Rapport de renseignement

Revue mensuelle rétroactive des cybermenaces

SOC – Centre opérationnel de sécurité

Novembre 2023

canton de vaud
LIBERTÉ ET PATRIE

Direction générale du numérique
et des systèmes d'information (DGNSI)

Table des matières

Introduction

Ce rapport présente, de façon mensuelle, les actualités liées à la sécurité informatique que le Centre opérationnel de sécurité (SOC) de l'État de Vaud a estimé intéressantes. Il couvre à la fois des éléments internationaux et suisses, des incidents auxquels le SOC a dû répondre et les vulnérabilités qui ont été particulièrement médiatisées.

Le paysage global des menaces

Actualités internationales

Le mois de novembre a commencé avec la révélation d'une attaque ransomware majeure qui a perturbé les services gouvernementaux locaux dans de nombreuses villes et districts de l'ouest de l'Allemagne. Survenant fin octobre et annoncée début novembre, cette attaque, orchestrée par un groupe de hackers non identifié, a ciblé Südwestfalen IT, un prestataire de services municipaux. Plus de 70 municipalités, majoritairement situées dans l'État de Rhénanie-du-Nord-Westphalie, ont été affectées, entraînant une sévère limitation des services gouvernementaux. Malgré l'indisponibilité des systèmes en ligne, les administrations ont maintenu des services en personne. Les autorités de police et les agences de cybersécurité allemandes ont mené une enquête, tandis que les experts en cybersécurité ont souligné la sensibilité temporelle de l'attaque, affectant potentiellement les transactions financières des gouvernements locaux. Une enquête complexe et approfondie a été anticipée pour évaluer l'ampleur des dégâts et identifier les responsables [1].

C'est dans ce contexte d'attaques ransomware sévissant depuis plusieurs mois que près de cinquante pays membres de l'International Counter Ransomware Initiative (CRI), dont la Suisse, se sont engagés à ne pas payer de rançons en cas de cyberattaque. Lors de son troisième sommet à Washington, la coalition a réaffirmé son engagement à combattre les gangs de ransomware. Les gouvernements ont promis de ne pas céder aux demandes de rançons pour décourager ces paiements et perturber l'écosystème de paiement des ransomwares. L'International Counter Ransomware Task Force (ICRTF), créée l'année dernière, favorisera le partage de connaissances et la collaboration transnationale pour contrer efficacement cette menace [2].

Dans les différentes démarches, cette fois techniques, visant à diminuer le risque d'exploitation et la surface d'attaque, l'information est tombée en début du mois que Microsoft va implémenter des politiques d'Accès Conditionnel nécessitant l'authentification multifacteur (MFA) pour les administrateurs accédant à des portails tels que Microsoft Entra, Microsoft 365, Exchange et Azure [3]. Ces politiques seront graduellement ajoutées en mode « rapport » et devront être examinées et activées par les administrateurs dans les 90 jours suivant leur déploiement. Les administrateurs pourront modifier ces politiques, y compris l'exclusion de comptes spécifiques. L'objectif est d'atteindre une authentification multi facteur à 100%, réduisant significativement le risque de prise de contrôle des comptes. Plus généralement, Microsoft, face à des défis croissants en matière de cybersécurité, a lancé l'initiative "Secure Future Initiative (SFI)" [4]. Cette démarche stratégique vise à développer des outils avancés pour protéger ses produits et services. Brad Smith, vice-président, annonce cette initiative comme réponse aux cyberattaques de plus en plus sophistiquées.

En novembre, la vulnérabilité Citrix Bleed, affectant les produits Citrix, a été massivement exploitée par des pirates informatiques liés à des États-nations et des gangs de cybercriminels, a alerté notamment l'Agence américaine de cybersécurité et de sécurité des infrastructures (CISA) avec le FBI [5]. Malgré un avertissement de Citrix en octobre classant la faille à 9,4 sur 10 en termes de gravité, de nombreux dispositifs restaient vulnérables en novembre, surtout en Amérique du Nord. La CISA américaine a ordonné la correction du bug pour les agences civiles fédérales avant le 8 novembre. Des attaques notables incluent celle contre Boeing, exploitée par le groupe de ransomware LockBit [6].

