le NCSC a activement prévenu les exploitants d'infrastructures critiques et de nombreuses autres entreprises suisses des deux vulnérabilités. À l'appui d'analyses techniques effectuées par le NCSC, les entreprises potentiellement visées ont par ailleurs été informées personnellement et ont reçu des recommandations d'action concrètes. Et malgré la criticité élevée des deux vulnérabilités, il n'y a proportionnellement que peu de victimes suisses confirmées.

Conclusion / Recommandation

Il est tout à fait réaliste que, pour un même produit, plusieurs vulnérabilités graves soient rendues publiques en l'espace de quelques jours seulement, comme le prouve remarquablement le cas d'Ivanti. Le facteur temps étant un critère très important dans la gestion des vulnérabilités, les correctifs publiés devraient dans tous les cas être installés sur les systèmes concernés sans délai. Quant aux recommandations du fabricant, elles doivent impérativement que

---

35 Nulldagssårbarhet i Ivanti Endpoint Manager (MobileIron Core) - Nasjonal sikkerhetsmyndighet (nsm.no)

36 CVE-2023-35081 - Remote Arbitrary File Write (ivanti.com)

37 Une *Access Control List* (liste de contrôle d'accès) est une technique logicielle, à l'aide de laquelle il est possible de restreindre les accès à des données et des fonctions. Voir Access Control List (wikipedia.org).

être suivies. Mais pour ce faire, il est indispensable que chaque organisation et entreprise connaisse son infrastructure et tienne un inventaire actuel des produits utilisés.

Agir rapidement pour combler les failles de sécurité garantit d'une part le bon fonctionnement des systèmes informatiques et réduit en parallèle la surface d'attaque d'une entreprise. D'autre part, cela permet dans certains cas d'éviter qu'un attaquant ne profite de ce que l'on appelle un «vulnerability chaining». Lors d'un enchaînement de plusieurs vulnérabilités, un intrus combine en effet plusieurs failles de sécurité existantes pour compromettre un système. Or, si un exploitant de système comble continuellement les vulnérabilités à l'aide d'un processus établi de gestion des vulnérabilités et des correctifs, l'activité de l'agresseur sera entravée et cela réduit ses chances de réussite.

3.3 Rançongiciels

3.3.1 Incidents de rançongiciels

Au cours de l'année sous revue, les attaques par rançongiciel en Suisse ont entre autres touché les entreprises de solution informatique, qu'elles soient au service d'administrations publiques ou de PME. Ces attaques de plus en plus fréquentes contre la chaîne d'approvisionnement nous rappellent l'importance de la mise en place préalable de certaines mesures de protection simples mais efficaces contre des attaques cyber, l'importance du partage d'expérience (national et international) ainsi que l'importance de savoir communiquer durant et après l'incident.[38]

3.3.1.1 Une vulnérabilité dans la chaîne d'approvisionnement (*supply chain*)

En novembre 2023, l'entreprise Concevis AG, fournisseur de services informatiques notamment pour des administrations publiques, a subi une attaque par rançongiciel aboutissant à une violation de données.[39] En réaction à la cyberattaque, de nombreux clients ont provisoirement suspendu l'utilisation des services proposés par l'entreprise, afin de protéger leurs systèmes d'une éventuelle propagation de l'incident via les interfaces avec le prestataire.

La chaîne d'approvisionnement fait l'objet d'un intérêt croissant de la part des cybercriminels. Par exemple, le groupe de rançongiciel Everest a réorienté ses opérations pour devenir un courtier d'accès initial (*Initial Access Broker*). Cela signifie que le groupe s'est spécialisé dans la détection de portes dérobées dans des systèmes d'organisations ainsi que dans la vente de ces accès à d'autres cybercriminels, au lieu d'exécuter lui-même les attaques comme il le faisait jusqu'à présent. Selon le FBI,[40] cette activité nécessite l'obtention d'un accès initial aux environnements des victimes par le biais de partenaires tiers, en exploitant des vulnérabilités de l'accès à distance contrôlé par le fournisseur ou des services tiers, et en utilisant des outils de gestion de système légitimes pour escalader les privilèges au sein des organisations victimes.

---

38 Voir aussi les recommandations de l'OFCS: Cyberattaque – comment communiquer? (ncsc.admin.ch).

39 Cyberattaque contre l'entreprise Concevis: l'administration fédérale est également concernée (ncsc.admin.ch)

40 FBI Private Industry Notification 231108.pdf (ic3.gov)

Conclusion / Recommandation

Les attaques et les incidents survenant dans les chaînes d'approvisionnement peuvent également entraver votre propre exploitation et provoquer d'importants dommages (consécutifs). Il est dès lors indispensable de thématiser la question de la cybersécurité et de la protection des données avec des partenaires, de la régler contractuellement et d'en vérifier la bonne exécution.[41]

3.3.1.2 Sauvegardes hors ligne et mises à jour logicielles régulières

En août 2023, le réseau du gouvernement srilankais, le *Lanka Government Network* (LGN), a subi une attaque par rançongiciel entraînant un chiffrement des systèmes et des données du LGN. Malgré une restauration des systèmes en douze heures, la récupération de certaines données datant d'il y a 3 mois n'a pas pu être effectuée. En effet, en l'absence de sauvegardes hors ligne, il a fallu recourir à la sauvegarde en ligne, laquelle avait également été corrompue. Cela a entraîné la perte de courriels envoyés ou reçus entre le 17 mai et le 26 août 2023. En outre, l'utilisation d'une version obsolète de Microsoft Exchange (2013) a rendu le LGN vulnérable aux cyberattaques.[42]

Conclusion / Recommandation

Faites régulièrement des copies (sauvegardes) de vos données (également) sur un support externe.[43]

Actualisez vos logiciels lorsque des mises à jour de sécurité sont disponibles. Anticipez la fin du cycle de vie d'un logiciel et remplacez-le à temps.

