Cybermenaces - quelle est l'ampleur du danger et quel est le niveau de protection de l'État, de l'économie et de la société contre ces menaces ?

Rapport de synthèse | 11e FSS Security Talk du 17 octobre 2022, Hôtel Schweizerhof, Berne

Comment l'UE et d'autres pays européens font-ils face à la cybermenace croissante ? Comment la Suisse y fait-elle face ? Où en est la "Stratégie Cyber 2021-2024" du DDPS ? Comment nos infrastructures critiques peuvent-elles être protégées ? Comment l'État, l'économie et la société peuvent-ils se protéger contre les cybermenaces ?

Ces questions centrales et d'autres ont été discutées par des experts renommés lors du 11e FSS Security Talk à Berne. Les 120 participants intéressés ont reçu des informations de première main. La manifestation a débuté par des exposés d'introduction de **Dr Stefanie Frey** (directrice de Deutor Cyber Security Solutions GmbH, Advisory Group ENISA), du colonel EMG **Robert Flück** (projet de commandement cybernétique, armée suisse) et de **Dr Peter Friedli** (Head of Defence AWK Group). Ensuite, une table ronde passionnante a réuni **Florian Schütz** (délégué de la Confédération à la cybersécurité), Dr Jörg Mäder (conseiller national PVL/ZH, programmeur indépendant), **Alexandra Arni** (responsable ICT, Association suisse des banquiers, vice-présidente de Swiss FS-CSC) et **Dr Urs Loher** (CEO Thales Suisse SA). Le FSS Security Talk a été animé par **Fredy Müller** (directeur général du FSS).

Les experts étaient fondamentalement d'accord sur le fait que les **cybermenaces concernent tout le monde** et qu'une collaboration à tous les niveaux est donc nécessaire pour pouvoir faire face à la menace croissante. Mais l'événement a également mis en évidence le fait que nous sommes encore loin d'appréhender **la cybermenace sous toutes ses facettes et de prendre les mesures nécessaires.**

Cybermenaces - "Nous connaissons l'ennemi, mais nous ne savons pas comment le combattre et nous protéger"

Stefanie Frey, directrice générale de Deutor Cyber Security GmbH, a entamé la table ronde. Elle a d'emblée constaté que si l'on parle aujourd'hui partout de cyber, la plupart des personnes n'ont **pas une idée claire** de ce que **signifie exactement cyber**. Trois constatations en rapport avec le terme cyber doivent être soulignées : "le cyber est **un moyen pour atteindre une fin** et non une fin en soi ; Il ne faut pas parler de cyber-guerre, mais plutôt de **cyber "en guerre"**; et la cybersécurité **ne se limite pas à la sécurité informatique**, elle concerne bien d'autres composantes organisationnelles et stratégiques".

Frey a ensuite mis en lumière la tendance actuelle à **l'augmentation des cyberattaques**. Cette forte croissance constitue un problème majeur. Chaque année, les délits doublent et il faut en outre tenir compte d'un nombre très élevé de **cas non déclarés**. Les dommages pour l'économie allemande sont par exemple estimés à 223 milliards d'euros pour la seule année 2020. Selon ce rapport, neuf entreprises allemandes sur dix ont été victimes de cyber-attaques au cours de la même année. Ce préjudice n'est pas supportable !

