Engagement accru de la Confédération dans le domaine de la cybersécurité : quel est le niveau de sécurité de la Suisse ?

Rapport de synthèse | 16e FSS Security Talk du 21 février 2024, Swiss Cyber Security Days

En tant que pays le plus innovant du monde, la Suisse représente une cible attrayante pour les cyberattaques. De nombreuses entreprises et organisations ont pris conscience du danger. La Confédération accorde elle aussi une grande importance au thème de la cybersécurité et d'autres changements institutionnels et législatifs importants ont été décidés l'année dernière. Lors du 16e FSS Security Talk, qui s'est tenu pour la première fois dans le cadre des Swiss Cyber Security Days, ces changements ont également été discutés par des experts de renom tels que **Martin von Muralt** (délégué pour le Réseau national de sécurité RNS), **Maja Riniker** (conseillère nationale, membre de la CPS-N et du groupe parlementaire Cyber), **Tobias Schoch** (Chief Security Officer, AXA Suisse), **Gerhard Andrey** (conseiller national, membre de la CPS-N et du groupe parlementaire Cyber) ainsi que **Florian Schütz** (directeur de l'Office fédéral de la cybersécurité).

Quels effets peut-on attendre de la création du nouveau Secrétariat d'État à la politique de sécurité SEPOS et de l'Office fédéral de la cybersécurité BACS sur l'architecture de la cybersécurité en Suisse ? Dans quelle mesure la loi sur la sécurité de l'information modifie-t-elle les exigences minimales en matière de sécurité de l'information de la Confédération ? Dans quelle mesure le secteur privé est-il responsable de l'augmentation de la cyber-résilience ?

Ces questions importantes et d'autres ont été abordées lors de la discussion de groupe animée par **Fredy Müller**, directeur du FORUM SÉCURITÉ SUISSE. Il a accueilli le public et expliqué que la discussion visait à favoriser la compréhension des récents changements dans l'architecture de la cybersécurité en Suisse.

Un record inquiétant

Après cette brève introduction, Fredy Müller a introduit le sujet en rappelant qu'au début du mois de novembre de l'année dernière, l'organisation de Florian Schütz, alors le Centre national de cybersécurité NCSC, avait enregistré 2000 cyberincidents signalés en une semaine, ce qui constituait un nouveau record. Il a également souligné qu'il ne s'agissait que des incidents déclarés et qu'il existait un grand nombre de cas non déclarés. Il s'est ensuite tourné vers les deux politiciens pour leur demander s'ils étaient surpris par ce chiffre.

Maja Riniker a déclaré qu'elle n'était guère étonnée, mais qu'elle appréciait beaucoup l'existence de l'Office fédéral de la cybersécurité, auquel on peut s'adresser d'une part pour toute question relative à la cybersécurité et qui assume d'autre part la fonction d'un service central d'alerte. La Commission de la politique de sécurité est également régulièrement confrontée au thème de la cybersécurité, ainsi qu'à la sécurité dans son ensemble. La réalité est malheureusement amère : les développements géopolitiques actuels font que l'on ne s'étonne plus aussi rapidement.

Gerhard Andrey n'est pas non plus surpris par ce chiffre, mais il estime qu'il y a toujours deux messages et que le tout doit être considéré de manière plus nuancée. D'une part, le nombre de cyber-incidents augmente effectivement de manière constante, mais d'autre part, ils sont également signalés de manière de plus en plus conséquente. En tant qu'optimiste, il a l'impression que certaines choses vont s'améliorer. Par exemple, certains projets de loi ont déjà été mis en place et sont désormais en vigueur. Cependant, il doit lui aussi reconnaître qu'il existe encore des domaines où la situation est épouvantable. Il y a donc à la fois de l'espoir et de la désillusion.

Pas de révolution mais une évolution

Suite à ces deux réponses, l'animateur a constaté que d'importants changements institutionnels dans le domaine de la cybersécurité étaient entrés en vigueur au début de l'année 2024. Il a ensuite demandé au nouveau directeur de l'Office fédéral de la cybersécurité, **Florian Schütz**, pourquoi ce nouvel office était nécessaire et ce que sa création allait améliorer.

Ce dernier a rétorqué que le Conseil fédéral avait discuté en août 2022 de la forme d'organisation du NCSC de l'époque et était arrivé à la conclusion qu'il était judicieux de créer un nouvel office fédéral. En effet, le NCSC était un peu en marge du paysage, les employés étaient subordonnés au Secrétariat général du DFF, mais Florian Schütz, en tant que délégué à la cybersécurité de l'époque, devait directement rendre des comptes au Conseil fédéral, ce qui a créé certaines zones de tension. Différentes formes d'organisation ont donc été discutées. La forme d'organisation choisie permettait au Conseil fédéral de piloter directement l'office et l'ancien NCSC avait en outre plus de poids en tant qu'office fédéral. Pour ces raisons, le NCSC a été transformé en un office fédéral de la cybersécurité au sein du DDPS le 1.1.2024, afin de mieux exploiter les synergies potentielles et existantes. Les premières synergies se sont déjà manifestées au début de l'année et d'autres seront analysées au cours de l'année en cours. A la question de savoir ce qui devrait être amélioré, Florian Schütz a répondu qu'il ne s'agissait pas d'une révolution mais d'une évolution du BACS. Les travaux existants seront poursuivis, mais les processus devront être optimisés afin d'être plus rapides et plus efficaces. Parallèlement, il faut analyser avec les cantons et les communes, à tous les niveaux de l'État, quelles prestations supplémentaires la Confédération devrait fournir. Le BACS recevra également des demandes de l'économie et de la population, mais celles-ci devront être définies par le biais de la politique et traitées en conséquence.

Fredy Müller s'est ensuite adressé à Maja Riniker pour savoir si l'on avait été informé de ce changement structurel au sein de la Commission de la politique de sécurité.

Maja Riniker pense que la création de l'office fédéral a permis de traiter correctement l'importance du sujet. En effet, la cybersécurité n'est pas la seule à être traitée de manière isolée, puisque le nouveau Secrétariat d'Etat à la politique de sécurité s'occupe également de la politique de sécurité générale. L'importance a donc été reconnue et les ressources correctement réparties. En outre, la consolidation sous un nouveau titre entraîne une amélioration et une modification de la perception internationale, ce qui est d'une importance capitale pour les thèmes qui ne s'arrêtent pas à une frontière cantonale ou nationale, car l'échange et la visibilité sont essentiels.