3.3.1.3 Une communication réfléchie est nécessaire pendant la gestion de l'incident

En mai 2023, Unico Data SA, un fournisseur suisse de solutions informatiques pour PME, a été victime d'une attaque par rançongiciel par le groupe Play. Suite à cette attaque, la plupart de ses services ont été hors ligne. L'entreprise a réagi rapidement à l'attaque en mettant en place une cellule de crise chargée de résoudre l'incident, de le signaler aux autorités compétentes et d'informer les clients concernés. Étant donné que l'entreprise Unico Data SA n'a pas payé de rançon, le groupe de rançongiciel a publié les données piratées sur le *darknet*. Peu de temps après, son directeur a commenté publiquement l'incident et a thématisé les conséquences financières de l'attaque ainsi que la question des ressources en personnel et en temps qui ont été nécessaires pour solutionner le problème.[44] Le directeur a aussi évoqué les leçons que son entreprise a tiré de l'incident. Il a appelé d'autres entreprises à se préparer à des cyberattaques et à se concentrer dans ce cadre sur des plans de reprise après sinistre

41 Supply chain security guidance (ncsc.gov.uk); ICT Supply Chain Resource Library (cisa.gov); Collaborer avec des prestataires externes de services informatiques (ncsc.admin.ch)

42 Sri Lankan government loses months of data following ransomware attack (therecord.media); Crisis & Consequences: An Emerging Cyber Quandary for Sri Lanka (capsindia.org)

43 S-U-P-E-R.ch – Sauvegarde de données: ce qu'il faut savoir (ncsc.admin.ch)

44 «Der Cyberangriff hat uns insgesamt weit über 1 Million Franken gekostet» (inside-it.ch)

(*disaster recovery*), mais également sur la communication interne et externe. Il a souligné à quel point il était important de définir quelles informations étaient communiquées par quelles personnes et par quels canaux.

Conclusion / Recommandation

Grâce à une communication réfléchie et proactive, les victimes de cyberattaques peuvent catégoriser les incidents et informer leur personnel, leur clientèle, leurs partenaires, les médias et la population de manière factuelle, évitant ainsi les spéculations.

Recommandations de l'OFCS sur Cyberattaque – comment communiquer? (ncsc.admin.ch).

3.3.2 Suivi des variantes de rançongiciels et des acteurs

Les groupes de rançongiciels s'adaptent rapidement aux changements de circonstances, qu'il s'agisse de nouvelles vulnérabilités, d'évolutions techniques ou personnelles, de mesures prises par les autorités ou encore de nouvelles dispositions légales. Un exemple de la première est l'exploitation d'une nouvelle vulnérabilité du logiciel Atlassian «Confluence», qui a été utilisée pour diffuser le rançongiciel C3RB3R.[45]

3.3.2.1 Evolution des acteurs et de leurs prestations

Durant l'année sous revue, il y a eu de nombreux changements au sein des groupes de rançongiciels et de leurs activités. Les groupes modifient souvent leur composition, leur nom et le type d'activités qu'ils exercent, ils fusionnent aussi parfois avec d'autres groupes ou décident de proposer leurs services, par exemple sous la forme de rançongiciels en tant que service (RaaS, *ransomware-as-a-service*). Le marché du rançongiciel est plus que jamais prolifique, permettant à des acteurs moins expérimentés de créer et de modifier facilement des maliciels à leur guise. C'était par exemple le cas du kit de construction de rançongiciel Lockbit 3.0, dont le code a fuité en septembre 2022. Les chercheurs de Kaspersky ont découvert 396 différents échantillons qui avaient intégrer le code de Lockbit.[46] L'existence de nombreuses variantes de Lockbit rend l'attribution des attaques à des groupes ou individus spécifiques difficile attaques pour les chercheurs en cybersécurité et complique le suivi de leurs activités. Une autre difficulté consiste en un nombre toujours plus important de nouveaux acteurs et de nouvelles variantes dans le paysage des rançongiciels.[47]

Par exemple, il semble que le groupe Royal ait laissé place au groupe BlackSuit. Il pourrait s'agir d'un changement de nom ou de marque et/ou d'une variante dérivée, puisque le maliciel BlackSuit comporte certaines caractéristiques de code qui sont similaires à celles de Royal[48].

---

45 C3RB3R Ransomware | Ongoing Exploitation of CVE-2023-22518 Targets Unpatched Confluence Servers (sentinelone.com)

46 Leaked Lockbit ransomware builder analysis (securelist.com)

47 Orange Cyber Defense publie régulièrement une liste des différents acteurs et variantes de rançongiciels: Map tracking ransomware, by OCD World Watch team (github.com)

48 Investigating BlackSuit Ransomware's Similarities to Royal (trendmicro.com) ; BlackSuit ransomware - what you need to know (tripwire.com)

L'année 2023 a été le théâtre non seulement de refontes mais aussi de l'apparition de nouvelles familles de rançongiciels, se voulant novatrices et uniques, comme le RaaS «Rhysida», actif depuis mai 2023. Celui-ci dispose d'un mécanisme d'autodestruction et est compatible avec les systèmes d'exploitation Microsoft plus anciens que Windows 10. Il a été écrit avec la langue de programmation C++ et peut être compilé à l'aide de l'instrument de développement MinGW et des bibliothèques partagées (*shared libraries*).[49]

3.3.2.2 Réaction à une opération policière

À la fin de l'année 2023, le FBI a mené une opération internationale contre le groupe BlackCat/ALPHV.[50] Pendant plusieurs jours, le Data-Leak-Site (DLS) du groupe portait la mention «mis sous séquestre». Les autorités de poursuite pénale ont pu récupérer 946 paires de clés qui leur ont permis d'accéder aux communications chiffrées des auteurs avec les victimes, aux sites contenant les données dérobées et aux panels d'affiliés du groupe. Les cybercriminels ont toutefois peu après mis un nouveau DLS en ligne, sur lequel six victimes présumées ont immédiatement été listées. Le groupe de rançongiciel Lockbit essaie depuis lors de recruter des partenaires et des développeurs de BlackCat/ALPHV.

