6 mai 2024 | Office fédéral de la cybersécurité OFCS

Stratégie de l'Office fédéral de la cybersécurité OFCS

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Aperçu / contenu

1 Contexte – défis pour la cybersécurité en Suisse

Les principaux défis[1] en matière de cybersécurité auxquels est actuellement confrontée la Suisse sont les suivants :

- grande vulnérabilité de l'économie, des autorités, du système éducatif et de la population dans le cyberespace ;
- capacité de réaction insuffisante face aux cyberincidents et aux cybercrises d'importance systémique ;
- faible maturité des produits et prestations numériques vis-à-vis de la cybersécurité et mécanismes lacunaires pour les contrôles de qualité ;
- compréhension des notions de cybersécurité uniquement ponctuelle dans l'économie, la société et le monde politique ;
- transparence lacunaire et données manquantes pour catégoriser les déclarations sur la cybersécurité et pour en déduire des mesures politiques et économiques appropriées ;
- protection limitée des acteurs qui ne font pas partie de la catégorie des infrastructures critiques ;
- flou juridique et coordination lacunaire entre les instruments de cybersécurité des autorités et ceux du domaine privé.

Ces défis permettent souvent aux cyberattaques d'aboutir, d'où des dommages économiques importants et un risque élevé de défaillance des infrastructures critiques nationales.

Les annonces de cyberincidents ayant occasionné des dommages ont augmenté de quelque 30 % par an ces dernières années. Le nombre d'entre elles émanant d'infrastructures non critiques a presque triplé ces douze derniers mois. En 2023, l'OFCS a traité 187 000 annonces de phishing et 8223 sites web établis en Suisse utilisés à ces fins ont été identifiés et mis hors service. Dans plusieurs centaines de cas, l'OFCS a décelé la présence de maliciels dans des infrastructures critiques et les a éliminés avec l'appui des entreprises touchées. Toutes les 40 heures en moyenne, une infection par de tels logiciels, pour lesquelles une aide au traitement est souhaitée, est signalée à l'OFCS.

Les cybercriminels visent de plus en plus les PME. Ils cryptent et volent des données au moyen d'attaques par rançongiciel, puis exigent une contrepartie financière pour leur décryptage et pour ne pas les publier. Les attaques étant fortement automatisées, elles ne demandent pas de gros efforts aux criminels qui n'ont dès lors pas de raisons d'épargner les petites entreprises. En Suisse, près du 75 % d'entre elles génèrent moins de CHF 500 000 de chiffre d'affaires par an. Aussi, pour ces PME tout spécialement, il est difficile d'investir dans la cybersécurité. Il est donc nécessaire à leurs yeux que le développement et la maintenance des produits et prestations numériques soient sûres ou que des services de sécurité soient disponibles à bas prix.

[1] D'après le rapport d'évaluation de l'efficacité de la stratégie nationale de protection de la Suisse contre les cyberrisques pour les années 2018 à 2022, de la cyberstratégie nationale (CSN), et les Weekly Reports et guichet pour les statistiques, GovCERT et OIC.

La population n'est pas non plus à l'abri. Elle est surtout confrontée au phénomène de la fraude en ligne. Une insécurité croissante et un besoin d'information et de soutien sont nettement perceptibles.

Dans un même temps, les hautes écoles suisses et les entreprises novatrices développent des solutions intéressantes pour la cybersécurité. La mise sur le marché de ces solutions, voire la création de normes mondiales, représentent toutefois un défi.

2 Vision de l'OFCS

La cybersécurité est une tâche commune à la politique, à l'économie, aux hautes écoles et à la société. Nombreuses sont les organisations et personnes qui ont du mal à estimer les cyberrisques et à les éviter. L'opacité qui entoure la sécurité des produits numériques mène à l'insécurité chez les consommateurs et à leur vulnérabilité. En raison de l'interconnexion croissante des réseaux, des systèmes insuffisamment protégés peuvent servir de vecteurs pour provoquer des dommages à grande échelle.

La Vision de l'OFCS est d'améliorer la cybersécurité en Suisse, en collaboration étroite avec tous les acteurs concernés :

L'OFCS fixe les fondements d'une utilisation sûre des services et infrastructures numériques en Suisse, permettant ainsi à cette dernière de se placer parmi les pays à la pointe d'une numérisation sûre.

