swisscom

Cyber Security Threat Radar
2021/2022

Réévaluer constamment les risques et l'environnement

Table des matières

«Seule une sécurité adaptée en tous points aux besoins des utilisateurs sera à même de remplir sa mission à moyen et long terme et de créer la résilience nécessaire.»

Cyber Security Threat Radar

Encore inimaginable il y a peu, c'est devenu une triste réalité depuis le 24 février: **la guerre en Europe bouleverse notre monde.**

La guerre qui frappe l'Ukraine m'a clairement rappelé le rôle et l'importance des médias (sociaux). On assiste à une alternance permanente de reportages bouleversants, de fausses informations flagrantes et de mises en scène savamment orchestrées sur fond de désinformation subtile.

Le fait est que les gouvernements, les organisations et les entreprises ont davantage pris conscience de nombreux risques et menaces depuis l'invasion russe en Ukraine, à comparer avec ces deux dernières années marquées par la pandémie. Cette situation tendue est perceptible dans toute la société.

Mais bonne nouvelle, nous n'avons pas observé de recrudescence des attaques sur l'infrastructure réseau suisse jusqu'ici, malgré la situation difficile.

Tout naturellement, les cybercriminels essaient de profiter de la guerre en Ukraine pour développer leurs activités illégales, notamment par le biais de tentatives d'hameçonnage ou de faux appels aux dons. Une pratique aussi regrettable que courante à chaque événement majeur de ce genre. Le volume des cyberactivités illégales se maintient donc à un niveau élevé; seule l'histoire sous-jacente a changé.

J'espère que ce Cyber Security Threat Radar 2021/2022 vous apportera de précieuses informations sur la cybersécurité et vous aidera à développer les activités ayant trait à la sécurité dans votre entreprise ou votre organisation.

Philippe Vuilleumier
Head of Group Security
Swisscom (Suisse) SA

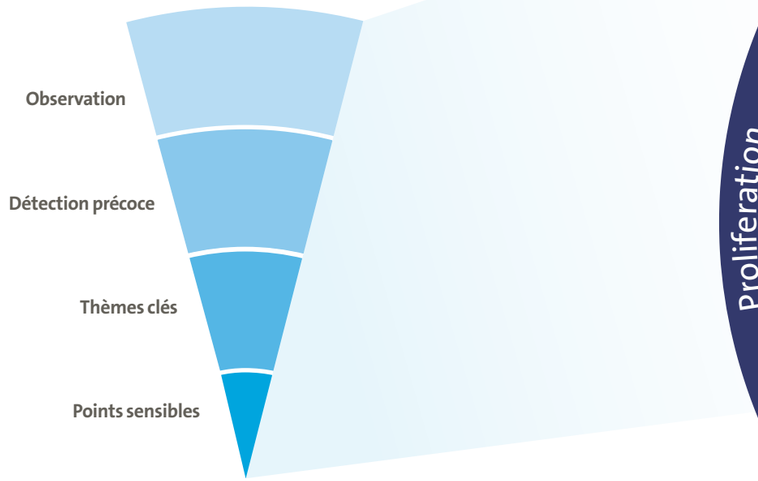
Ma déclaration tirée du Cyber Security Threat Radar de l'année dernière: «Les situations particulières exigent des mesures particulières lorsqu'il s'agit de sécurité, de protection et de sensibilisation aux risques» n'a pas pris une ride, bien au contraire. Il est d'autant plus important de garder une bonne vue d'ensemble dans ce contexte disruptif, afin de prendre les mesures appropriées.