À l'heure actuelle, il n'existe pas d'outil de déchiffrement universel pour le rançongiciel BlackCat/ALPHV. Quelques victimes peuvent toutefois restaurer leurs données à l'aide des clés qui ont été récupérées durant l'opération policière.

3.3.2.3 Adaptation des chantages à l'évolution régulatoire

Les cybercriminels s'adaptent aussi aux nouvelles prescriptions et régulations introduites, comme par exemple la mise en place d'une obligation d'annoncer.

Le nouveau groupe RansomedVC utilise ainsi une tactique d'extorsion, visant à avertir la victime de l'amende qui l'attend en vertu de la législation sur la protection des données (telle que le RGPD ou autres textes de loi) si elle ne paie pas la rançon demandée. Le groupe appelle sa demande de rançon «taxe pour la paix numérique» (en anglais *Digital Peace Tax*), de la même manière que le groupe de rançongiciels LockBit qualifie ses opérations de «service de test d'intrusion avec paiement a posteriori».

3.3.2.4 Des branches attractives pour les cybercriminels: énergie et santé

Les secteurs de l'énergie et de la santé sont des cibles privilégiées pour les acteurs de rançongiciels. Dans ces deux branches, au vu des prestations fournies, une indisponibilité du service ne peut être tolérée que sur de courtes périodes. Dans le cas des organisations du secteur de la santé, il faut par ailleurs souligner qu'elles offrent aux patients des services indispensables, souvent même vitaux, et qu'elles s'appuient pour ce faire de plus en plus sur des systèmes en réseau, des dossiers électroniques de patients et la télémédecine. Cela peut inciter les exploitants d'infrastructures critiques à rapidement payer la rançon exigée pour récupérer l'accès à leurs systèmes.

S'agissant des incidents survenus au cours du deuxième semestre de l'année 2023 dans le secteur de la santé, le traitement des patientes et patients a pu se poursuivre sans entraves

---

49 Kaspersky crimeware report: GoPIX, Lumar, and Rhysida. (securelist.com)

50 Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant (doj.gov)

majeures, et les activités des cliniques ont été maintenues. Les soins d'urgence sont souvent partiellement affectés voire parfois préventivement indisponibles, entraînant ainsi des retards ou des réaffectations de patients vers des hôpitaux environnants.

S'agissant des incidents dans le secteur énergétique (incluant les centrales nucléaires et les instituts de recherche), on constate depuis 2022 une nouvelle hausse des attaques par rançongiciels. Dans de nombreux cas, un tel incident a certes un impact sur les systèmes informatiques et entraîne le chiffrement de fichiers, mais il ne provoque pas de perturbations dans la production ou la distribution, l'approvisionnement en énergie pouvant se poursuivre sans interruption.

Recommandations

Sur le site web de l'OFCS, vous trouverez une liste de mesures préventives pour se protéger des rançongiciels et des consignes à suivre en cas d'incident.

3.4 Fuites de données / Gestion des données

Les données sont l'or de l'ère de l'information. Les fuites de données ont de sérieuses conséquences pour les organisations directement touchées, puisque les données volées peuvent aussi être utilisées pour d'autres attaques, visant cette fois des particuliers. Les cybercriminels sont conscients de cette évolution, raison pour laquelle les maliciels destinés à la collecte de données (appelés *infostealer*) et les plateformes illégales de vente de données sont de plus en plus populaires.[51] En décembre 2023, deux importantes fuites de données ont ainsi fait la une des journaux. D'une part, pendant les fêtes de fin d'année, différents pirates ont proposé gratuitement sur le *darknet* des millions de données personnelles sensibles provenant de fuites de données du monde entier.[52] D'autre part, l'entreprise 23andme, qui propose des tests génétiques pour la recherche par l'ADN, a annoncé que les données personnelles et génétiques de près de 7 millions de ses clients avaient été affectées par la fuite de données intervenue en octobre 2023.[53] Les auteurs de l'attaque se sont servis de mots de passe faibles et réutilisés d'utilisateurs, issus de fuites de données plus anciennes, ce qui a augmenté le risque d'autres attaques pour les personnes concernées, telles que des piratages de comptes, des attaques d'hameçonnage, des vols d'identité ou d'escroqueries financières. Ces incidents soulèvent une fois de plus la question de la responsabilité des organisations en matière de protection adéquate des données personnelles sensibles de leurs clients, même si les individus ont eux aussi la responsabilité de protéger leurs propres comptes en prenant des mesures de sécurité adaptées. En outre, il est nécessaire de prendre davantage conscience des données que l'on souhaite partager et avec quelles organisations.

---

51 Voir l'étude de *Trend Micro* sur les données et marchés: Your Stolen Data for Sale (trendmicro.com)

52 Cybercriminals launched «Leaksmas» event in the Dark Web exposing massive volumes of leaked PII and compromised data (resecurity.com)

53 23andMe confirms hackers stole ancestry data on 6.9 million users (techcrunch.com)

Recommandations

N'enregistrez que les données dont vous avez réellement besoin (économie de données) et effacez celles dont vous n'avez plus besoin ou archivez celles qui sont dignes d'être conservées mais que vous n'utilisez plus activement hors ligne. Protégez les accès aux comptes et aux données à l'aide de mots de passe solides et si possible d'une authentification multifactorielle (MFA).[54]

Remarque

La loi fédérale sur la protection des données (LPD) totalement révisée est entrée en vigueur le 1er septembre 2023. Celle-ci exige notamment que toute violation de la sécurité des données soit annoncée au Préposé fédéral à la protection des données et à la transparence (PFPDT).[55]

3.4.1 Fuites de données dans le secteur de la santé (à l'international)

Lors du deuxième semestre 2023, la tendance de fuite de données importante dans le secteur de la santé s'est poursuivie. Au niveau mondial, ce secteur occupe la troisième place en termes de fréquence des fuites de données, en particulier dans les pays anglophones. En Europe également, les organisations de santé sont dans la ligne de mire des cyberacteurs.