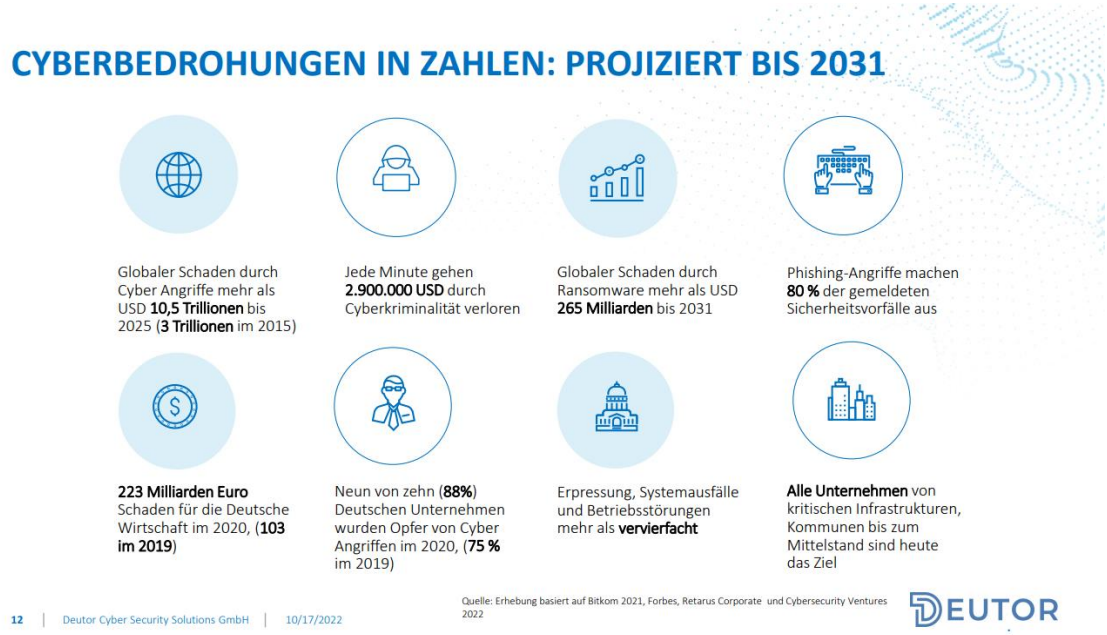

Illustration 1 : Les chiffres parlent d'eux-mêmes : les cybermenaces causent déjà d'énormes dégâts et la problématique va encore s'accentuer à l'avenir.

La question se pose de savoir pourquoi les dommages causés par la cybercriminalité sont si importants. La réponse est relativement simple: "Nous luttons contre **un ennemi que nous connaissons, mais que nous ne savons pas combattre parce que le problème n'était pas suffisamment analysé**. C'est pourquoi il serait d'abord important que nous analysions le problème et que nous **apprenions** à comprendre comment fonctionne la cybercriminalité".

Frey a également fait remarquer qu'aujourd'hui, tout est automatisé et numérisé, ce qui est toutefois **très dangereux sans une sécurité suffisante**. On peut par exemple observer que les systèmes d'armes sont mis en réseau sans penser suffisamment à la sécurité. Le cyber n'est donc pas toujours une bonne idée, mais seulement avec **une bonne équipe et suffisamment d'argent** pour pouvoir **prendre en compte tous les aspects de sécurité nécessaires**. "Il faut une numérisation avec sécurité et avec intelligence".

"...nous devons apprendre à penser comme les auteurs..."

Pour avoir une meilleure vue d'ensemble des différentes facettes de la problématique, Frey s'est ensuite penché d'un peu plus près sur les **différents types de cybermenaces** que sont la cybercriminalité, l'espionnage, la subversion et le sabotage. "La cybercriminalité rapporte **beaucoup d'argent** ! Il y a **des têtes pensantes à l'œuvre**, prêtes à tout pour de l'argent, **très motivées** et qui réussissent malheureusement trop souvent". Mais la motivation n'est pas toujours évidente. Dans un cas du secteur de la santé qu'elle a elle-même suivi, il s'agissait par exemple de la divulgation de données de patients. L'auteur n'est jamais allé chercher l'argent du chantage qu'il était promis, ce qui a donné lieu à des suppositions sur les auteurs et leurs motivations. Un autre cas qu'elle a mentionné et qui concernait à nouveau des données personnelles concernait le groupe Conti. Ce cas a montré que les entreprises **ne connaissent souvent pas assez leur propre infrastructure informatique** et ses failles de sécurité. "Mais si les malfaiteurs peuvent trouver et exploiter les points faibles existants, **nous devrions également les connaître et les éliminer.** Il n'y a **pas d'excuse** : Ce que les auteurs peuvent faire, nous le pouvons aussi" ! Dans le cas des infrastructures critiques, le sabotage via des cyberattaques est plus souvent utilisé.

©Daniel Saxer (iOf App, Defence & Security News)

Enfin, M. Frey a abordé des **problèmes** importants dans le cadre de la **lutte** contre les cybermenaces. "Nous devrions apprendre à **penser comme les auteurs**". Si une entreprise est victime d'une cyberattaque, **toute honte et tout silence sont erronés**. Mais il y a aussi souvent le problème que beaucoup de choses sont imposées du haut vers le bas, comme par exemple la législation sur la protection des données, qui compliquerait beaucoup de choses. Il serait pourtant **préférable** de développer et d'améliorer la sécurité des données dans un **processus de bas en haut**.

Pour Mme Frey, il est clair qu'une **évaluation complète des risques** devrait être la norme pour toute décision dans le domaine cybernétique. En effet, on apprend aujourd'hui dans chaque cours de formation comment une situation de menace peut être rassemblée avec une analyse des points faibles pour former une évaluation des risques qui devrait servir de **base aux décisions**. "Cela serait également **possible dans le domaine cybernétique**, mais personne ne le fait jusqu'à présent ! Nous devons apprendre à vivre cette séquence : nous analysons d'abord notre situation de **cybermenace**, puis nos vulnérabilités dans le domaine cybernétique, et cela nous permet ensemble d'identifier notre **profil de risque** et d'engager des actions ciblées pour **éliminer nos cybervulnérabilités**".