3 Mission: les quatre piliers stratégiques

L'OFCS a pour mission principale de renforcer la cybersécurité des infrastructures critiques, de l'économie, du système éducatif, de la population et des autorités en coordonnant la mise en œuvre de la cyberstratégie nationale (CSN). Pour ce faire, il oriente ses prestations selon les quatre piliers stratégiques suivants :

1. **vulgarisation des cybermenaces**
2. **mise à disposition de moyens empêchant les cyberattaques**
3. **réduction des dommages dus aux cyberincidents**
4. **augmentation de la sécurité des produits et prestations numériques**

3.1 Vulgarisation des cybermenaces

L'OFCS vulgarise en fonction des groupes cibles les corrélations complexes qui mènent aux cybermenaces. Il permet ainsi d' instaurer à un dialogue constructif sur la cybersécurité entre le monde de la politique, celui de l'économie et la société. Cela permet à chacun d'eux d'assumer sa propre responsabilité dans la diminution des risques systémiques.

Une des questions les plus fréquemment posées par les conseils d'administration, les directions d'entreprise et les personnes privées est la suivante : « Que pouvons-nous faire pour nous protéger des cyberincidents ? » Le thème de la cybersécurité est aussi souvent abordé en politique. Les instances décisionnaires sont constamment confrontées au défi d'évaluer les cybermenaces et d'identifier les contre-mesures correspondantes.

L'OFCS recueille des informations sur les divers aspects des cyberincidents, montre leurs corrélations et élabore à partir de là des champs d'action, des thèmes de discussion et des recommandations. Il permet ainsi un dialogue constructif sur la cybersécurité et donne à tous les acteurs la capacité d'assumer leur propre responsabilité dans la diminution des risques systémiques. Ses analyses offrent une base aux fournisseurs de solutions de cybersécurité afin de développer leurs produits et prestations en ciblant les besoins.

3.2 Mise à disposition de moyens empêchant les cyberattaques

L'OFCS réduit la surface d'attaque des personnes et organisations suisses dans le cyberespace. Il signale des attaques et fournit des informations, voire des instruments, permettant de les éviter plus facilement.

Les cyberattaques exigent une préparation. En d'autres termes, les attaquants recherchent des failles du côté des cibles, achètent ou développent eux-mêmes des maliciels, et font des tentatives d'intrusions. Ils sont nombreux à recourir aux mêmes méthodes et procédures. L'OFCS relève leur profil et communique les informations et les avertissements correspondants à ses partenaires et aux victimes potentielles. Les informations vont des données techniques sur les vecteurs utilisés pour les attaques aux conclusions sur le choix donné d'un attaquant pour telle ou telle cible. Elles permettent d'alerter les organisations touchées afin que celles-ci augmentent leur protection.

La réduction de la surface d'attaque est plus importante encore que la détection précoce des cyberattaques. Trois facteurs affaiblissent sensiblement la cybersécurité : 1) les failles des systèmes, 2) les configurations incorrectes des systèmes, et 3) les mauvaises manipulations commises par les utilisateurs.

L'OFCS réduit la surface d'attaque des systèmes utilisés par les personnes et organisations suisses en favorisant la détection précoce et l'élimination des failles. Il signale des attaques et fournit des informations pour les contrecarrer. Pour prévenir toute attaque de grande ampleur aux conséquences potentiellement systémiques, l'OFCS utilise des instruments technologiques de manière ciblée et collabore avec les autorités compétentes pour prescrire réglementairement des mesures de protection.

L'OFCS développe des technologies de défense et de détection des dangers. Il les fournit lorsqu'aucun produit correspondant n'est disponible sur le marché ou que la situation justifie une intervention sur ledit marché. Les logiciels et méthodologies qui lui sont propres sont proposés autant que possible en open source.

3.3 Réduction des dommages dus aux cyberincidents

L'OFCS aide les personnes et organisations touchées par des cyberincidents à réduire les dommages et à circonscrire tout risque d'extension à d'autres victimes.

Les cyberincidents provoquent des dommages de toute sorte en fonction du modèle d'affaires ou de la situation personnelle des personnes ou organisations touchées. Ils renferment aussi le danger d'une extension des dommages : l'attaque peut être menée à travers le réseau de la victime pour cibler d'autres cibles ou occasionner par ricochet des dysfonctionnements ou des pannes lourdes de conséquences auprès de tiers.