De nombreux acteurs malintentionnés ont des motifs financiers, ce qui rend leur choix concret des cibles essentiellement opportuniste. Le secteur de la santé est spécialement attractif pour les pirates, car ils partent du principe que les hôpitaux, les assurances-maladies et autres fournisseurs de prestations dans ce domaine seront enclins à payer la rançon exigée pour éviter la publication de ces données particulièrement sensibles et les dommages consécutifs, comme la perte de confiance ou les conséquences juridiques liées aux violations de la vie privée et de la protection des données. Les conséquences pour les clients et patients peuvent aussi être dévastatrices. Pour beaucoup, le fait de savoir que leurs données de santé peuvent être consultées par des personnes non autorisées constitue une grosse charge mentale. Les données volées peuvent être utilisées pour faire chanter les patients eux-mêmes (extorsion de données), mais permettent aussi des vols d'identité, des fraudes à l'assurance et d'autres infractions. Elles peuvent également tout simplement être revendues à des tiers.

Les attaques se différencient par leur complexité et leur forme. Les auteurs se servent pour ce faire de différents vecteurs d'attaque comme l'hameçonnage (voir chap. 2.3) et d'autres techniques d'ingénierie sociale[56] ou de vulnérabilités dans les logiciels et solutions cloud et d'attaques dirigées contre des prestataires de services tiers. Ce sont avant tout les attaques contre la chaîne de livraison (voir chap. 4.5.2 du rapport semestriel 2023/1) qui ont contribué à la hausse marquée des signalements. Certaines tendances déjà décrites au cours du premier semestre 2023, telles que les fuites de données causées par le groupe Cl0p ou les attaques

54 Voir Protégez vos comptes (ncsc.admin.ch).

55 DataBreach (edoeb.admin.ch)

56 Social Engineering – der Mensch als Schwachstelle (bsi.bund.de)

contre des fournisseurs de services logiciels, se sont poursuivies au deuxième semestre.[57] Alors que certains acteurs combinent parfois le vol de données avec des logiciels de chiffrement (comme les groupes Hunters International[58] et BlackCat/ALPHV), d'autres se concentrent sur le simple vol de données, comme le groupe Karakurt. Par le passé, quelques acteurs malintentionnés ont prétendu explicitement renoncer à attaquer des organisations dans le domaine de la santé, en raison de leur criticité. Mais ils constituent justement le type de groupes qui vendent leurs compétences sous forme de service (*ransomware-as-a-service*). Ces groupes comptent actuellement parmi les acteurs les plus actifs – comme le groupe LockBit ou BlackCat/ALPHV – ce qui ne les empêche pas de s'éloigner de cette attitude.[59]

Alors que les institutions de santé suisses ne se trouvent actuellement pas dans le viseur des acteurs malintentionnés, les attaques opportunistes peuvent également toucher le secteur suisse de la santé. Une cyberattaque contre le fournisseur de solutions numériques de santé Medgate en août puis une autre en septembre 2023 ont certes pu être neutralisées avec succès, mais des ruptures de services en ont quand même résulté, sur de courtes durées.[60] En octobre 2023, une attaque par logiciel de chiffrement contre le service psychiatrique de Bâle-Campagne a provoqué une panne technique des systèmes pendant douze jours, même si l'incident a pu être maîtrisé sans conséquences graves.[61] L'OFCS n'a connaissance d'aucune information indiquant que d'éventuelles fuites de données ont eu lieu dans le cadre de ces incidents.

3.4.2 Fuite de données à la ville de Baden

Le 4 décembre 2023, un cas de fuite de données au sein de la ville de Baden dans le canton d'Argovie a été rapporté.[62] Environ 3 Go de données de la ville ont été mis à disposition sur le forum de pirates BreachForum. Une analyse approfondie a montré que les données contenaient des informations telles que des noms, adresses, numéros de téléphone, numéros IBAN et factures d'habitantes et d'habitants, mais aussi des informations sur des investissements de la ville de Baden.[63]

La ville a réagi rapidement, en mandatant des experts externes pour la réponse aux incidents, en informant la population à travers un communiqué de presse[64] et en mettant en place un

---

57 L'exploitation en masse d'une vulnérabilité du logiciel de transfert de documents «MOVEit», qui a débuté en mai 2023, concerne désormais les données d'environ 90 millions de personnes dans le monde (état: décembre 2023), voir Unpacking the MOVEit Breach: Statistics & Analysis (emsisoft.com).

58 P. ex. les attaques contre le centre américain pour le cancer Fred Hutchinson et le centre de santé Crystal Lake: Hunters International ransomware gang claims to have hacked the Fred Hutch cancer center (securityaffairs.com); Ransomware gang claims to have stolen Crystal Lake Health Centers data (databreaches.net)

59 ALPHV a levé cette restriction dans un message datant de décembre 2023, en réaction apparemment à des mesures répressives des autorités américaines de poursuite pénale: ALPHV/BlackCat Claims Healthcare Restrictions Removed for Affiliates (hipaajournal.com). LockBit a attaqué un hôpital pour enfants aux États-Unis en décembre 2023, en contradiction avec ses promesses passées: Ransomware-Bande Lockbit wirft Skrupel über Bord (inside-it.ch)

60 Communiqué de presse: Cyberangriff auf Teile der IT-Infrastruktur von Medgate.pdf (medgate.ch)

61 Psychiatrie Baselland nimmt Normalbetrieb wieder auf - Psychiatrie Baselland (pbl.ch)

62 Baden ist Opfer eines Hackerangriffs geworden (nzz.ch)

63 Hackerangriff auf Baden: Meldeformular eingerichtet (badenertagblatt.ch)

64 Communiqué de presse: IT-Sicherheit der Stadt Baden (baden.ch)

formulaire d'annonce[65] pour les possibles victimes. Elle a également déposé une plainte auprès de la police. Selon les propres indications de la ville de Baden, les services informatiques ont remarqué à la mi-octobre 2023 que des inconnus tentaient d'obtenir un accès non autorisé aux serveurs des services des technologies de l'information et de la communication (TIC) des deux villes d'Aarau et de Baden. La faille de sécurité a toutefois été immédiatement comblée et d'autres mesures de sécurité ont été prises. En outre, la nature des données a permis de conclure qu'elles provenaient d'un système interne à l'administration, dans lequel sont gérées des factures adressées à la ville de Baden et émises par elle.[66] Il a par ailleurs été constaté qu'aucun autre système n'avait été compromis dans ce cadre.