Manque de clarté dans les domaines de responsabilité des nouvelles unités administratives

Le modérateur a résumé que le Secrétariat d'Etat à la politique de sécurité, le SEPOS, et l'Office fédéral de la cybersécurité, le BACS, ont été créés et qu'une architecture de sécurité adaptée a ainsi été mise en place dans le domaine cybernétique. Il a ensuite demandé à **Gerhard Andrey quelle** était l'importance de la création de ces structures, à la fois comme signe vers l'intérieur et vers l'extérieur.

Ce dernier a accueilli très favorablement la création de l'office fédéral et s'est souvenu de l'annonce faite à ce sujet par le conseiller fédéral de l'époque, Ueli Mauer. Il a également mentionné qu'avant l'annonce officielle, il avait déjà posé la question au Parlement de savoir si un tel office devait être créé. Mais à l'époque, le Conseil fédéral aurait réagi avec beaucoup de réserve. Même si le BACS existait maintenant, il y aurait toujours de gros points d'interrogation, notamment en ce qui concerne l'organisation. En effet, à peine le BACS a-t-il été créé qu'un nouveau secrétariat d'État est déjà créé, avec lequel il y a des chevauchements d'activités. Il est donc nécessaire d'y voir plus clair. Il a ajouté qu'en général, il fallait que quelque chose d'ancien fonctionne correctement avant de commencer quelque chose de nouveau. En effet, actuellement, le Conseil fédéral est encore occupé par la mise en œuvre et l'organisation de l'office fédéral, bien que celui-ci soit déjà opérationnel.

L'animateur a ensuite glissé à **Florian Schütz la** question de savoir s'il n'y avait pas de conflits de compétences ou une confusion des informations entre le SEPOS, le commandement Cyber et le BACS, et comment ce nœud gordien pouvait être résolu.

L'interlocuteur a répondu qu'à son avis, il ne s'agissait pas d'un nœud gordien. Il est d'avis qu'au cours des quatre dernières années et demie, la collaboration avec l'armée a été beaucoup plus claire. En effet, l'armée est responsable des tâches de l'armée, tandis que les tâches civiles incombent aux autorités policières au niveau cantonal ou fédéral, tout en collaborant étroitement et en se soutenant mutuellement. Le Secrétariat d'Etat se charge en premier lieu des questions stratégiques de la politique de sécurité, dont le cyber n'est qu'une partie. Il y a certains chevauchements que l'on veut et doit délimiter à l'avenir. Le transfert du service spécialisé dans la sécurité de l'information et l'intégration de la sécurité de l'entreprise et des contrôles de sécurité des personnes au sein du SEPOS ont permis d'y créer un pôle de sécurité interne. Le BACS peut ainsi se concentrer davantage sur ses tâches

principales, à savoir la mise en œuvre de la cyberstratégie nationale et l'amélioration de la protection de l'économie, de l'éducation, de la société et des autorités. En tant qu'autorité, la Confédération reste un utilisateur important des services du BACS et profite d'une protection directe - préventive et réactive. Enfin, Florian Schütz a ajouté qu'il existe toujours différents modèles permettant d'organiser une telle collaboration. C'est pourquoi, selon lui, il faut maintenant continuer à élaborer le modèle actuel et vérifier à la fin de l'année si son fonctionnement est judicieux.

L'animateur a piqué du nez et a voulu savoir ce qu'était le Bureau de la sécurité de l'information et ce que signifiait son implantation au sein du SEPOS.

Florian Schütz a répondu qu'avant l'entrée en vigueur de la LSI, les instruments étaient limités au niveau fédéral. A l'époque, il existait deux organes différents, d'une part les directives de sécurité informatique au NCSC et d'autre part les directives de protection des informations au Secrétariat général du DDPS. Cette séparation était difficile à mettre en œuvre et les deux ne pouvaient agir que sur la Confédération. Avec la nouvelle LSI, les prescriptions s'appliqueront à tous ceux qui traitent des données de la Confédération. La Confédération obtient donc par exemple aussi des droits d'audit qui ne pouvaient pas être exercés auparavant. La gestion de la chaîne d'approvisionnement par des tiers en est un exemple.

Le réseau national de sécurité - un cas unique

Fredy Müller est passé à un nouveau sujet et a demandé **à Martin von Muralt**, le délégué du Réseau national de sécurité (RNS), d'expliquer au public quel était son domaine d'activité exact.

Il a tout d'abord précisé qu'il n'était pas le délégué du Conseil fédéral, mais de la Confédération et des cantons. C'est important pour comprendre la nature exacte de sa mission. L'ASJ est en effet un cas unique qui n'a de sens que dans un Etat fédéral. Le SVS est responsable des bons services au sein de la Suisse, entre les trois niveaux de l'Etat dans le domaine de la sécurité. Le cyber joue un rôle important dans ce domaine, mais ce n'est pas le seul. La force du SVS réside dans le fait qu'il est paritaire et que les communes sont également impliquées dans les thèmes liés à la sécurité. L'association est agile et se saisit des thèmes qui sont à la fois actuels et d'importance stratégique et politique à un moment donné. Par exemple, il y a dix ans, la cybercriminalité n'était pas encore un thème du SVS, mais elle est devenue entre-temps un élément central qui restera important à l'avenir. Le SVS est un mécanisme qui veille à ce que des conditions-cadres correctes soient créées au sein de la Confédération et à ce que la Confédération, les cantons et les communes discutent entre eux des thèmes liés à la sécurité. On recherche le consensus et les domaines où il est nécessaire d'agir et on élabore des catalogues de mesures et des stratégies à cet effet. Le SVS est donc aujourd'hui actif aussi bien dans le domaine de l'extrémisme et du radicalisme que dans celui de la traite des êtres humains, du cyberespace et de la gestion de crise, ainsi que dans d'autres thèmes futurs qui sont déjà dans le pipeline. L'alliance est une construction qui permet le dialogue entre les niveaux étatiques dans le domaine de la sécurité de manière agile et thématique. Les thèmes sont aujourd'hui différents de ceux qu'ils seront dans cinq à dix ans. Dans le domaine cybernétique, le SVS a aujourd'hui deux rôles. Le premier est apparu il y a environ cinq ans, lorsque la cyberstratégie nationale a été introduite et qu'il a fallu adapter les stratégies cantonales existantes. L'élaboration de la cyberstratégie nationale NCS par le NCSC s'est faite en étroite collaboration avec les cantons. Pour la mise en œuvre de la NCS, il est prévu de créer un groupe d'experts en cybersécurité avec tous les partenaires concernés au niveau fédéral, cantonal et communal, de sorte que les questions de l'autonomisation, de la résilience et de la gestion des incidents puissent être abordées et traitées ensemble.