Dans un contexte géopolitique bien chargé, l'analyse post-mortem publiée par Mandiant le 9 novembre 2023 a révélé une attaque de cyber espionnage russe sophistiquée contre le réseau électrique ukrainien et attribué au groupe ATP Sandworm [7]. En octobre 2022, les hackers militaires russes ont déclenché des disjoncteurs d'une sous-station, causant une panne de courant temporaire. Qualifiée de forme rare et avancée de cyberwarfare, elle a été caractérisée par Mandiant comme une "attaque cybernétique multi-événements", utilisant des techniques innovantes pour infiltrer les systèmes de contrôle industriel (ICS). Cette opération souligne la sophistication croissante des capacités cybernétiques de la Russie. Par ailleurs, une attaque majeure contre l'infrastructure critique danoise a été signalée en mai 2023 et publiée le 12 novembre par SektorCERT, une organisation à but non lucratif soutenue par des entreprises danoises spécialisées dans les infrastructures critiques [8]. Cette dernière a découvert que 22 entreprises danoises de l'énergie ont été compromises lors d'une attaque coordonnée, exploitant une vulnérabilité critique dans les produits de Zyxel, un fabricant de pare-feu. Cette attaque, la plus étendue de l'histoire du Danemark, a été réalisée en deux vagues, affectant les systèmes de contrôle

industriels de ces entreprises. Bien que l'implication du groupe APT lié à la Russie, Sandworm, n'ait pas été confirmée avec certitude, la nature et l'ampleur de l'attaque suggèrent une possible implication d'acteurs étatiques. Ces révélations mettent en lumière comme les infrastructures critiques à l'échelle mondiale sont désormais de plus en plus ouvertement visées, avec la Russie se distinguant particulièrement, notamment grâce au groupe Sandworm, par son expertise et sa détermination à les cibler.

Dans une escalade audacieuse des tactiques de ransomware, le groupe ALPHV, également connu sous le nom de "BlackCat", dans le courant du mois de novembre a déposé une plainte officielle auprès de la Securities and Exchange Commission (SEC) des États-Unis contre MeridianLink, une entreprise qu'ils ont attaquée, pour non-respect des règles de divulgation en cas de violation de sécurité [9]. Cette tactique d'extorsion inhabituelle s'ajoute à l'arsenal d'ALPHV, qui s'est également illustré par la formation d'alliances avec des groupes criminels violents comme "the Com" [10], spécialisés dans le "SIM swapping". Cette collaboration [11], soulignée par leur rôle dans le piratage des casinos MGM, mélange ingénierie sociale et menaces physiques, marquant un tournant dans les méthodes de cyberchantage par l'extrémisation de techniques de pression et la collaboration entre les groupes de ransomware d'Europe de l'Est et les criminels anglophones.

Toujours concernant l'évolution des ransomwares, en fin de mois, les chercheurs de la société Adlumin se sont penchés sur la souche de rançongiciel nommée Play, utilisé entre-autres dans l'attaque contre Xplain, qui est récemment passée à un modèle de Ransomware-as-a-Service (RaaS). Adlumin a découvert que les attaques récentes utilisant le ransomware Play montraient des tactiques presque identiques, suggérant une exécution par des affiliés suivant des instructions précises [12]. Initialement, les opérateurs de Play exploitaient des failles dans Microsoft Exchange Server et menaient eux-mêmes les attaques. Cette évolution marque un tournant, rendant Play plus accessible et diversifiant les menaces, en attirant notamment des cybercriminels moins expérimentés [13].