En outre, nous devrions penser comme les auteurs présumés qui envisagent une cyberattaque contre notre entreprise ou notre personne. "Cette remise en **question critique** de notre matériel et de nos logiciels informatiques permettrait déjà de gagner beaucoup". Mais pour cela, il faut du temps et de l'argent, et ne pas numériser tout et n'importe quoi sans arrêt. La cybersécurité est un défi majeur pour chaque entreprise, chaque pays et même chaque individu. Seulement, la menace est mal analysée, ce qui explique le boom de la cybercriminalité qu'il faut endiguer d'urgence. Sinon, la situation ne s'améliorera pas, bien au contraire.

"Le cybercommandement de l'Armée suisse sera opérationnel en 2024 !"

Le deuxième orateur, **le colonel EMG Robert Flück**, a donné un aperçu de la manière dont **l'Armée suisse** se prépare à faire face aux cybermenaces. Il a notamment souligné la création **du cyber bataillon 42**, qui devrait être pleinement opérationnel **dès 2024** et qui jouera un **rôle important** dans la lutte contre les cybermenaces.

Flück a tout d'abord informé sur les deux tâches fondamentales de l'armée dans le domaine cybernétique: "Afin de garantir sa capacité d'engagement et sa liberté d'action en tout temps et dans toutes les situations, l'armée est en permanence en mesure **d'identifier les cybermenaces**, de se **protéger** contre les attaques et de les **repousser**. En cas de conflit, elle est en outre en mesure de **soutenir des actions militaires par des cyberactions**".

©Daniel Saxer (iOf App, Defence & Security News)

Il s'est ensuite penché plus en détail sur la cyber-organisation de l'armée. Il faut distinguer la gestion des systèmes TIC, la détection & la défense, la situation & les opérations, l'exploitation des systèmes TIC et l'acquisition de renseignements & les effets. Concrètement, **cinq champs d'action** seront à l'avenir pris en charge par le **commandement Cyber** : Il s'agit d'une part de **l'autoprotection**, d'autre part de l'orientation du fournisseur de services informatiques vers le **commandement militaire**, de la création des conditions nécessaires à la **numérisation de l'armée**, du **combat** électronique **et des cyberopérations**, ainsi que de la capacité de coopération et de soutien au sein du **réseau national de sécurité.**

Le commandement cybernétique devrait être pleinement opérationnel à partir de 2024 et continuer à se développer par la suite. Pour cela, la **formation du personnel** joue actuellement un rôle central. Une sélection rigoureuse permet de choisir les informaticiens qui, après une formation de 42 semaines, serviront à l'avenir au sein du commandement Cyber dans différentes fonctions de milice.

Illustration 2 : "Cyber est un people's business" - En conséquence, la formation du personnel du commandement Cybers occupe une place centrale dans la lutte de l'armée contre les cybermenaces.

Il en résulte un **bénéfice mutuel**. "D'une part, les personnes concernées profitent dans leur domaine **d'engagement civil** de leur **expérience cybernétique à l'armée** et l'armée profite de forces d'intervention parfaitement formées".

Flück a ajouté que le commandement cyber ne peut bien fonctionner que s'il peut tirer profit de la **coopération** avec différents domaines, comme la cryptologie. En outre, le commandement Cyber peut

apporter **un soutien subsidiaire aux autorités civiles** lorsque les moyens de ces dernières sont épuisés ou inexistants et que les fournisseurs de prestations commerciaux ne sont pas disponibles dans la mesure requise ou en temps voulu.

M. Flück a ensuite présenté plus en détail le calendrier et la structure organisationnelle du projet de commandement Cyber. La phase d'initialisation a débuté en 2021, suivie de la conceptualisation en 2022 et de la réalisation en 2023. Enfin, l'année 2024 sera celle de **l'introduction du commandement Cyb**er, qui sera ensuite **développé en permanence**. Dans la structure organisationnelle, il faut surtout souligner l'élément "développement à long terme" et "l'élément d'engagement de la milice". Dans le contexte du cyber, il est très important de pouvoir se projeter dans l'avenir et d'identifier les tendances à temps. Le système de milice permet en outre d'intégrer des capacités cyber du monde civil dans l'armée et de les y développer, ce qui est un grand avantage aussi bien pour l'armée que pour la société.

En résumé, on peut retenir que le cyber est avant tout un **people's business** - "il faut des **personnes**, des spécialistes de l'informatique, capables de reconnaître les cybermenaces et de les gérer". En outre, il faut une **organisation appropriée au sein de l'armée**. Ce rôle est assumé par **le bataillon cybernétique 42**, en cours de constitution. Enfin, nous nous trouvons au début **d'une évolution visant à renouveler l'armée suisse et à l'orienter vers des besoins modernes.**

"La convergence croissante entre IT et OT n'est pas assez prise en compte".