L'incident illustre de manière exemplaire l'évolution d'un acteur malintentionné qui tente de s'établir dans un contexte criminel pour y gagner en crédibilité. Les données ont d'abord été publiées par une personne se faisant appeler DragonForce. À ce moment-là, cette personne n'était pas encore une utilisatrice de longue date sur cette page, car elle ne s'était enregistrée sur la plateforme que quelques jours avant. Le fait que les données aient été publiées sans contrepartie est aussi rare. Usuellement, la mise à disposition gratuite de données ne se s'effectue qu'en cas de non-coopération de la victime (voir aussi chap. 3.3) ou alors lorsqu'il s'agit d'hacktivistes, qui suivent le principe du *hack and leak*.[67] La ville de Baden n'a toutefois pas reçu de demande de rançon[68] et DragonForce n'a pas non plus démontré une attitude d'hacktiviste. Tout laisse donc à penser que cet acteur voulait se faire un nom sur la scène criminelle. Le fait que DragonForce ait ensuite créé à la mi-décembre sa propre page de fuite de données sur le *darknet*, en y listant une nouvelle fois la ville de Baden parmi les victimes, corrobore cette théorie. L'acteur y a ensuite également ajouté d'autres prétendues victimes. La liste de victimes se trouvant aux quatre coins du monde montre que l'acteur agit de manière opportuniste et non pas d'un ciblage précis.

Conclusion / Recommandations

Le principe suivant s'applique: les données sont précieuses. C'est la raison pour laquelle il existe un intérêt criminel à se procurer et à vendre ces données par des moyens déloyaux ou à faire chanter les victimes en les menaçant de publier des données sensibles. Par conséquent, le débat relatif à la sécurité des données ne devrait plus être de savoir si une fuite de données peut se produire mais plutôt de savoir quand elle va se produire et comment les données peuvent être rendues inutiles pour l'attaquant, même dans le cas extrême d'un incident. Il est en effet difficile d'obtenir une protection complète contre les fuites de données, en particulier celles causées par des acteurs malintentionnés très sophistiqués dotés de cybercapacités élevées. Les facteurs difficilement contrôlables tels que les vulnérabilités jouent un rôle à cet égard. D'où l'importance de respecter des principes essentiels en matière de sécurité et de gestion des données.

Le **fondement** de la conservation des données est le suivant: il faut définir quelles sont les données qui sont enregistrées et traitées, sous quelle forme, par quelles personnes, à quel

65 Meldestelle Datenexposition (baden.ch)

66 Stadt Baden: «Nur Rechnungsdaten betroffen» (inside-it.ch)

67 Voir le rapport semestriel 2023/1 (ncsc.admin.ch), chap. 2.3

68 Communiqué de presse: IT-Sicherheit der Stadt Baden (baden.ch)

endroit et avec qui elles sont partagées. Cela signifie notamment qu'il est plus judicieux d'enregistrer les données avec précaution, car s'il y a peu données à conserver, alors moins de données devront être protégées contre un accès non autorisé. Le stock de données devrait également être contrôlé à intervalles réguliers et les données inutiles effacées. Il faut aussi vérifier s'il est possible de procéder à un archivage des données électroniques hors ligne.

Les **aspects techniques** sont des points tout aussi importants dans la mise en œuvre. En plus des mesures traditionnelles pour une cyberhygiène[69] efficace, les données devraient si possible être stockées sous une forme chiffrée.

Sensibilisation: le personnel devrait être régulièrement sensibilisé à cette problématique. Des processus clairs et réalisables pour le traitement et la protection des données devraient par ailleurs être définis, mis en œuvre et contrôlés. Enfin, chacun devrait être conscient que les informations circulent librement sur le net, que ce soit de manière volontaire ou non. En effet des acteurs mal intentionnés peuvent les exploiter et les utiliser à des fins d'ingénierie sociale. En cas d'incident, ne vous laissez pas mettre sous pression, gardez votre calme et faites le cas échéant appel à des spécialistes.

Vérification: les données issues d'anciennes fuites de données peuvent être réutilisées pour d'autres attaques. Vérifiez périodiquement que vos données d'accès n'ont pas fuité, par exemple sur le site web Have I Been Pwned: Check if your email has been compromised in a data breach (haveibeenpwned.com) ou sur Identity Leak Checker du Hasso Plattner Institut (hpi.de). Utilisez si possible plusieurs de ces sites web, car si vos données d'accès ne sont pas identifiées comme ayant fait l'objet d'une fuite de données sur un site web, cela ne veut pas automatiquement dire que vos données d'accès n'ont pas fuité.

3.5 Systèmes de contrôle industriels (SCI) et technologie opérationnelle (TO)

La mise en réseau et la numérisation de tous les domaines de la vie progressent inexorablement et n'épargnent pas l'environnement industriel. Les dispositifs de commande de processus basés sur la technologie opérationnelle et intégrés dans les processus commerciaux numériques permettent des gains d'efficacité considérables et une mise en œuvre plus flexible. Une telle imbrication des mondes physique et numérique permet toutefois aussi des attaques de plus grande envergure contre les environnements de systèmes industriels. Des acteurs étatiques et aussi de plus en plus d'hacktivistes s'attaquent à des dispositifs de commande industriels insuffisamment sécurisés afin de manipuler des processus ou encore de susciter de l'inquiétude auprès de la population concernée. La plus grande menace pour l'exploitation des systèmes de contrôle industriels reste toutefois l'attaque par rançongiciel contre des systèmes informatiques périphériques et insuffisamment protégés, pouvant du moins temporairement entraver le bon fonctionnement du réseau dans son entier.