En fin du mois, la société spécialisée dans la gestion des identités et des accès Okta a publié une mise à jour concernant le piratage précédemment annoncé en revoyant l'impact fortement à la hausse. En effet, l'attaque subie en septembre a été plus étendue que prévu, affectant tous les utilisateurs de son système de support client et pas seulement le 1% précédemment évoqué. Cette brèche a été initiée par le vol d'identifiants d'accès valides à partir du compte Google personnel d'un employé, qui avait utilisé ce compte pour se connecter au navigateur Chrome sur un ordinateur portable géré par Okta et y avait sauvegardé son nom d'utilisateur et mot de passe. Bien qu'il n'y ait pas eu de vol présumé de "données personnelles sensibles", Okta a averti du risque d'attaques de phishing ou d'ingénierie sociale visant les utilisateurs, en particulier les administrateurs, en utilisant les informations dérobées [14].

Actualités suisses

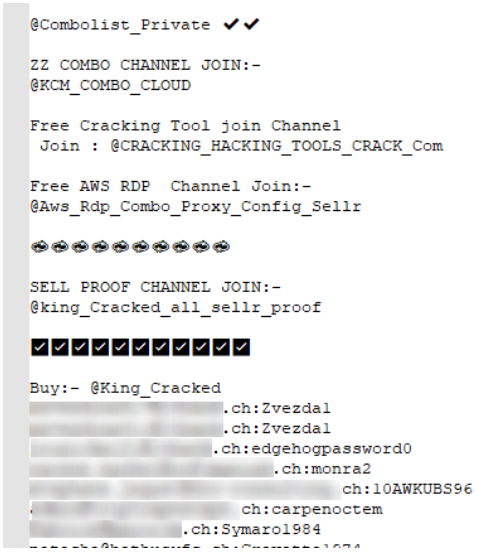
Le Conseil fédéral a récemment apporté des clarifications importantes concernant les missions de l'Office fédéral de la cybersécurité (22 novembre 2023 - [15]). Ces ajustements visent à renforcer le rôle de l'office dans la protection des infrastructures critiques contre les cybermenaces. Le gouvernement suisse cherche ainsi à améliorer la coordination et la collaboration en matière de cybersécurité pour faire face aux défis croissants dans ce domaine. Cependant, ces avancées sont contrebalancées par une évolution préoccupante signalée dans un autre article (9 novembre 2023 - [16]) : le pouvoir du Centre national de cybersécurité s'affaiblit. Des modifications récentes ont conduit à une diminution de l'autorité de cet organe dans la gestion des questions de cybersécurité. Ces changements soulèvent des inquiétudes quant à la capacité du centre à protéger efficacement les systèmes informatiques nationaux contre les cybermenaces. Ce paradoxe entre la clarification des tâches de l'Office fédéral de la cybersécurité et l'affaiblissement du pouvoir du Centre national de cybersécurité met en lumière les défis complexes auxquels est confrontée la Suisse dans la protection de ses infrastructures critiques dans un paysage numérique en constante évolution. Il souligne également la nécessité de trouver un équilibre délicat entre différentes entités pour assurer une défense robuste contre les attaques cybernétiques.

La Confédération a communiqué le 14 novembre [17] que l'un de ses fournisseurs de logiciels, la firme bâloise Concevis, avait subi une attaque par ransomware. Le butin des hackers malveillants pourrait contenir d'anciennes données opérationnelles de l'administration fédérale. Le 16 novembre, les administrations de Bâle-Ville et de Bâle-Campagne ont confirmé être touchées par l'attaque contre Concevis. Les cantons utilisent les logiciels du fournisseur bâlois et ont déposé