©Daniel Saxer (iOf App, Defence & Security News)

Le troisième intervenant était le **Dr Peter Friedli, Head of Defence, AWK Group**, qui a ouvert l'image des **menaces informatiques connues vers les menaces dans le domaine des technologies opérationnelles**. Les menaces dans l'espace d'information ou dans l'IT ("Information Technology") sont omniprésentes et connues de tous. Le fameux phishing, c'est-à-dire le vol de mots de passe pour s'introduire dans les ordinateurs d'autres personnes et entreprises et leur causer des dommages financiers ou autres, en est un exemple. **Outre l'IT, il existe également l'OT, la "Operational Technology"**, qui comprend le **matériel et les logiciels de surveillance et de contrôle** des processus physiques, des appareils et des infrastructures. L'industrie de production, mais aussi les systèmes dans le domaine médical, la gestion du trafic, l'approvisionnement en énergie ou le traitement de l'eau dépendent de l'OT. La sécurité de l'exploitation, la disponibilité et les cycles de production sont toutefois au centre des préoccupations. Mais la **convergence croissante entre l'IT et l'OT** fait naître des risques importants pour l'OT. "Avec la numérisation croissante de l'OT, les possibilités de **cyber-attaques sont également de plus en plus grandes dans l'OT**". L'infrastructure toujours plus performante et complexe a pour conséquence que les relations deviennent de plus en plus difficiles à saisir. Par conséquent, il devient plus difficile de comprendre comment un risque à un endroit donné se conjugue à travers tout le réseau d'éléments interdépendants.

Les cas d'entreprises industrielles paralysées par des cyberattaques ou de coupures d'énergie se sont multipliés, et dans le domaine de la santé notamment, de telles cyberattaques peuvent mettre des vies en danger. "Mais que constatons-nous ? **Dans le domaine de l'OT, la sensibilisation aux risques de sécurité est souvent insuffisante**".

Illustration 3 : L'IT et l'OT convergent de plus en plus - mais beaucoup ne sont pas encore suffisamment conscients des risques qui y sont liés.

Les meilleures pratiques connues de l'IT ne sont pas utilisées dans l'OT et il manque une vision complète de **la chaîne de création de valeur de bout en bout**. Dans de nombreuses entreprises, l'IT et l'OT sont séparés, bien qu'ils convergent de plus en plus avec la numérisation croissante des processus de production. "Dans la **distribution d'énergie** en particulier, on constate qu'il **n'existe pas suffisamment de mesures de protection** contre les éventuelles cyberattaques". Il est intéressant de noter qu'il n'y a pas de corrélation entre la taille des distributeurs d'énergie et la cybermaturité, c'est-à-dire le développement des mécanismes de protection.

Heureusement, il existe aussi des bonnes pratiques dans le domaine de la sécurité OT. D'une part, la sécurité OT se base également sur une identification précoce des risques, où il convient d'analyser tous les éléments interdépendants et les risques qui y sont liés. Dans ce contexte, il est également important de bien comprendre les interfaces entre l'IT et l'OT. On y parvient également en impliquant les fournisseurs et les fabricants, en formant le personnel et en exploitant les installations avec soin.

Enfin, M. Friedli souhaitait transmettre **quatre messages clés** aux auditeurs : **les cybermenaces existent aussi dans le domaine physique** et représentent un risque important ; la numérisation croissante multiplie les vecteurs d'attaque, **l'OT et l'IT convergent** ; la **sécurité opérationnelle** n'est pas garantie pour de nombreuses infrastructures critiques et représente donc un risque important ; et la sécurité de l'OT et de la chaîne d'approvisionnement comble des lacunes de sécurité importantes - et doit toujours **impliquer les fabricants, les prestataires de services et les exploitants**. "Il y a donc encore beaucoup à faire pour améliorer la sécurité OT et la protéger contre d'éventuelles cyber-attaques".