Fredy Müller s'est montré visiblement étonné par l'ampleur des tâches de l'ASJ et a voulu savoir de **Martin von Muralt combien** de collaborateurs il avait à sa disposition et à combien il pouvait faire appel pour l'aider dans les groupes de travail.

Celui-ci a souligné une nouvelle fois que la SVS était un mécanisme ou un label qui impliquait la parité et la neutralité. En conséquence, elle n'a pas de ressources propres ni de pouvoir de décision, à l'exception de son propre secrétariat. C'est pourquoi le personnel de l'ASJ est plutôt réduit, avec seulement 5,4 FTE (postes à temps plein). Il y a cependant six membres au niveau fédéral et six autres au niveau cantonal, qui sont finalement responsables de la mise en œuvre. La SVS n'est responsable que de la coordination, qui permet d'identifier les besoins d'action et les catalogues de mesures et d'élaborer des stratégies. La mise en œuvre incombe ensuite aux partenaires respectifs. L'ASPO peut éventuellement effectuer un suivi stratégique a posteriori et accompagner le tout. Mais elle est rattachée à la stratégie et à la politique et ne peut donc pas recourir directement aux ressources en personnel.

Coordination entre les différents niveaux de gouvernement

L'animateur voulait en savoir plus sur la coordination entre les trois niveaux de gouvernement et a demandé quelle serait la réaction en cas de cyberincident explosif.

Florian Schütz a estimé que l'approche d'un incident était relativement simple. Les incidents attirent l'attention parce qu'ils sont passionnants à écouter et qu'ils ont une certaine intensité dramatique. Le traitement est complexe et la recherche de points faibles peut s'avérer difficile. Mais il est bien plus difficile de construire des systèmes sûrs. Nous devrions nous concentrer davantage sur la création de systèmes qui préviennent les incidents. C'est l'aspect le plus intéressant. En ce qui concerne une cyberattaque contre un canton, il a répondu que si un seul canton était touché, il agirait lui-même. S'il n'est pas en mesure de le faire, il s'adresse au BACS et reçoit un soutien approprié. La situation se complique lorsque plusieurs cantons sont concernés et qu'il s'agit d'incidents ayant un impact important, comme ce fut le cas pour Xplain. A l'époque, de nombreux cantons et entreprises avaient

été touchés. La coordination dans cet incident n'a pas encore fonctionné de manière optimale. Il est donc apparu clairement qu'il manquait un certain nombre d'instruments, par exemple sur la manière de classer et de coordonner les incidents de manière identique à tous les niveaux étatiques et sur la manière de traiter les questions stratégiques. C'est pourquoi le BACS collabore avec la CDC, la CCDJP, les différents services de la Confédération, le SVS mais aussi le monde politique, afin d'uniformiser les processus sans porter atteinte à l'autonomie du système fédéral.

Fredy Müller a ensuite demandé comment se déroulait une telle collaboration, s'il y avait un échange régulier.

Schütz a ensuite expliqué qu'il fallait abandonner l'idée d'une pièce dans laquelle des réunions sur la situation actuelle auraient lieu régulièrement toutes les quelques heures. Cela ne fonctionne pas dans la pratique, en particulier pour la gestion des incidents. Tout se passe aujourd'hui par téléphone, par des services de messagerie cryptés et par des plateformes numériques, et le BACS exploite également un espace numérique pour les infrastructures critiques et les cantons. En outre, des réunions d'harmonisation sont organisées ponctuellement. Les organes existant en Suisse, également au niveau cantonal, sont importants pour la préparation.

Fredy Müller a ensuite demandé à **Martin von Muralt** ce qu'il en était de la conscience d'une cyber-résilience accrue face aux cyberattaques dans les cantons et les communes.

Il est d'avis que ce dernier devient de plus en plus important. Il a fait une remarque complémentaire concernant la collaboration des organes de sécurité suisses, à savoir que l'échange dans le domaine de la cybersécurité entre la Confédération et les cantons devrait se faire via les plateformes de la SVS. Cela a été rendu possible récemment. En effet, cela fait des années qu'il a demandé que Florian Schütz devienne membre de la plateforme opérationnelle du SVS, ce qui a été accepté. Nous nous trouvons maintenant dans une phase pilote. Les communes sont également représentées au sein de la SVS, comme le montre l'obligation d'annoncer les incidents sur les infrastructures critiques. A ce sujet, on a demandé aux communes si elles se sentaient concernées et si l'obligation d'annoncer était perçue différemment selon la taille de la commune. Toutes les communes ont cependant salué l'égalité de traitement. Cela montre que les petites communes sont également conscientes des cyberrisques. Il a été agréablement surpris de constater que les petites communes sans capacités informatiques propres, c'est-à-dire les communes qui ont externalisé leur informatique à des entreprises du secteur privé, sont conscientes du risque. Les défis à relever dans un État fédéral aux structures différentes restaient toutefois importants. Zurich ne peut en effet pas être assimilée et comparée à une petite commune.