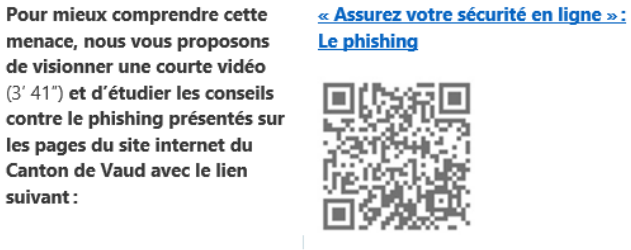
une plainte pénale après avoir été informés de l'attaque par ransomware. Les services affectés incluent la police et l'Office cantonal des affaires sociales de Bâle-Campagne, ainsi que l'Office de l'environnement et de l'énergie de Bâle-Ville. Le 17 novembre, la ville de Lucerne annonce que Concevis l'a alertée sur le cyberincident. La ville, cliente de l'éditeur touché par le ransomware, estime que des données personnelles anciennes liées aux demandes d'autorisation ont été affectées, incluant des informations telles que le nom, l'adresse, la date de naissance et l'e-mail. Le 24 novembre, une mise à jour révèle que des fragments des données volées à Concevis ont potentiellement émergé sur le Darknet. Les données, transmises par une source anonyme, comprennent des informations sensibles de clients américains auprès de banques suisses. Concevis aurait reçu une demande de rançon, mais ne prévoit pas d'y répondre. La Confédération n'a jamais vérifié la sécurité informatique de Concevis malgré l'attaque récente via le fournisseur Xplain. Le Préposé fédéral à la protection des données a ouvert une enquête préliminaire, et des révélations indiquent que les mandats attribués à Concevis par l'administration fédérale n'ont pas fait l'objet d'appels d'offres publics selon Republik. [18]

Principales observations et interventions du SOC

Des fichiers contenant des adresses e-mails associées à des mots de passe ont été trouvés sur Internet, touchant spécialement des adresses en « .ch ». Et une centaine parmi celles-ci concernait des utilisateurs « @vd.ch ». Après une analyse plus approfondie, il apparaît que ces combinaisons sont très probablement créées de toutes pièces, sous forme de « credential stuffing ». Cette technique utilise des paires de nom d'utilisateur et de mot de passe obtenues à partir de fuites de données sur d'autres sites ou services, et exploite la mauvaise habitude courante de réutiliser les mêmes mots de passe sur plusieurs comptes en ligne. Si l'attaquant trouve un nom d'utilisateur et un mot de passe qui fonctionnent sur un site, il peut les essayer sur d'autres sites en pariant sur la réutilisation des mots de passe. Les fichiers trouvés contenaient également de la publicité et des liens Telegram pour acheter ce genre de listes ou des outils de hacking. Ceci laisse à penser que les données ne sont pas valides :



Un e-mail de sensibilisation au phishing a été envoyé à tous les employés à fin novembre, qui a suscité un certain nombre de commentaires. Un élément intéressant est la réaction au QR-code contenu dans le message :



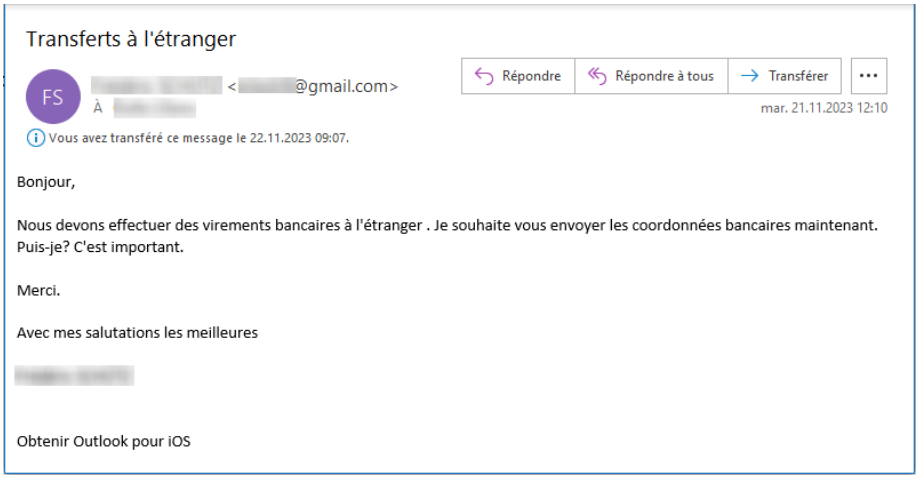
Des attaques de phishing utilisant des QR-code sont récemment apparus et des utilisateurs trouvaient que son utilisation dans un message de sensibilisation était contre-productive. Au contraire, nous pensons que de permettre aux utilisateurs d'être confrontés aux méthodes de communications les plus récentes et d'en comprendre les risques et possibilités est justement du ressort de la sensibilisation.