"Pensons davantage en termes d'opportunités qu'en termes de risques" - Le panel

Après trois exposés très informatifs, la discussion du panel a suivi. Le modérateur **Fredy Müller** a commencé par diviser la discussion en trois domaines : D'une part, le **domaine militaro-civil**, d'autre part, la question de savoir comment **l'industrie** aborde la problématique et enfin, comment la **politique** se positionne par rapport à ces thèmes. Pour la question d'ouverture, il s'est adressé à **Florian Schütz, délégué fédéral à la cybersécurité**, et a voulu savoir quelles étaient ses conclusions clés dans le domaine cybernétique au cours des 20 dernières années. Pour Schütz, il est clair que la pertinence du sujet a clairement augmenté. Mais cela ne devrait étonner personne en raison de la numérisation et de la mise en réseau croissantes. Malheureusement, la société a accordé trop peu d'attention dans le débat politique et au niveau de la direction au fait qu'il s'agit d'un thème technique , dans le débat politique et au niveau de la direction,. C'est donc **une erreur de ne pas promouvoir les spécialistes de l'informatique au niveau du management**. "Vous n'avez pas non plus de directeur financier qui ne comprend rien aux finances", a ajouté Schütz pour illustrer son propos. Il existe pourtant un **grand potentiel** grâce à l'excellente formation en Suisse. **Schütz a également constaté que l'histoire se répétait** : "L'aviation et les voitures étaient également nouvelles et il fallait d'abord trouver comment s'en servir. Ici, nous pouvons toutefois dire que nous avons reconnu l'évolution. Nous allons de l'avant, nous avons certes encore un potentiel d'amélioration, mais nous ne sommes pas si mauvais que ça".

Le modérateur s'est ensuite tourné vers le **Dr Jörg Mäder, programmeur indépendant et conseiller national PVL/ZH**, pour lui demander comment cette thématique était perçue au Palais fédéral. Mäder a certes confirmé que la cyber est bien un sujet en politique, **mais pas autant qu'il serait souhaitable**. Jusqu'à présent, toute la numérisation a plutôt été considéré comme **un moyen pour atteindre une fin**. On veut certes utiliser l'informatique, mais personne ne veut vraiment réfléchir aux risques.

Alexandra Arni, responsable ICT de l'Association suisse des banquiers et vice-présidente du Swiss FS-CSC, a souligné que le secteur bancaire et financier était l'une des premières branches à reconnaître l'importance du thème Cyber. Arni a expliqué que les banques ont toujours été **une cible populaire et puissante des cyberattaques.**

Urs Loher, CEO de Thales Suisse SA, a souligné qu'il trouvait faux que tout soit présenté aujourd'hui comme plus complexe. **Autrefois aussi, il fallait protéger les informations, mais aujourd'hui, cela se passe simplement à un autre niveau**, que beaucoup de gens ne comprennent plus tout à fait : "Nous devons revenir en arrière et simplifier les choses de manière à ce que l'on comprenne à nouveau ce que l'on fait". Il s'agit de protéger les informations et de savoir qui a accès à quoi. Ce principe n'a pas changé.

Les cyberattaques contre les entreprises, une source de revenus lucrative

L'animateur Fredy Müller a mentionné que la **cybercriminalité génère aujourd'hui plus d'argent que le trafic de drogue** dans le monde. C'est pourquoi il a demandé à **Florian Schütz** s'il fallait se mettre davantage dans **la perspective des délinquants**. Schütz a répondu que les experts comprenaient déjà très bien comment les délinquants fonctionnent. Ceux-ci veulent obtenir **un rendement maximal** avec **un minimum d'efforts**. La cybercriminalité organisée est souvent **structurée comme une entreprise avec une répartition régionale ou mondiale**. Les opérations sont souvent menées depuis l'Afrique, où il y a beaucoup de talents et un petit marché du travail. En revanche, on trouve plutôt un soutien en Europe du Nord, car on y parle de nombreuses langues. On peut s'appuyer sur cette compréhension, mais il faut persévérer. Pour cela, la Suisse dispose du SRC et de la poursuite pénale. Mais, bien sûr i y aurait toutefois encore **un potentiel d'amélioration dans l'image de la situation**.

Müller s'adresse à **Jörg Mäder**, qui est **membre du comité de la Digitalen Gesellschaft**. Il y a beaucoup de bricoleurs et de développeurs, mais l'aspect sécurité est souvent oublié. **Jörg Mäder** a répondu qu'en raison de **l'Internet des objets**, les frontières physiques ne garantissent plus la sécurité, car tout peut être mis en réseau. Tant que les bricolages ne sont réalisés que pour s'amuser, le potentiel de dommages est faible. Mais s'ils doivent être utilisés pour **des systèmes de production**, cela devient plus difficile. Toutefois, le niveau de sensibilisation dans ce domaine est désormais très élevé et des normes de sécurité existent. Il suffit de s'y tenir et de suivre et **d'appliquer régulièrement les correctifs et les mises à jour.**

©Daniel Saxer (iOf App, Defence & Security News)