Maja Rinker a ajouté que cette habilitation des personnes, des entreprises ou des communes, le niveau le plus bas de l'État, était très importante. Des attaques ou des abus peuvent toujours survenir et il est donc essentiel de savoir comment les gérer. Un exemple tiré de la Commission de la politique de sécurité illustre cette situation. Il s'agissait du fait que les demandes d'asile peuvent également être déposées auprès des communes, qui sont organisées différemment. Cependant, toutes les communes sont confrontées à des demandes faites avec un passeport falsifié. Un appareil spécial est nécessaire pour le détecter, le point décisif n'étant pas le prix, mais la disponibilité de ces appareils et la formation du personnel. Elle estime donc que la SVS remplit une mission très précieuse. Elle partage également l'avis de Florian Schütz selon lequel le système devrait permettre d'éviter les attaques et l'État devrait offrir une meilleure protection.

Une meilleure vue d'ensemble des cybermenaces actuelles grâce à la nouvelle obligation de notification des infrastructures critiques

Avec la révision de la nouvelle loi sur la sécurité de l'information, les exploitants d'infrastructures critiques doivent annoncer les cyberattaques qui portent atteinte au système. Fredy Müller a demandé au directeur du BACS ce que cela allait améliorer pour la collectivité.

Florian Schütz a expliqué qu'en Suisse, il est possible depuis 2004 de notifier volontairement des cyber incidents pour toutes les infrastructures critiques. Ces annonces ont augmenté, mais certaines entreprises et organisations ont pris la notification plus au sérieux que d'autres. La Confédération et le Parlement ont donc estimé qu'une obligation de déclaration était nécessaire afin d'établir la parité, étant donné que l'on dépendait de statistiques correctes. L'argent du contribuable étant investi, les statistiques doivent montrer de manière transparente les principales zones problématiques. Malheureusement, la cybercriminalité est une affaire de marketing, comme l'ont montré les attaques par déni de service de l'année dernière. Les journaux ont été subitement remplis d'experts qui faisaient la promotion de la grande attaque russe. Il s'agissait en réalité d'une attaque DDoS qui n'aurait même pas eu d'impact sur le produit intérieur brut. En fait, on n'a fait que donner du succès aux pirates, en leur offrant une plus grande plate-forme et donc une plus grande portée. Parallèlement, le piratage de Xplain a posé un grave problème. En raison de l'obligation de notification, le BACS est tenu d'aider les exploitants d'infrastructures critiques concernés en cas d'attaque. Jusqu'à présent, cela s'est fait sur une base volontaire. Cela deviendra un défi à l'avenir, car une augmentation de 30% des incidents est synonyme de travail supplémentaire. Actuellement, le BACS reçoit toutes les quarante minutes une information sur une infection par un logiciel malveillant, ce qui ne concerne pas seulement les infrastructures critiques, mais toutes les entreprises. Il est d'avis que le BACS devrait à l'avenir également proposer son aide aux infrastructures non critiques - qui ne sont pas soumises à l'obligation de notification. En ce qui concerne les infrastructures critiques, la loi définit une limite maximale quant aux personnes soumises à l'obligation de notification. Le BACS est en train d'élaborer l'ordonnance et prévoit une consultation cette année, qui définira le seuil effectif.

L'interdépendance des données

Suite à l'attaque du groupe de pirates chinois "Volt Typhoon" contre des infrastructures critiques aux Etats-Unis, le présentateur a demandé s'il existait une liste des infrastructures critiques en Suisse.

Florian Schütz a répondu par l'affirmative et a renvoyé à l'Office fédéral de la protection de la population, qui est responsable de cette liste. Il estime qu'il est plus important de se demander s'il est pertinent de ne parler que d'infrastructures critiques. Car la cybersécurité concerne toutes les entreprises. Dans le cadre de l'obligation de notification, la limitation aux infrastructures critiques est judicieuse, car il existe également une définition claire des infrastructures critiques dans la LSI. L'une des missions de l'Office fédéral de la cybersécurité consiste aujourd'hui à soutenir les infrastructures critiques en cas d'incident. Mais si une PME rencontre des difficultés, elle ne peut pas être aidée directement par le BACS, les PME sont livrées à elles-mêmes, en exagérant un peu. Cette distinction entre infrastructures critiques et non critiques est donc quelque peu problématique. De plus, environ 75 % des entreprises suisses réalisent un chiffre d'affaires inférieur à un demi-million de CHF par an. Selon la branche, il reste donc un budget de quelques milliers de francs suisses pour la cybersécurité. Cela permettrait éventuellement d'acheter une licence antivirus. S'il arrivait que toutes les pharmacies de Suisse soient victimes d'une attaque de ransomware à grande échelle exploitant une faille dans le système des pharmacies, il s'agirait d'un problème systémique, même si une seule pharmacie n'est pas nécessairement importante pour le système. Il est donc important que le BACS puisse également aider les infrastructures non critiques - lorsque cela est pertinent.

Gerhard Andrey a ajouté qu'il aimerait lui aussi remettre en question la distinction entre infrastructure critique et non critique. Dans le même temps, il a souligné le risque que certaines entreprises acceptent trop facilement une interruption de service due à une cyberattaque. Le problème de cette perspective est que, dans la plupart des cas, d'autres personnes sont également touchées. Il a pris l'exemple d'un cabinet médical dans lequel plusieurs milliers de dossiers de patients ont été dérobés, ce qui a finalement des répercussions sur les personnes concernées, car leurs données personnelles ont été détournées et pourraient encore être utilisées à mauvais escient. C'est précisément ce fait que d'autres personnes sont encore trop souvent prises à la légère à ses yeux. De tels incidents se sont également produits chez CH-Media ou à la NZZ, où une porte s'est soudainement ouverte sur une autre. Il est essentiel de tenir compte de l'importance des données dérobées et de ne pas les considérer comme quelque chose d'isolé. Comme nous l'avons déjà mentionné, il a l'impression que certaines entreprises font preuve d'une certaine négligence dans ce domaine.

Quelles sont donc les conséquences du vol de données, a demandé le présentateur à l'assemblée.