Incidents et activités externes et/ou globaux

Un partenaire de l'ACV, utilisant le RCV pour son accès Internet, a contacté le SOC pour un souci opérationnel sur son accès VPN SSL. N'ayant pas de visibilité réseau sur les requêtes externes effectuées sur cet équipement, plusieurs logs nous ont été demandés. Après investigation et avoir déclenché un exercice de réponse à un cyber incident, leur équipement VPN était activement scannée depuis Internet. L'intervention rapide de l'équipe Télécom a permis d'isoler le flux à quelques IP. Le partenaire a profité de cet incident pour décommissionner le VPN SSL pour une solution plus robuste et récente.

Parmi les e-mails soumis au SOC deux ont retenu notre attention en particulier.

Le premier concerne un cas dit « d'arnaque au président », sous la forme d'un e-mail envoyé au secrétariat d'une école professionnelle et usurpant le nom de son directeur :


Transferts à l'étranger

FS <[redacted]@gmail.com>

À [redacted]

Répondre | Répondre à tous | Transférer | ...

mar. 21.11.2023 12:10

Vous avez transféré ce message le 22.11.2023 09:07.

Bonjour,

Nous devons effectuer des virements bancaires à l'étranger . Je souhaite vous envoyer les coordonnées bancaires maintenant. Puis-je? C'est important.

Merci.

Avec mes salutations les meilleures

[redacted]

Obtenir Outlook pour iOS

Ce message, typique de ce type d'arnaque, enjoint son destinataire à effectuer un virement bancaire frauduleux. Des recherches ont été effectuées par l'attaquant, qui a repéré le nom du directeur ainsi que d'une personne du secrétariat, et utilise le français pour son message. Heureusement, l'utilisation d'une adresse e-mail Gmail permet rapidement de détecter ce cas. Le SOC a averti l'équipe IT/sécurité concernée et signalé à Google les adresses e-mail Gmail utilisées dans cette attaque. Ceci nous permet de rappeler que les défenses les plus efficaces contre ces cas sont : sensibiliser les utilisateurs potentiellement exposés (par exemple avec droit de signature, etc.), et s'assurer que les processus de paiements sont suffisamment robustes (contrôle 4 yeux, validation, etc.).

Le second cas concerne des e-mails de phishing envoyés à partir d'une adresse compromise. Ce genre de cas est malheureusement très fréquent mais ici l'adresse et le compte en question était celui d'un partenaire ayant participé à des projets internes. Le phishing avait pour objectif apparent de récupérer d'autres accès à des comptes Office 365 afin de mener de nouvelles attaques. Il faut néanmoins également considérer le risque que les données échangées par e-mail avec ce partenaire soient compromises, car l'attaquant ayant eu accès à la messagerie aura éventuellement pris le temps d'en extraire tous les messages. Selon la nature et la confidentialité des échanges il est important de pouvoir prendre les mesures nécessaires. Dans le cas présent, le SOC a pris contact avec le partenaire afin d'établir si une exfiltration d'e-mails avait eu lieu ainsi que la quantité et nature des données échangées par e-mails. Il est important de rappeler ici l'importance de mettre en place des politiques de sécurité claires concernant l'échange d'informations sensibles ou simplement l'échange de fichiers.

Vulnérabilités les plus médiatisées du mois

Ce tableau dresse une liste non exhaustive des failles fortement relayées par les médias durant le mois. L'application régulière des mises à jour en cas de composant vulnérable est l'une des protections les plus importantes contre les cyberattaques.