[69] Les thèmes-clés d'une cyberhygiène saine devraient notamment englober les sujets suivants: la gestion des mots de passe (p. ex. le hachage et le salage), le principe du moindre privilège, la segmentation du réseau et la gestion des correctifs et du cycle de vie des produits.

3.5.1 La plus grande agilité des acteurs étatiques dans le domaine des TO

Alors que les attaques de missiles contre les villes ukrainiennes et les infrastructures critiques ont dominé la couverture médiatique concernant les opérations de guerre, l'acteur Sandworm, attribué aux services de renseignement militaire russes, a mené une attaque de cybersabotage contre un opérateur du réseau électrique ukrainien le 10 octobre 2022. Selon le rapport[70] du prestataire de cybersécurité Mandiant de novembre 2023, les agresseurs ont obtenu un accès à l'infrastructure grâce à laquelle était exploitée une commande microSCADA servant à contrôler l'environnement de technologie opérationnelle (TO) des sous-stations de l'entreprise électrique. L'accès ainsi obtenu a ensuite été utilisé pour exécuter des ordres de mise hors service des sous-stations. La particularité de l'attaque analysée réside dans le mode opératoire appliqué, à savoir un recours à des fonctionnalités existantes pour l'attaque. Cette approche appelée *Living-of-the-Land* (LOTL) est observée depuis un certain temps déjà dans l'informatique et a désormais fait son entrée dans l'environnement TO. Par rapport à un maliciel[71] développé en interne, comme celui utilisé lors des attaques contre l'approvisionnement électrique à Kiev en 2016, ce procédé permet de réduire la durée entre l'obtention de l'accès au réseau et l'exécution de l'attaque de sabotage proprement dite. Comme les composants piratés sont aussi utilisés dans de nombreux autres environnements système, ce mode opératoire peut aussi s'adapter de manière plus flexible à d'autres objectifs.

Outre les attaques dirigées contre l'approvisionnement en électricité, d'autres actes de cybersabotage contre des cibles dans l'agriculture ukrainienne ont également été observés, parallèlement à des attaques de missiles.[72]

3.5.2 Perturbation de l'approvisionnement en eau par des hacktivistes

Dans le contexte de conflits internationaux tels que la guerre en Ukraine ou au Proche-Orient, les hacktivistes n'hésitent pas, outre les attaques contre la disponibilité (DDoS) ou la publication d'informations exfiltrées, à effectuer aussi des manipulations de sabotage sur les appareils TO exposés (voir aussi le chap. 3.6). Le groupe d'hacktivistes CyberAv3ngers a par exemple commencé à attaquer des appareils du fabricant israélien Unitronics.[73] Les activités ont perturbé des systèmes d'approvisionnement en eau et d'évacuation des eaux aux États-Unis[74] et en Irlande.[75] Leur proximité avec les Gardiens de la révolution iraniens est avérée[76]. Il utilise l'attention publique ainsi obtenue pour diffuser son message de propagande anti-israélienne (voir la figure 4).

---

70 Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology (mandiant.com)

71 CrashOverride Malware (cisa.gov)

72 Russian influence and cyber operations adapt for long haul and exploit war fatigue (blogs.microsoft.com)

73 Exploitation of Unitronics PLCs used in Water and Wastewater Systems (cisa.gov)

74 Water Utility Control System Cyber Incident Advisory: ICS/SCADA Incident at Municipal Water Authority of Aliquippa (waterisac.org)

75 Two-day water outage in remote Irish region caused by pro-Iran hackers (therecord.media)

76 IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities (cisa.gov)

Fig. 4: message de propagande sur des appareils compromis.[77]

En représailles, le groupe Predatory Sparrow a de nouveau perturbé le bon fonctionnement des stations-service[78] en Iran. Dans le contexte de la guerre en Ukraine, des hacktivistes comme la Team OneFist ou la People's Cyber Army of Russia publient régulièrement aussi sur leurs réseaux sociaux des informations présumées d'attaques contre des dispositifs de commande industriels.

Conclusion / Recommandations

Sécurisez vos systèmes industriels, afin d'empêcher les attaques décrites dans le présent chapitre. L'OFCS propose pour ce faire des mesures de protection pour les SCI.

Les normes minimales par secteur élaborées par l'Office fédéral pour l'approvisionnement économique du pays (OFAE) en collaboration avec les organisations sectorielles concernées proposent des solutions quant à elles un peu plus complètes.

Afin de vérifier si vos propres dispositifs de sécurité suffisent pour se protéger contre les menaces actuelles dans l'environnement industriel, il est possible de recourir au Emb3d Framework de MITRE.

3.5.3 Appareils IoT utilisés comme infrastructure d'attaque

L'utilisation d'appareils comme infrastructure d'attaque contre d'autres cibles est encore plus fréquente que les attaques contre les processus contrôlés par TO ou contre les appareils eux-mêmes. Les appareils (I)IoT[79] mal protégés ou arrivés en fin de cycle de vie, tels que les

77 Iranian Cyber Av3ngers Compromise Unitronics Systems (secureworks.com)

78 Iran petrol stations hit by cyberattack, oil minister says (reuters.com)

79 Internet des objets (wikipedia.org); Internet industriel des objets (wikipedia.org)

routeurs, caméras et autres sont particulièrement touchés. Le SektorCERT[80] danois a publié auprès de ses membres issus de la branche de l'approvisionnement en énergie en novembre 2023 une analyse sur une série de routeurs Zyxel compromis en mai 2023. Les vulnérabilités de ces appareils ont aussitôt été utilisées par plusieurs acteurs, afin de les intégrer par exemple dans des réseaux de zombies, qui peuvent ensuite être détournés pour des attaques DDoS contre d'autres cibles exposées sur Internet, telles que des sites web. Plusieurs routeurs de ces modèles ont été compromis en Suisse également. L'OFCS a informé les exploitants de ces routeurs, afin que les appareils puissent être nettoyés.