Selon **Florian Schütz,** les conséquences peuvent être très diverses. Elles vont du vol d'identité à l'amélioration du phishing, etc. Mais en règle générale, ce qui est rendu public reste public et ne peut plus être annulé. Enfin, il existe différents instruments pour lutter contre le vol de données. D'une part, les autorités de poursuite pénale devraient être habilitées à mettre hors d'état de nuire de tels groupes. Peu avant cette discussion de groupe, on a pu lire dans les informations qu'une attaque internationale contre Lockbit, avec la participation de la Suisse, avait été menée à bien. Il convient de noter ici que les autorités de poursuite pénale suisses sont actives et efficaces. D'autre part, il faut considérer le sujet dans son ensemble. Outre la poursuite directe des criminels et la confiscation de leur infrastructure, il existe d'autres instruments. Les criminels veulent gagner de l'argent. Plus on leur complique la tâche et plus on interrompt les flux financiers, moins c'est rentable pour les criminels. La Suisse est relativement active dans ce domaine, y compris dans le dialogue international, par exemple avec Singapour, dans le domaine des mécanismes de lutte contre le blanchiment d'argent et de financement du terrorisme pour les VSOP et les cryptomonnaies. La Suisse est également représentée dans des organes internationaux, par exemple la Counter Ransomware Initiative, initiée par les États-Unis et regroupant environ 50 États. De tels cas doivent être examinés avec précision et les flux financiers doivent également être suivis. Plus de 95% des cyber incidents sont de nature criminelle, ce qui est une bonne nouvelle pour tous les spectateurs, car il n'est pas nécessaire d'être le meilleur en matière de cyberdéfense, mais simplement meilleur que les autres, car les criminels choisissent toujours la voie de la moindre résistance.

Échanges entre le secteur privé et la Confédération

Fredy Müller s'est alors adressé au représentant de l'économie privée dans le panel, **Tobias Schoch**, et a voulu savoir si une compagnie d'assurance comme AXA faisait également partie de l'infrastructure critique.

Celui-ci a confirmé qu'AXA était une infrastructure critique. Comme Florian Schütz l'a déjà mentionné, il existe une définition des infrastructures critiques et les assurances en font partie. C'est un secteur qui a besoin d'une protection étendue. AXA elle-même est concernée et donc fortement réglementée par la FINMA. C'est pourquoi nous avons des exigences claires qui doivent être remplies.

Le modérateur a ensuite demandé à **Tobias Schoch** s'il existait une sorte d'organe ou d'instance permettant un échange entre le secteur privé et la Confédération.

Selon lui, l'échange et la collaboration avec la Confédération constituent aujourd'hui un élément clé. Il a 20 ans d'expérience dans le domaine de la sécurité informatique et a donc pu observer qu'à l'époque, la situation était très différente de celle d'aujourd'hui. Le sujet a pris de l'ampleur et aujourd'hui, cette possibilité de collaboration est de plus en plus utilisée. Un exemple illustratif est l'appel hebdomadaire du BACS le mercredi matin, où les exploitants d'infrastructures critiques peuvent se connecter et être informés pendant environ un quart d'heure des dernières attaques et des entreprises concernées. Ces appels sont également très précieux pour AXA, car il s'agit d'informations que l'on n'avait pas auparavant, et surtout pas à la vitesse à laquelle on les trouve aujourd'hui. A cet égard, la numérisation a fortement contribué à rendre possible un tel échange.

Fredy Müller a demandé à **Florian Schütz** quelles seraient les réactions à cette offre.

Celui-ci a répondu que les réactions étaient très positives, mais qu'il avait l'impression qu'il existait même un intérêt largement partagé pour davantage de possibilités d'échange. En plus de ces appels, les personnes souhaitent principalement des informations qui peuvent être consultées de manière asynchrone. Le BACS travaille déjà sur ce point et espère pouvoir répondre à ces souhaits le plus rapidement possible.

Fredy Müller s'est alors tourné une nouvelle fois vers le secteur privé et a voulu savoir comment une grande entreprise comme AXA gère les cyberattaques.

Tobias Schoch ne voit pas AXA dans une position particulière, ils sont confrontés aux mêmes problèmes que d'autres grandes entreprises. AXA a peut-être l'avantage d'avoir identifié le problème très tôt. Il a commencé à travailler chez AXA il y a cinq ans et était auparavant dans le secteur bancaire. Dans ce secteur, on investit massivement dans la sécurité informatique. Dans le cas d'AXA, le siège principal se trouve à Paris et des exigences claires sont envoyées de là à la succursale en Suisse. Il n'y a pas beaucoup de marge de négociation, car en fin de compte, il s'agit toujours de protéger l'ensemble d'AXA dans le monde entier. Son équipe d'environ 30 personnes est toutefois responsable de la Suisse. Parmi les quelque 150'000 collaborateurs dans le monde, une partie se concentre sur la sécurité et la défense contre les cyberattaques. Il existe différentes attaques, chaque "ping" n'est pas considéré comme tel. Il y a bien sûr aussi les attaques internes ou les incidents, lorsque des données sortent par erreur alors qu'elles ne devraient pas. Dans ce cas, c'est plutôt la protection des données qui joue un rôle.

Un appel à la responsabilité individuelle des PME

L'animateur a poursuivi cette réflexion en faisant référence à l'affirmation de Florian Schütz selon laquelle 75% des entreprises suisses ont un chiffre d'affaires annuel inférieur à 500 000 CHF et a demandé aux politiciens si cette réalité ne les inquiétait pas.

Gerhard Andrey répond par une analogie imagée. De nombreuses PME laissent leur porte ouverte pendant le week-end. Il faut faire appel à ces entreprises pour qu'elles prennent leurs responsabilités. Il augmenterait la pression sur ces points faibles, car ils concernent potentiellement d'autres acteurs. Dans son entreprise également, il a pu constater des cas où des fournisseurs de prestations ont eu des problèmes, ce qui a eu des conséquences négatives pour son entreprise. Par le passé, il a envoyé 130 lettres recommandées sur le thème "Fermez donc une fois la porte". Ce sont des bases et chacun est en principe responsable de sa propre sécurité. Il lui manque ce delta ou la conscience que d'autres pourraient aussi être concernés et que l'on devrait soi-même être plus prudent. A cet égard, la politique doit être plus dure. C'est pourquoi il voit une solution dans la responsabilité des organes. En tant que conseil d'administration, par exemple, on a des tâches non délégables, comme la responsabilité de s'assurer qu'il existe une gouvernance financière digne de ce nom. Il est également d'avis qu'au 21e siècle, la gouvernance des données fait partie des tâches non délégables. Il est clair que chacun est responsable de sa propre sécurité, mais aussi de la chaîne d'approvisionnement, des clients et des clientes, et que quelque chose doit encore être fait dans ce domaine.