Identifiant	Informations
CVE-2023-42916 CVE-2023-42917	Apple iOS 17: Les deux failles ont été découvertes dans le moteur de navigation WebKit, permettant aux attaquants d'accéder à des informations sensibles via une vulnérabilité de lecture hors limites, et d'exécuter du code arbitraire via une faille de corruption de mémoire sur des appareils vulnérables en utilisant des pages web malveillantes.
n/a	Palo Alto Networks : Le 31 décembre 2023, les certificats root des pare-feu et appareils de Palo Alto Networks utilisant le logiciel PAN-OS arriveront à expiration. Si vous ne renouvelez pas vos certificats avant cette date, vos pare-feu et appareils Panorama ne pourront plus établir de nouvelles connexions aux services cloud de Palo Alto Networks, ce qui aura un impact sur le trafic réseau et pourrait entraîner une interruption du réseau. [19]
Reptar CVE-2023-23583	Cette vulnérabilité, révélée par Google [20], impacte de nombreux processeurs Intel [21], y compris ceux utilisés dans les environnements de cloud computing et dans les hyperviseurs. Sa portée étendue, affectant potentiellement une grande variété d'ordinateurs et de serveurs, en a fait un sujet de préoccupation.
CVE-2023-47246	Cette vulnérabilité dans le logiciel de gestion des services informatiques (ITSM) SysAid [22] a été utilisée par des cybercriminels pour lancer des attaques avec le ransomware Clop. Cette vulnérabilité zero-day a été largement exploitée dans des attaques de ransomware [23], attirant une attention significative sur les dangers de sécurité des logiciels ITSM fréquemment employés et dotés d'un portail d'accès internet.

Sources

Cette section fournit les sources d'informations utilisées pour la rédaction du contenu de ce rapport.

[1] « Massive ransomware attack hinders services in 70 German municipalities ». Consulté le: 12 décembre 2023. [En ligne]. Disponible sur: https://therecord.media/massive-cyberattack-hinders-services-in-germany

[2] « Près de cinquante pays s'engagent à ne pas céder aux gangs de ransomware ». Consulté le: 12 décembre 2023. [En ligne]. Disponible sur: https://www.ictjournal.ch/news/2023-11-06/pres-de-cinquante-pays-sengagent-a-ne-pas-ceder-aux-gangs-de-ransomware

[3] « Microsoft will roll out MFA-enforcing policies for admin portal access », BleepingComputer. Consulté le: 12 décembre 2023. [En ligne]. Disponible sur: https://www.bleepingcomputer.com/news/microsoft/microsoft-will-roll-out-mfa-enforcing-policies-for-admin-portal-access/

[4] B. Smith, « A new world of security: Microsoft's Secure Future Initiative », Microsoft On the Issues. Consulté le: 14 décembre 2023. [En ligne]. Disponible sur: https://blogs.microsoft.com/on-the-issues/2023/11/02/secure-future-initiative-sfi-cybersecurity-cyberattacks/

[5] « #StopRansomware: LockBit 3.0 Ransomware Affiliates Exploit CVE 2023-4966 Citrix Bleed Vulnerability | CISA ». Consulté le: 12 décembre 2023. [En ligne]. Disponible sur: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-325a

[6] « 'Citrix Bleed' vulnerability targeted by nation-state and criminal hackers: CISA ». Consulté le: 12 décembre 2023. [En ligne]. Disponible sur: https://therecord.media/citrix-bleed-bug-targeted-cisa

[7] « Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology », Mandiant. Consulté le: 12 décembre 2023. [En ligne]. Disponible sur: https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology

[8] « SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf ». Consulté le: 12 décembre 2023. [En ligne]. Disponible sur: https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf

[9] « Hackers Weaponize SEC Disclosure Rules Against Corporate Targets ». Consulté le: 13 décembre 2023. [En ligne]. Disponible sur: https://www.darkreading.com/cyber-risk/hackers-weaponize-sec-disclosure-rules-against-corporate-targets