Les cyber-attaques dans le quotidien d'une entreprise

Cela a amené Fredy Müller à demander à **Urs Loher** comment Thales gère les cyberattaques. Celui-ci a confirmé que **Thales était presque quotidiennement attaquée.** Mais jusqu'à présent, elles s'en sont bien sorties. Pour une entreprise d'armement, la sécurité est évidemment très importante, car elle est directement liée à la crédibilité de l'entreprise. On investit beaucoup dans la sécurité opérationnelle. Mais on n'est jamais sûr à 100%. L'animateur a donc voulu savoir pourquoi les inhibitions étaient si grandes lorsqu'il s'agissait de parler de cyberattaques. Loher considère lui aussi ce phénomène comme une difficulté majeure : tout le monde voudrait régler de telles attaques en silence. Mais ce n'est pas la bonne approche. Au sein d'un groupe, l'échange fonctionne parfaitement**, mais entre les groupes et avec les autorités, il y a probablement trop peu de communication.**

Alexandra Arni a ensuite expliqué que le Swiss FS-CSC était donc en train de **mettre en place une organisation de crise qui interviendrait en cas d'attaque bancaire**. Arni a illustré l'importance de cette organisation par un exemple : "Si une banque d'importance systémique était victime d'une attaque DDoS, cela aurait une influence sur l'ensemble du trafic des paiements en Suisse et donc sur l'ensemble de l'économie nationale. Dans un tel cas, il faut une organisation de crise rigoureuse qui puisse décider, grâce aux politiques en cours d'élaboration, comment remettre les systèmes en marche le plus

rapidement possible". Dans un tel cas, les clients doivent bien entendu être informés en conséquence dès le moment où la banque ne fonctionne plus. Cette **stratégie de communication** est en train d'être élaborée au sein de la toute jeune **Swiss FS-CSC**.

« Une répartition claire des compétences est essentielle »

Des entreprises comme Zalando sont aussi régulièrement menacé par des cyberattaques, a mentionné Fredy Müller, qui a donc demandé à **Florian Schütz**, ancien responsable **chez Zalando**, comment le détaillant **en ligne** avait géré la situation. Schütz a expliqué que les attaques étaient monnaie courante chez Zalando. Les attaques ont parfois entraîné des pertes d'exploitation qui, en quelques minutes, ont causé des dommages à cinq chiffres. C'est pourquoi des **décisions rapides** et **une attribution claire des compétences** sont élémentaires dans la cyberdéfense. Schütz a ensuite souligné que les risques pouvaient également donner lieu à de **nouvelles opportunités**. Il cite comme exemple un cas où un formulaire a été mis en place sur le site web pour les clients "bloqués" afin qu'ils puissent tout de même passer leur commande. Il en a résulté une intelligence du marché et de nouvelles idées de marketing, et le coût de telles mesures de sécurité n'est plus un problème majeur.

Vu l'importance d'une gestion de crise rapide en cas de cyberattaque, Fredy Müller a demandé à **Alexandra Arni** si Swiss FS-CSC avait déjà préparé un journal de bord pour de tels cas et si les **scénarios de crise étaient activement exercés.** Arni a confirmé qu'il était élémentaire que des exercices cyber opérationnels soient organisés pour de tels cas et que tous les participants connaissent très précisément leurs rôles et agissent en conséquence.

A la question de savoir s'il existe également des mesures de prévention des cyberrisques au Palais fédéral, le conseiller national **Jörg Mäder** a expliqué que le Palais fédéral est "malheureusement" encore relativement bien équipé, car **la numérisation n'est pas encore très avancée**. En cas d'urgence, on peut recourir à des méthodes éprouvées comme les scrutateurs pour maintenir le fonctionnement du Parlement. Mais ce qui lui semble beaucoup plus important, c'est qu'il faut parler davantage de tels incidents et de tels risques. "C'est comme une maladie sexuellement transmissible : cela touche beaucoup de gens, mais ils ne savent rien les uns des autres, alors que cela pourrait justement aider. Pour pouvoir se défendre proprement contre les attaques, il faut connaître son adversaire et plus il y aura de cas connus, mieux ce sera possible". **La réalité est toutefois contraire**, a poursuivi Mäder. On ne veut pas perdre sa réputation, mais on ne veut pas non plus se retrouver seul en cas de problème.

Que faire en cas de cyber-attaque ?

Que faire en cas de cyber-attaque concrète contre une entreprise ? Faut-il appeler directement le Centre national de cybersécurité (NCSC) ou le cyberdélégué de la Confédération ? **Florian Schütz** a expliqué à ce sujet **la répartition des tâches de la Confédération**, que de nombreuses entreprises ne connaissent pas. En cas d'acte criminel, ce qui, selon les statistiques, représente environ 95% des cas, c'est la **poursuite pénale** qui est compétente. En cas de sabotage, c'est le Service de renseignement de la Confédération (**SRC**) qui prend le relais. Tout incident peut être signalé au NCSC. Le NCSC offre une première aide et informe les bons partenaires.. Schütz a ajouté que la distinction actuelle entre infrastructure critique et non critique a de moins en moins de sens. Il faudrait plutôt faire une **distinction entre l'économie et la population** et ensuite seulement classer les infrastructures en fonction de leur criticité. En principe, il recommande donc de toujours faire appel à la police en cas de délit.. Le NCSC fait ensuite toujours office de **soutien technique**. En cas de sabotage, le NCSC fournit surtout des analyses au SRC. La question suivante était de savoir comment traiter les **demandes de rançon**. Schütz a précisé qu'il **ne fallait jamais payer de rançon**, car cela ne ferait que soutenir les agissements des agresseurs. Il est toutefois important de demander de l'aide. La police peut souvent négocier avec les malfaiteurs et gagner ainsi un temps précieux. Un point était toutefois