Fredy Müller s'est adressé à Maja Riniker pour lui demander si de telles propositions étaient également discutées au sein de la CPS-N, la Commission de la politique de sécurité du Conseil national. Il voulait également savoir quel était l'état d'esprit qui y régnait et si tout relevait de la responsabilité propre des PME en cas de fuite de données par erreur.

Maja Riniker a posé la question rhétorique de savoir quelle était la tâche de la politique. Selon Riniker, celle-ci est en premier lieu responsable de la sécurité extérieure, où l'on discute de l'armée, mais aussi de la sécurité intérieure, qui comporte des tâches importantes. Il s'agit du blanchiment d'argent, de la criminalité, de la police fédérale, etc. Elle est d'avis que chaque entrepreneur est responsable des

premières étapes et qu'il doit également assumer les risques. Riniker, en tant que membre du PLR et soutien de l'entrepreneuriat, admire chaque entrepreneur, mais l'État n'est pas responsable d'assurer et de soutenir toutes les personnes et entreprises. La commission de politique de sécurité ne discuterait pas à cette hauteur, ce ne serait pas non plus adéquat selon elle. Elle reconnaît néanmoins qu'il s'agit d'une discussion pertinente, notamment pour déterminer à partir de quelle taille une entreprise a besoin d'une cyberassurance. L'étape suivante consisterait à déterminer qui doit la contrôler. "Si l'entrepreneur n'y veille pas, quelles sont les sanctions ?", s'est demandé Maja Riniker. Il y aurait des amendes et des poursuites pénales. La Suisse ne serait pas encore très avancée dans la répression des très graves délits. Il serait possible d'investir davantage de moyens dans des poursuites pénales correctes. Mais tant que des moyens supplémentaires n'auront pas été alloués, Riniker estime qu'il n'est pas juste de poursuivre chaque "PME" si elle n'a pas souscrit la bonne cyberassurance.

Comme Martin von Muralt est souvent en contact avec les cantons et les communes, Fredy Müller l'interpelle sur le thème de la responsabilité individuelle et des PME.

Martin von Muralt ne s'est pas exprimé sur les PME, mais a fait référence à la responsabilité individuelle, au critère de subsidiarité, qui font partie de l'ADN de la Suisse. Les communes, les cantons et la population sont responsables d'eux-mêmes. La Confédération ne peut pas venir à la rescousse à chaque attaque. Il faut veiller à ce que les cantons et les communes soient autonomes. Ils le sont déjà en grande partie. Mais les communes sont comme des PME, elles n'ont pas des moyens illimités. C'est pourquoi il serait judicieux de réfléchir à la manière d'utiliser les synergies et les meilleures pratiques, de favoriser les échanges entre les cantons, que ce soit pour l'autonomisation ou la gestion des incidents. Monsieur von Muralt était d'accord avec ce qu'avait dit Maja Riniker, à savoir que la responsabilité individuelle s'applique également aux PME au niveau de l'Etat. Des questions subsistaient : quand une commune et un canton peuvent-ils espérer un soutien de la Confédération ? Quand le soutien de la BACS interviendra-t-il ? Ce sont des choses qui, selon lui, nécessitent encore d'être clarifiées.

Florian Schütz a encore évoqué la perspective de la sécurité et l'économie. En fin de compte, il s'agit de savoir "si je peux acheter une prestation sur le marché et si je sais ce que j'ai acheté". Le cybermarché est un marché bruyant et on ne voit souvent pas ce qui est réellement acheté sur le marché. Le BACS traite des cas où les personnes concernées n'auraient pas subi d'incident si elles avaient été chez un autre fournisseur de services Internet. Elles ont ainsi subi un préjudice de plusieurs dizaines de millions d'euros. Le BACS ne peut toutefois pas donner d'estimation sur les différents fournisseurs, car cela fausserait la concurrence. En même temps, il serait de la responsabilité des entrepreneurs de se poser la question "qu'est-ce que j'obtiens de ce contrat et qu'est-ce que j'autorise sur le marché en général" ? Quel est le rôle des magazines de protection des consommateurs dans ce contexte ? Si l'on achète par exemple un ours en peluche contenant un colorant toxique et que l'on s'en aperçoit, celui-ci doit être retiré du marché. Le cas échéant, des dommages et intérêts seraient réclamés. En revanche, si un produit informatique est vendu sur le marché alors qu'il est truffé de points faibles et que des données sont exportées à l'étranger, cela n'aurait aucune conséquence. Le fabricant pourrait continuer à vendre le produit. M. Schütz n'est pas d'avis qu'il faille procéder ici avec la massue réglementaire, ni que la réglementation soit toujours le bon instrument. Mais il faut des incitations économiques, des produits de bonne qualité et un processus propre pour aborder ces questions. Chaque produit a des points faibles lorsqu'il est mis sur le marché, mais ceux-ci doivent être pris au sérieux et les consommateurs doivent réaliser pour quoi ils ont dépensé leur argent.

Tobias Schoch a poursuivi en louant l'exemple de la comparaison avec d'autres entreprises. AXA fait de même. L'objectif est d'être dans le top 25% dans le domaine des banques et des assurances. C'est un bon niveau dans ce domaine. Le conseil d'administration a également approuvé cet objectif, de sorte qu'il est possible d'investir suffisamment pour atteindre les 25%. AXA sera comparée à 37 banques et assurances et fera l'objet d'une évaluation. Dans le domaine des PME, il est très important de savoir dans quelle mesure le management est conscient du sujet. Souvent, cette prise de conscience est étonnamment faible. Et il ne faut alors pas longtemps pour que quelque chose se produise. M. Schoch a été choqué de voir à quel point on fait souvent preuve de négligence dans ce domaine.

Sensibilisation et démystification

Fredy Müller a évoqué avec Maja Riniker l'entretien préliminaire, au cours duquel elle avait parlé de sensibilisation et de démystification, ainsi que de ses filles, qui étaient déjà sensibilisées à ce sujet à l'école.