[10] A. J. Vicens, « Youth hacking ring at the center of cybercrime spree », CyberScoop. Consulté le: 13 décembre 2023. [En ligne]. Disponible sur: https://cyberscoop.com/youth-hacking-ring-at-the-center-of-cybercrime-spree/

[11] J. Cox ·, « SIM Swappers Are Working Directly with Ransomware Gangs Now », 404 Media. Consulté le: 13 décembre 2023. [En ligne]. Disponible sur: https://www.404media.co/sim-swappers-are-working-directly-with-ransomware-gangs-now/

[12] « PlayCrypt Ransomware-as-a-Service Expands Threat from Script Kiddies and Sophisticated Attackers | Adlumin SaaS Security ». Consulté le: 13 décembre 2023. [En ligne]. Disponible sur: https://adlumin.com/post/playcrypt-ransomware-as-a-service-expands-threat-from-script-kiddies-and-sophisticated-attackers/

[13] « Play Ransomware Goes Commercial - Now Offered as a Service to Cybercriminals », The Hacker News. Consulté le: 13 décembre 2023. [En ligne]. Disponible sur: https://thehackernews.com/2023/11/play-ransomware-goes-commercial-now.html

[14] M. Bagwe, M. J. S. November 29, et 2023, « Okta Says Hacker Stole Every Customer Support User's Details ». Consulté le: 13 décembre 2023. [En ligne]. Disponible sur: https://www.databreachtoday.eu/okta-says-hacker-stole-every-customer-support-users-details-a-23712

[15] « Le Conseil fédéral clarifie les tâches de l'Office fédéral de la cybersécurité ». Consulté le: 8 décembre 2023. [En ligne]. Disponible sur: https://www.ictjournal.ch/news/2023-11-22/le-conseil-federal-clarifie-les-taches-de-loffice-federal-de-la-cybersecurite

[16] « Le pouvoir du Centre national de cybersécurité s'affaiblit ». Consulté le: 8 décembre 2023. [En ligne]. Disponible sur: https://www.ictjournal.ch/news/2023-11-09/le-pouvoir-du-centre-national-de-cybersecurite-saffaiblit

[17] « Cyberattaque contre l'entreprise Concevis: l'administration fédérale est également concernée ». Consulté le: 15 novembre 2023. [En ligne]. Disponible sur: https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-98595.html

[18] « Concevis: des données du fisc auraient fuité (update 3) ». Consulté le: 8 décembre 2023. [En ligne]. Disponible sur: https://www.ictjournal.ch/news/2023-11-24/concevis-des-donnees-du-fisc-auraient-fuite-update-3

[19] « LIVEcommunity - Emergency Update Required - PAN-OS Root and Default Certificate Expiration - LIVEcommunity - 564672 ». Consulté le: 8 décembre 2023. [En ligne]. Disponible sur: https://live.paloaltonetworks.com/t5/customer-advisories/emergency-update-required-pan-os-root-and-default-certificate/ta-p/564672
[20] « Google researchers discover 'Reptar,' a new CPU vulnerability », Google Cloud Blog. Consulté le: 12 décembre 2023. [En ligne]. Disponible sur: https://cloud.google.com/blog/products/identity-security/google-researchers-discover-reptar-a-new-cpu-vulnerability
[21] « INTEL-SA-00950 », Intel. Consulté le: 12 décembre 2023. [En ligne]. Disponible sur: https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00950.html
[22] M. Mahajna, « SysAid On-Prem Software CVE-2023-47246 Vulnerability », SysAid. Consulté le: 12 décembre 2023. [En ligne]. Disponible sur: https://www.sysaid.com/blog/service-desk/on-premise-software-security-vulnerability-notification
[23] E. Kovacs, « SysAid Zero-Day Vulnerability Exploited by Ransomware Group », SecurityWeek. Consulté le: 12 décembre 2023. [En ligne]. Disponible sur: https://www.securityweek.com/sysaid-zero-day-vulnerability-exploited-by-ransomware-group/