Outre Zyxel, d'autres anciens appareils Cisco et Netgear ont également été utilisés pour créer le *KV-Botnet,*[81] qui est attribué à l'acteur Volt Typhoon. Volt Typhoon est quant à lui lié à des attaques en reconnaissance contre des infrastructures critiques aux États-Unis.

Afin de rendre les abus plus difficiles à commettre contre de tels appareils à l'avenir, l'UE a fait passer une loi sur la cyberrésilience.[82] La nouvelle législation introduit des exigences en matière de cybersécurité à l'échelle de l'UE pour la conception, le développement, la production et la mise à disposition sur le marché de produits matériels et logiciels. Le règlement s'applique à tous les produits qui sont directement ou indirectement connectés à un autre dispositif ou à un réseau.

Conclusion / Recommandation

De nos jours, non seulement les appareils de réseau au sens propre du terme, tels que les routeurs, mais aussi de nombreux autres appareils électroniques domestiques sont connectés en réseau et constamment en ligne. Ces appareils doivent également être sécurisés de manière adéquate et mis à jour dès que des vulnérabilités sont connues.[83]

3.6 Le cyber dans les conflits

Le dernier rapport semestriel passait en revue les principaux événements dans le cyberespace en lien avec la guerre en Ukraine et indiquait qu'il n'y avait aucun signe de ralentissement des activités malveillantes. Il concluait qu'il existait un risque accru de dommages collatéraux liés à des groupes d'hacktivistes cherchant à mener des attaques destructrices.[84] Les deux pronostics se sont confirmés, comme le montrent les principaux développements dans les conflits au cours du deuxième semestre de l'année 2023.

80 The-attack-against-Danish-critical-infrastructure.pdf (sektorcert.dk)

81 Routers Roasting on an Open Firewall: the KV-botnet Investigation (blog.lumen.com)

82 Législation sur la cyberrésilience: accord du Conseil et du Parlement sur les exigences en matière de sécurité pour les produits numériques (consilium.europa.eu)

83 Cyberconseil: précautions à prendre avec l'Internet des objets (ncsc.admin.ch); Sécurité de l'Internet des objets (ncsc.admin.ch)

84 Voir le rapport semestriel 2023/1 (ncsc.admin.ch), chap. 4.7

3.6.1 La guerre en Ukraine

Les activités malintentionnées dans le cyberespace en lien avec la guerre en Ukraine se sont encore accélérées durant la deuxième moitié de l'année 2023. Le CERT ukrainien a ainsi indiqué avoir traité en 2023 un total de 2'543 incidents, soit 15% de plus qu'en 2022. Ces incidents concernaient la diffusion de maliciels, l'hameçonnage ou encore la compromission de comptes et de systèmes.[85] L'administration publique, la défense, l'approvisionnement énergétique et les télécommunications feraient apparemment partie des secteurs les plus ciblés. L'Ukraine a également fait état d'une tendance croissante de la Russie à cibler les autorités ukrainiennes qui enquêtent sur d'éventuels crimes de guerre russes par des campagnes d'espionnage. L'Ukraine a par ailleurs dénoncé des tentatives répétées d'attaque contre des cibles déjà attaquées par le passé.[86] Une nouvelle manière d'opérer des autorités ukrainiennes consiste à cet égard à rendre publics les résultats des cybercampagnes. Les services de renseignement militaires ukrainiens ont ainsi indiqué en novembre 2023 qu'une cyberopération complexe leur avait permis de mettre la main sur de nombreux documents confidentiels de l'Agence fédérale russe du transport aérien.[87] L'incident le plus marquant survenu durant ce semestre concerne toutefois l'Ukraine. Le 12 décembre 2023, le plus grand fournisseur de télécommunications du pays, qui approvisionne plus de la moitié de la population ukrainienne en téléphonie mobile et accès Internet, Kyivstar, a en effet été touché par un cyberincident. L'attaque a provoqué des interruptions de service pour les usagers de Kyivstar et également des services hébergés chez ce dernier. Cela s'est traduit par un accès limité aux services financiers pour une partie de la population et par une disponibilité de réception irrégulière d'alertes en cas de raids aériens.

Une restauration partielle des services a pu être effectuée au soir du 13 décembre 2023, mais il a fallu plus d'une semaine jusqu'à ce que tous les services soient à nouveau disponibles.[88] Les groupes d'hacktivistes KillNet et Solnetspek ont revendiqué cette attaque. KillNet n'a pas fourni de preuves et s'était déjà vanté par le passé d'être à l'origine d'incidents dont il n'était pas l'auteur. Solnetspek a en revanche publié des captures d'écran attestant de son accès privilégié aux systèmes de Kyivstar. Selon l'Ukraine et diverses entreprises de sécurité informatique occidentales, le groupe Sandworm, que l'on attribue aux services de renseignement militaire russes et qui avait déjà pris pour cible des entreprises de télécommunications par le passé, serait à l'origine de l'attaque, se servant de Solnetspek comme façade.[89] L'incident aurait été une combinaison entre des attaques DDoS et un usage de maliciels d'effacement de données (aussi appelés *wipers*). Solnetspek prétend avoir «détruit» plus de 10'000 stations et 4'000 serveurs de Kyivstar, y compris toutes les mémoires dans le cloud et les systèmes de sauvegarde. En mars 2023, il y avait déjà eu de premières tentatives de pénétrer dans les systèmes de l'organisation. En mai 2023, les pirates ont finalement réussi à obtenir un premier accès en compromettant le compte d'un collaborateur de Kyivstar et ont pu se propager dans

---

85 The CERT-UA Team has processed 2,543 cyber incidents over 2023 (cip.gov.ua)

86 How russian government-controlled hacking groups shift their tactics, objectives and capacities (cip.gov.ua)

87 Defence Intelligence of Ukraine conducted a cyber operation against Rosaviatsia (gur.gov.ua)

88 NetBlocks on X: Metrics show that connectivity on Ukraine telco Kyivstar is now largely restored (twitter.com); Russian hackers were inside Ukraine telecoms giant for months (reuters.com)

89 Hacker Group Linked to Russian Military Claims Credit for Cyberattack on Kyivstar (wired.com); Russia's Sandworm blamed for Kyivstar telecom cyberattack (theregister.com)

les systèmes.[90] Cet accès non détecté pendant des mois aurait permis, entre autres, d'obtenir des informations sur les clients, de localiser des téléphones portables, d'intercepter des SMS et de compromettre notamment des comptes Internet protégés par une authentification liée à un numéro de téléphone portable, comme par exemple Telegram.