particulièrement important pour Schütz : "En fait, nous parlons du mauvais moment. En cas d'attaque, je suis déjà en retard. On pourrait aussi construire le système de manière sûre, nous n'aurions alors pas besoin d'en discuter. Croyez-moi : vous ne traverseriez pas non plus un pont construit de manière aussi peu sûre que de nombreux systèmes informatiques". C'est pourquoi, pour Florian Schütz, l'informatique est clairement une discipline d'ingénierie. C'est là que l'accent devrait être mis et moins sur l'attaque et la défense. **Jörg Mäder** a complété et souligné qu'il était important d'avoir une stratégie pour un arrêt et un redémarrage rapides des systèmes. Une meilleure sensibilisation est nécessaire.

Systèmes de cyberdéfense spéciaux pour les armées et les États

Fredy Müller a demandé à Urs Loher quels systèmes Thales construisait pour offrir **aux Etats et aux armées la sécurité nécessaire - également dans le domaine du cloud**. Urs Loher a clairement expliqué que Thales construit des systèmes qui **rendent la vie aussi difficile que possible à un attaquant**, au cas où **il aurait déjà réussi à pénétrer dans le système**. L'objectif et la première priorité sont bien entendu d'empêcher les attaquants de pénétrer dans les systèmes. Pour cela, il faut construire des systèmes séparés et travailler avec des pare-feu ou des mécanismes de protection de nature opérationnelle, comme la limitation des droits d'accès. Des **mises à jour régulières** sont également nécessaires pour combler les éventuelles lacunes. Loher explique que la cryptographie joue en outre un rôle central. Dans ce domaine, Thales est leader dans la protection et le cryptage des données, la transmission de données et les solutions cloud pour les États ou l'OTAN. Dans ces domaines, on investit déjà dans les systèmes du futur, comme par exemple la **cryptographie quantique**. Il est toutefois important de toujours utiliser différentes voies de sécurité en même temps et d'avoir par exemple une authentification à deux facteurs.

"La cybersécurité est un processus qui nécessite une analyse permanente des risques"

Le modérateur Fredy Müller a ensuite ouvert la discussion au public. **Hans-Peter Steffen, cadre de RUAG**, a fait remarquer qu'il y avait une course technologique entre l'innovation / la mise en réseau totale et la prévention des abus. Il a donc voulu savoir s'il existait **une autre approche** que le contrôle total de toutes les données vitales. Il a cité l'exemple du **Predictive Policing**, qui permet de mieux identifier les menaces futures. **Florian Schütz** a répondu qu'il fallait toujours trouver un équilibre **entre sécurité et liberté** et que les deux n'étaient possibles que dans une mesure limitée. Mais pour lui, il est clair qu'il faut abandonner l'idée que la sécurité est un état. La sécurité, y compris la cybersécurité, est **plutôt un processus** qui nécessite **une analyse permanente des risques**. Selon lui, un système de crédit social comme en Chine ne serait pas compatible avec notre conception des valeurs. Schütz a également fait référence à la Constitution fédérale, qui stipule clairement à l'article 6 que ce n'est pas l'État qui protège, mais **que chaque personne doit gérer ses décisions de manière responsable**. **Jörg Mäder** a ajouté que l'on connaissait déjà l'évaluation des risques dans d'autres domaines: "Vous avez probablement aussi une clé de porte d'entrée et une clé de vélo, qui sont de qualité différente parce que le sinistre serait d'un montant différent". Mäder a encore ajouté que dans le cadre de la police prédictive, de nombreux systèmes opèrent avec l'intelligence artificielle, ce qui pose d'autres problèmes.