Maja Riniker était convaincue que l'on ne devrait plus avoir honte lorsqu'une erreur est commise ou qu'une attaque a eu lieu. Dans de tels cas, l'Office fédéral de la cybersécurité offre un point de contact. Elle était d'avis que l'on devrait être confronté très tôt à de tels sujets. Ses deux filles adolescentes sont déjà sensibilisées à l'école. Elle a également parlé d'une bonne amie, CEO d'une grande entreprise, qui a subi une cyber-attaque l'année dernière. Cette amie en a parlé dans les médias et a dit que sans une bonne assurance qui avait immédiatement mis des liquidités à disposition, elle n'aurait pas pu se procurer le nouveau matériel informatique dans les trois jours. Il faut pouvoir en parler et ne plus en avoir honte. Il faut déstigmatiser. Maja Riniker est d'avis que les attaques font partie du quotidien et que l'on devrait pouvoir en tirer des leçons.

Gerhard Andrey a clarifié ce point de vue. Il a fait allusion à un panel de la Journée de l'industrie 2023, où ils étaient tous deux représentés. Il a été impressionné par la façon dont certains CEO s'y sont tenus et ont raconté comment ils avaient été victimes de telles attaques, ce qui concernait leur responsabilité personnelle et où une éventuelle négligence s'était produite. Cette démystification de tels incidents est également essentielle aux yeux d'Andrey. Il a ensuite évoqué la loi sur l'information et la sécurité (LSI), qu'il aurait souhaité voir élargie. Selon lui, les vulnérabilités qui n'étaient pas encore connues auraient également dû être signalées à l'ancien NCSC (Centre national de cybersécurité), aujourd'hui le BACS. Le Conseil national aurait pu être entendu au début, mais l'industrie n'était pas encore prête.

Fredy Müller a parlé à **Gerhard Andrey** du whistle blowing.

Andrey a nié avoir parlé de whistle blowing, mais il aurait plutôt pensé à Heartbleed ou Lockbit (deux vulnérabilités concrètes). Si une faille apparaissait dans une infrastructure critique et que quelqu'un s'en apercevait, il aurait souhaité qu'il y ait une obligation de notification au BACS. Mais on n'en était pas encore là. Andrey était certain que ce n'était qu'une question de temps avant que cette obligation n'arrive. A la fin de la journée, le constat "il y a le feu chez moi, alors il pourrait y avoir le feu chez toi aussi" serait très efficace. Ce raisonnement devrait être l'objectif.

Fredy Müller s'est adressé à Florian Schütz et lui a demandé si les PME pouvaient également se connecter aux appels hebdomadaires.

Florian Schütz a nié que les entreprises non critiques puissent participer. Pour l'instant, les appels se limitent aux infrastructures critiques. Mais il y a bien sûr aussi des PME qui sont considérées comme des infrastructures critiques. Il est prévu de les ouvrir, mais il faut se demander si la forme actuelle a encore un sens. Il ne sert à rien, par exemple, qu'une commune soit informée des grands vecteurs d'attaque internationaux si elle ne peut pas traiter l'information. Il faut gérer cela en fonction des niveaux et des besoins.

Fredy Müller a donné la parole à **Tobias Schoch**. AXA est un groupe mondial qui investit beaucoup. Des investissements élevés coûtent moins cher à AXA que si elle devait payer une rançon. La Suisse est un pays très innovant. C'est pourquoi la sensibilisation en Suisse est probablement plus élevée en comparaison internationale. Fredy Müller voulait savoir si AXA Suisse était plus touchée par les attaques que d'autres pays.

Selon Schoch, ce n'est pas le cas. La Suisse est par exemple sous les feux de la rampe lors de certains événements, comme le WEF, où des attaques DDoS ont eu lieu. Si l'on observe l'ordre mondial actuel, on constate une forte augmentation des attaques dans le domaine cybernétique, notamment en raison de la guerre en Ukraine, qui dure depuis deux ans. A cet égard, la Suisse est également dans la ligne de mire, mais pas plus que d'autres pays. Schoch voit un préjugé dans le fait que les agresseurs supposent qu'il y a beaucoup d'argent à extorquer en Suisse. En tant que plus grande assurance, AXA est probablement plus visée que les petites assurances en raison de la quantité d'argent.

Exercice de sécurité interconnecté 2025

Fredy Müller a conclu en demandant à Martin von Muralt de partager quelques informations sur le prochain exercice de sécurité interconnecté "exercice de conduite stratégique 25" et a souhaité savoir si la sensibilisation et la prévention contre de telles attaques étaient exercées.

Martin von Muralt a confirmé qu'il s'agissait de sensibilisation, mais pas de prévention, car il s'agit de gestion de crise et la prévention se fait en amont. Il s'agit d'un exercice intégré, car les exercices de sécurité coordonnés et les exercices de conduite stratégique sont réunis. Pour la première fois en Suisse, le Conseil fédéral s'entraînera avec les conseillers cantonaux et d'Etat, les infrastructures critiques et les milieux scientifiques. Le thème est connu et relativement large : "menace hybride sur

la Suisse". Il y a trois objectifs principaux pour cet exercice. Premièrement, il s'agit de vérifier comment se déroule l'entrée en crise, deuxièmement la capacité d'endurance, et troisièmement la coordination de la communication. La cybersécurité, la résilience, la gestion des incidents, mais aussi la cyberguerre font partie de la cybersécurité. Cette dernière, en rapport avec la communication, est souvent due à la désinformation. En réponse à cela, il faut se demander "comment maîtriser, comment réagir, comment se coordonner lorsque des campagnes de désinformation étrangères sont utilisées" ? C'est ce qui sera au centre de cet exercice.

Connaissances pour le public

Pour conclure, Fredy Müller a voulu savoir quels étaient les principaux enseignements pour le public dans le domaine de la cybersécurité.

Pour **Florian Schütz**, l'ensemble de la thématique dépassait le cadre de l'État et de l'économie et de la société. Il ne faut pas considérer l'attaque et la défense de manière isolée, ce serait trop réducteur. De bonnes approches et mises en œuvre stratégiques créeraient une valeur ajoutée en tenant compte des aspects sociaux et économiques.