Mais les dommages peuvent être réduits si l'on sait s'organiser et circonscrire à temps leurs effets. Pour sa part, l'OFCS se consacre en priorité à empêcher les dangers systémiques qui menacent le fonctionnement de l'État. En l'occurrence, il ne s'agit pas seulement de pannes dans les systèmes, mais aussi de dommages importants sur l'économie pouvant avoir un impact considérable sur le PIB (produit intérieur brut). L'OFCS aide les concernés dans la maîtrise des incidents en leur fournissant des conseils techniques et un appui organisationnel. Ces prestations de soutien dépendent de l'étendue potentielle des incidents et vont de simples conseils à une gestion complète de la cybercrise avec mesures techniques de défense et de réparation. Pour les organisations et personnes privées, c'est le principe de subsidiarité qui s'applique. Cela signifie que les victimes doivent, autant que possible, gérer elles-mêmes les incidents en recourant aux services proposés sur le marché.

L'OFCS crée des structures tant nationales qu'internationales permettant de simplifier la coordination de la gestion des cyberincidents et donne aussi la possibilité aux organisations et aux personnes privées de se préparer adéquatement à cette gestion en mettant des documents et des recommandations dites de bonnes pratiques à leur disposition. En cas d'attaque touchant plusieurs autorités en Suisse, c'est l'OFCS qui prend la direction des affaires.

3.4 Augmentation de la sécurité des produits et prestations numériques

L'OFCS incite les fournisseurs à proposer des produits et prestations sûrs à des prix abordables et encourage les modèles économiques correspondants. Il favorise la transparence pour les utilisateurs, de sorte que ceux-ci puissent, au regard de la cybersécurité, opter en toute connaissance de cause pour une variante ou pour une autre.

Les chercheurs ont constaté que presque chaque application présente au moins une faille de sécurité. Le matériel informatique n'est pas non plus à l'abri d'erreurs menaçant la cybersécurité. Vu la complexité des systèmes actuels, de telles erreurs ne sont pas totalement évitables. Une grands partie d'entre elles peuvent toutefois être esquivées ou rapidement détectées puis éliminées par un processus de développement et des tests bien structurés tout au long du cycle de vie des produits. Évidemment, des investissements importants dans la cybersécurité majorent

forcément les prix des produits qualifiés de sûrs, que des articles meilleur marché viennent d'emblée concurrencer. Pour le consommateur toutefois, il est difficile de juger si tel ou tel produit est sûr ou non, ou si un prix élevé est synonyme d'une plus grande sécurité.

L'OFCS appuie et élabore des initiatives et des modèles apportant de la transparence dans le domaine de la cybersécurité et favorisant le marché des produits qualifiés de sûrs. Ainsi, de tels modèles vont des schémas de labellisation à des propositions de réglementation, des incitations et des modèles de financement.

4 Modèle de fonctionnement de l'OFCS

Pour concrétiser cette garantie de performance de la manière la plus efficace possible, l'OFCS consolide et assemble des contenus, assure leur qualité, puis les transmet aux fournisseurs et aux bénéficiaires de services selon les besoins.

Il est tenu de respecter le modèle de coopération fixé dans la CSN et collabore étroitement avec les cantons, les milieux économiques et les hautes écoles. Le but de cette collaboration est de concentrer les connaissances et de se soutenir mutuellement de sorte à pouvoir optimiser la protection contre les cybermenaces.

L'OFCS fournit des contenus ou des services originaux uniquement si des contenus adéquats de tiers ne sont pas disponibles ou s'ils doivent être dispensés directement par la Confédération pour des raisons de législation ou de confiance. Il se qualifie notamment d'incubateur initiant de nouvelles prestations pour lesquelles il existe un besoin. Il les transmet à d'autres organisations dès qu'elles atteignent un certain degré de maturité et qu'un autre organe peut mieux les satisfaire.

Dans la mesure du possible, les services de l'OFCS sont fournis en tant que prestations numériques dans un modèle de plateforme. Une fourniture directe ne s'impose que là où cela s'avère nécessaire, en particulier dans le domaine du soutien à la gestion des incidents et celui de la sensibilisation. L'accent mis sur le modèle de plateforme permet l'échelonnement des prestations, tout en assurant un engagement clair des moyens.

À cet effet, l'OFCS met sur pied et gère une plateforme self-service donnant accès à des informations sur les cybermenaces, à des recommandations spécifiques ou générales, et à des moyens de prévention et de partage d'informations.