La question suivante a été posée par **David Ribeaud, CEO de Helvetia Specialty Markets**. Il a expliqué que l'Helvetia voyait deux défis en ce qui concerne le cyber : d'une part, la prévention ne suffit pas pour une Suisse résiliente, d'autre part, il n'existe **pas de solutions d'assurance pour les cybermenaces.** L'Helvetia propose donc que le secteur privé de l'assurance développe, avec le **soutien financier de la Confédération**, un programme de soutien aux sociétés axé sur la prévention. Les compagnies ne bénéficieraient toutefois de tels soutiens que si certaines mesures étaient prises pour accroître la cybersécurité. Suite à ces explications, il a demandé à Florian Schütz ce qu'il pensait d'une

telle idée. **Florian Schütz** a trouvé l'idée intéressante, mais s'est montré **sceptique quant à un soutien financier** de la part de la Confédération. Si le modèle est économiquement intéressant, il devrait être financièrement autonome. Il ne commencerait pas directement par le soutien, mais **développerait d'abord le modèle** en lui-même et **discuterait ensuite des bailleurs de fonds dans une deuxième phase.**

Jörg Mäder a demandé à M. Ribeaud ce qu'il en était de la réassurance et de l'évaluation des risques à long terme. Celui-ci a répondu qu'il n'y avait **pas de réassurance** et qu'il fallait donc réduire les mesures. Il a fait une comparaison avec la pandémie, lors de laquelle le risque était également mal diversifié, raison pour laquelle la Confédération a dû intervenir à titre subsidiaire. **Schütz** a fait remarquer que la question était en fait de savoir s'il ne fallait pas apprendre à **mieux comprendre les risques** pour pouvoir ensuite les quantifier, **ou si cela n'était pas possible** et qu'il fallait effectivement une solution de substitution à la suppression de l'assurabilité. Dans ce dernier cas, on peut tout à fait discuter de modèles tels que celui proposé par Helvetia. Il **n'est pas fermé à ce modèle**, il faut juste l'examiner de près.

Une autre question a été posée par **Yann Schmuki, collaborateur de la Base d'aide au commandement de l'armée.** Il voulait savoir comment l'État et l'armée peuvent s'assurer que les investissements dans le domaine cybernétique sont judicieux et qu'ils garantissent la protection que l'on souhaite. En réponse, **Florian Schütz** a fait référence aux fonctions du marché privé : "Il est faux de croire que l'État peut tout faire lui-même. C'est pourquoi, par le passé, l'État est de plus en plus allé dans le sens inverse et a privatisé différents domaines". La dernière question du public a été posée par **l'étudiante Yvonne Aregger**, qui souhaitait savoir si, en raison des cyberrisques, il existait également des approches de **solutions qui conduiraient à une "dé-numérisation".** Urs Loher a indiqué qu'il en allait de même pour les chaînes d'approvisionnement, où des réflexions similaires ont été menées. Cependant, il faut **réfléchir au trade-off** qu'une telle mesure entraînerait. Peut-être qu'à l'avenir, on ne numérisera plus certaines choses que l'on aurait autrement numérisées. **Florian Schütz** trouve également **l'idée séduisante**, mais y voit une petite erreur de raisonnement. Aujourd'hui, sur un marché mondial**, il n'est plus important d'être sûr, mais d'être rapide.** Il y a un **transfert de pouvoir des États vers les**

entreprises qui opèrent sur les marchés mondiaux. Il l'a illustré par l'exemple des puces électroniques, dont les composants sont tous fabriqués ailleurs dans le monde. De nombreuses choses ne peuvent donc plus être faites manuellement.

Enseignements et pistes à suivre

Lors de la table ronde finale, les intervenants ont transmis **d'importants messages clés** au public. Pour **Jörg Mäder**, les campagnes d'information fédérales sont importantes, mais il faut mettre **encore plus l'accent sur la formation** pour que l'informatique et les technologies de l'information puissent être utilisées correctement à l'avenir. **Alexandra Arni** a précisé que **la numérisation était là et qu'elle ne pouvait plus être annulée**. Il faut donc apprendre à la gérer. En outre, il faut une prise de conscience croissante de la responsabilité individuelle dans le domaine cybernétique. La cybersécurité n'est pas réservée aux nerds, mais doit toucher tous les secteurs de la société, jusqu'au niveau du management. Pour **Urs Loher**, le cyber est bien plus vaste que les attaques sur les réseaux informatiques. Il faut faire autant d'efforts dans la construction de systèmes et dans le développement de mesures. Le mot de la fin est revenu à **Florian Schütz** : "Prenez les nerds avec des qualités de direction et faites-en des cadres et, deuxièmement, pensons davantage en termes d'opportunités qu'en termes de risques et à saisir ces opportunités". C'est sur ce plaidoyer que le panel s'est clôturé. Le public a ensuite eu l'occasion de discuter de nombreuses autres questions passionnantes lors de l'apéritif qui a suivi.

©Daniel Saxer (iOf App, Defence & Security News)

Nous remercions nos partenaires de l'événements !

helvetia

AWK Group
a member of eraneos group

THALES

bedag

....et nos partenaires annuels !

spa
Sicherheit & Schutz

LKMD

VSSU