Gerhard Andrey a approuvé et a complété par un autre aspect. Il est également membre de la commission des finances et de la sécurité. Trouver un équilibre entre les moyens à disposition et les besoins en matière de sécurité et de défense n'est pas chose aisée. Il a critiqué les montants transférés qui vont à l'armée et non à la défense. Selon lui, c'est le moyen qui reçoit l'argent et pas forcément la fin. De nombreuses choses sont liées à la sécurité, pas seulement l'armée, et il veut s'engager pour trouver un bon équilibre. Car tous les risques, qui sont déjà douloureux aujourd'hui et qui augmenteront encore à l'avenir, ne peuvent pas être maîtrisés avec de la tôle, de l'acier et des canons. Et c'est là qu'il faudrait veiller à ce que l'équilibre ne soit pas rompu et que l'on ne tombe pas dans le militarisme.

Selon **Tobias Schoch**, il n'est pas si difficile pour l'économie privée de maintenir la protection immédiatement nécessaire. L'authentification multifactorielle, le cryptage et les sauvegardes immuables pour les attaques de ransomware devraient être intégrés. Il s'agit d'éléments clés qu'il faut mettre en œuvre. Il est d'avis que les PME sont également bien positionnées avec ces éléments clés. Cela n'offre pas une protection à 100%, mais c'est un pas en avant. Si l'on investissait un peu dans ce domaine, la Suisse dans son ensemble se développerait.

Martin von Muralt a évoqué la complexité de l'ensemble du sujet. Mais cette complexité existe bel et bien. Il y a la cyberdéfense, la poursuite pénale et la sécurité. De plus, la responsabilité est répartie entre les trois niveaux de l'Etat, ce qui augmente en même temps le besoin de coordination. Mais cela présente aussi des avantages. Grâce à ce système fédéraliste, de nouvelles idées et de petits laboratoires voient le jour partout. Cela a un caractère créatif et pourrait générer de bonnes idées ainsi qu'une collaboration ciblée. La deuxième chose est la proximité avec la population, qui est assurée par les cantons et les communes. Il y a ici une grande diversité, mais aussi un risque lié aux différents fournisseurs dans le domaine cybernétique. Néanmoins, il offre également une protection, car tout n'est pas centralisé en un seul endroit et la Suisse ne peut donc pas être attaquée en un seul point. Si l'on veut parler de résilience des infrastructures, il faut pour cela coordonner les différents moyens, mettre en place des processus et des normes minimales, et c'est là que réside le défi.

Maja Riniker a conclu en se montrant rassurante. En politique, on ne dépense pas seulement de l'argent pour "l'acier et l'artillerie". Il y a un cyberbataillon, une cyber école de recrues et de la recherche dans ce domaine. Beaucoup d'argent est également investi dans ce domaine. La Commission de la politique de sécurité est consciente que le thème du cyber est très important. La commission n'est peut-être pas composée de cracks, comme le public des Swiss Cyber Security Days, mais le thème

est toujours à l'ordre du jour, que ce soit dans les échanges avec l'approvisionnement du pays, lorsque l'Office fédéral de la protection de la population, le directeur de l'Office fédéral de la cybersécurité, Monsieur Schütz, ou la directrice de fedpol, Madame della Valle, sont présents dans la commission. Le public peut aujourd'hui avoir la certitude que la politique est confrontée à ce thème et qu'elle le prend certainement au sérieux. La protection totale n'existera probablement jamais. Mais la conscience est là.

Les demandes ont montré que l'intérêt du public était grand.

Fredy Müller remercie et donne la parole au public.

Une spectatrice a demandé comment l'obligation d'annonce évoquée pouvait être exécutée ou contrôlée en cas de cyberattaques.

Florian Schütz a répondu en expliquant la procédure à suivre. Il y aura un formulaire de déclaration pour l'exécution. Selon le secteur, il existe déjà des obligations de déclaration auprès des régulateurs, comme c'est déjà le cas par exemple dans le secteur financier. On travaille actuellement à ce qu'il n'y ait si possible qu'un seul bureau de déclaration, qui distribuera la déclaration dans un deuxième temps. Cela doit se faire de manière très simple et il n'est pas nécessaire d'entrer dans les détails. On ne veut pas imposer de charge supplémentaire. Si quelque chose n'est pas déclaré et que le BACS en prend connaissance, l'entreprise peut être mise en garde et informée qu'il s'agit d'un événement à déclarer ultérieurement. Si l'organisation concernée ne s'acquitte pas de son obligation d'annonce après des rappels répétés, une amende pourrait être infligée.

Un spectateur a partagé une suggestion avec les panélistes. Il a été question dans le débat de la responsabilité des entreprises. Il voulait faire référence à l'industrie financière et au comité consultatif Brunetti du Conseil fédéral sur l'avenir de la place financière, qui a été à l'origine du système de milice et de la collaboration entre la Confédération et l'industrie. Selon lui, la Confédération ou la politique peuvent parfois être l'étincelle qui stimule ensuite le système de milice correspondant.

Gerhard Andrey peut soutenir cela. Il a évoqué une interpellation qu'il avait déposée et dans laquelle il demandait au Conseil fédéral s'il n'était pas possible d'apprendre des exemples de bonnes pratiques. Il est lui-même membre du conseil d'administration d'une banque, la Banque alternative, et connaît donc un peu le fonctionnement. Il y a des années déjà, la FINMA a publié des circulaires au ton acerbe. C'est pourquoi il y a probablement moins de cas d'attaques dans le secteur financier, mais il faut tenir compte du fait que le secteur a déjà fait très tôt des transactions virulentes. Dans son interpellation, il a demandé au Conseil fédéral s'il existait déjà des organes de surveillance dans les industries qui, à l'instar de la FINMA, pouvaient assumer la surveillance des domaines concernés. Il ne peut plus reproduire la réponse exacte du Conseil fédéral. Mais il s'est clairement prononcé en faveur d'une approche basée sur les bons exemples.

Fredy Müller a ensuite fermé la séance plénière et a remercié le public pour son attention ainsi que Jürg Walpen et Nicolas Mayencourt pour l'organisation des Swiss Cyber Security Days.