Il est hautement improbable que la Suisse soit la cible de telles actions de sabotage commises par des acteurs étatiques. Il est toutefois probable que des groupes d'hacktivistes impliqués dans un conflit prennent la Suisse dans leur viseur. C'est ainsi que NoName057(16), un groupe d'hacktivistes prorusse, qui avait déjà mené des campagnes d'attaques DDoS en juin 2023 contre des sites web suisses,[91] a perpétré cinq attaques DDoS contre des sites web suisses durant le deuxième semestre de l'année 2023. Ces attaques étaient avant tout une réaction aux activités suisses en lien avec la guerre en Ukraine. Le 28 novembre, soit trois jours après la visite du président de la Confédération en Ukraine, NoName057(16) a par exemple mené des attaques contre des sites web de l'administration fédérale et d'organisations actives dans le secteur financier et le tourisme. Ces attaques n'ont certes eu que peu d'impact (il n'y a pas eu de restriction notable de la disponibilité), mais elles sont utilisées par les groupes d'hacktivistes à des fins de propagande.[92] À l'inverse des campagnes précédentes, NoName057(16) n'attaque plus continuellement des sites web d'un même pays pendant une semaine, mais change de cible de jour en jour.

3.6.2 Conflit au Proche-Orient

Après l'attaque du Hamas contre Israël le 7 octobre 2023, qui a entraîné une nouvelle escalade de la violence dans la région, d'innombrables groupes d'hacktivistes ont annoncé leur implication dans le conflit. À maints égards, le hacktivisme lié à ce conflit fut similaire à celui observé dans la guerre en Ukraine. Une grande partie des activités de ces groupes d'hacktivistes consiste en de la propagande et/ou de la désinformation. Seule une petite partie d'hacktivistes ont mené des actions dans le cyberespace qui ont eu un impact direct sur des systèmes informatiques. Ces actions concernaient principalement la défiguration de sites web et/ou des attaques DDoS. Elles ont également été observées contre des cibles situées hors de la zone de conflit, généralement en réponse à des déclarations de soutien à l'un des protagonistes.[93] Plusieurs groupes d'hacktivistes ont toutefois exécuté des actions à la fois plus raffinées et plus dommageables. Le groupe Cyber Toufan aurait ainsi compromis plus d'une centaine d'organisations israéliennes, publiant des données sensibles après avoir perturbé leur infrastructure en utilisant des *wipers.*[94] Le groupe Karma aurait lui aussi infiltré plusieurs organisations israéliennes, afin d'y déployer un *wiper* unique en son genre, proposant une version pour les systèmes Windows et une autre pour les systèmes Linux.[95] Quant au groupe Cyber Av3ngers, il a ciblé des systèmes de contrôle industriels de production israélienne, en défigurant leur interface utilisateur et en la rendant inutilisable. Les systèmes ont été pris dans

---

90 CEO of Ukraine's largest telecom operator describes Russian cyberattack that wiped thousands of computers (therecord.media); Exclusive: Russian hackers were inside Ukraine telecoms giant for months (reuters.com)

91 Voir le rapport semestriel 2023/1 (ncsc.admin.ch), chap. 2.1
Rapport d'analyse détaillé sur les attaques DDoS «NoName057(16)» (ncsc.admin.ch)

92 Ukraine-Krieg: Russische Hackergruppe schürt in der Schweiz Verunsicherung (nzz.ch)

93 Hacktivist Involvement in Israel-Hamas War Reflects Possible Shift in Threat Actor Focus (securityscorecard.com)

94 Cyber Toufan goes Oprah mode, with free Linux system wipes of over 100 organisations (doublepulsar.com)

95 Mission «Data Destruction»: A Large-scale Data-Wiping Campaign Targeting Israel (securityjoes.com)

le viseur indépendamment de leur situation géographique, ce qui a provoqué des incidents dans plusieurs pays situés hors de la zone de conflit.[96] Pour certains de ces groupes, on suppose qu'ils servent de façade pour des acteurs étatiques, en particulier l'Iran, ou qu'ils sont soutenus par un État.[97] Les États peuvent en effet profiter de la difficulté de prouver de tels liens pour nier leur responsabilité tout en augmentant l'impact médiatique de leurs actions.

3.6.3 Développements futurs

Rien n'indique que les cyberactivités en lien avec la guerre en Ukraine ou le conflit au Proche-Orient vont diminuer. La tendance d'implication dans le cyberespace de groupes d'hacktivistes émanant de la seule société civile ou servant de façade à un État tiers dans le cadre de conflits semble se consolider et s'établir comme une nouvelle norme. Bien que ces groupes ne semblent avoir été décisifs pour aucun des protagonistes, selon les informations disponibles à ce jour, leurs activités pourraient également inciter les forces gouvernementales à s'engager dans le domaine cyber et retenir leur attention. De plus, ces bruits de fond supplémentaires, combinés à la vue incomplète de la situation due au conflit, rendent son évaluation plus difficile.

---

96 Voir chap. 3.5.2

97 Iranian Hacktivist Proxies Escalate Activities Beyond Israel (checkpoint.com); Iran surges cyber-enabled influence operations in support of Hamas (microsoft.com)