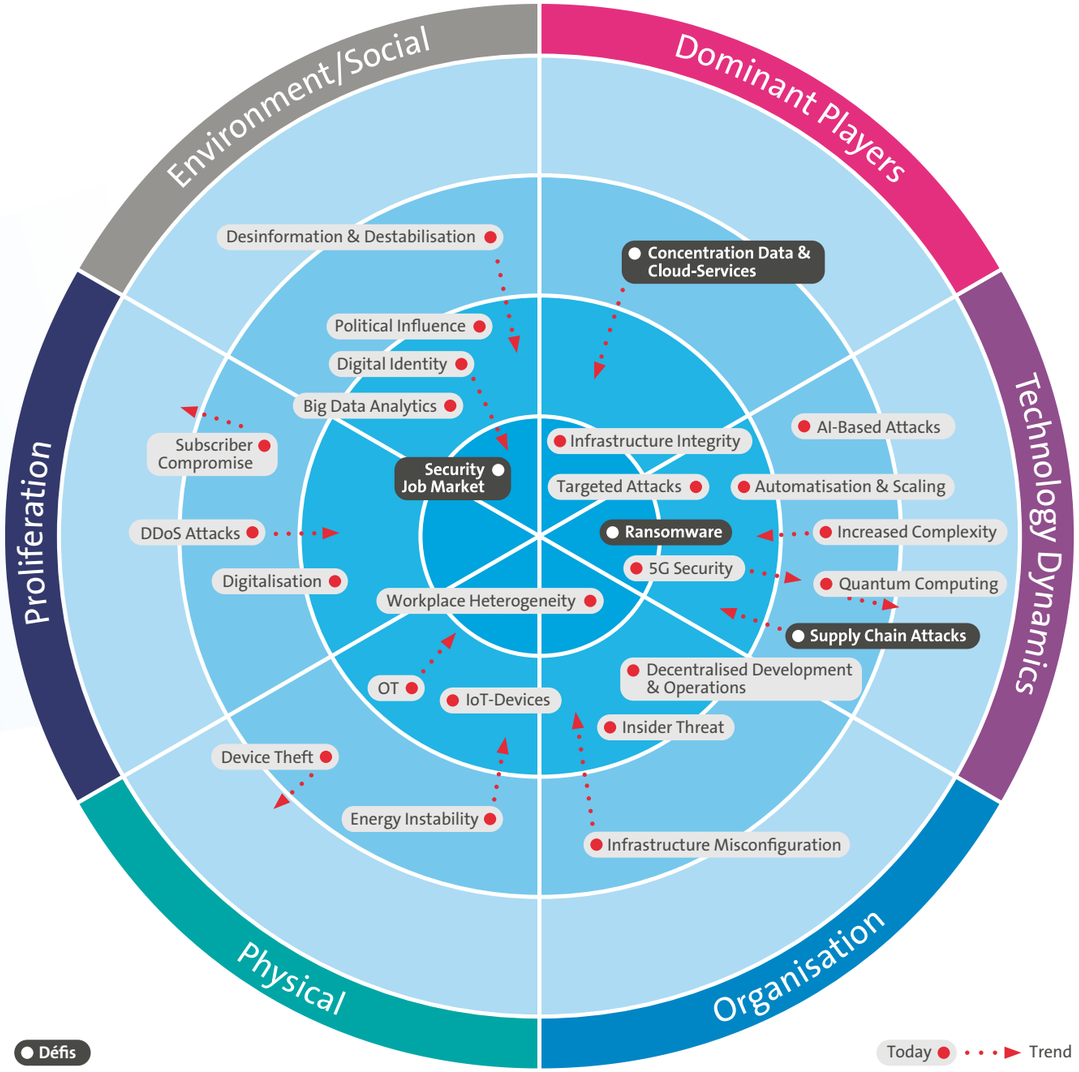
Ces mesures doivent s'articuler autour du facteur humain. Les technologies sont évidemment indispensables à tout arsenal de sécurité digne de ce nom. Pour autant, elles ne suffisent pas à garantir la protection. C'est pourquoi je recommande instamment de placer le facteur humain au centre de toutes les réflexions, les solutions et les mesures de sécurité. Seule une sécurité adaptée en tous points aux besoins des utilisateurs sera à même de remplir sa mission à moyen et long terme et de créer la résilience nécessaire.

État des lieux – radar des menaces

Pouvoir recourir en temps utile à des stratégies et des procédures de sécurité consolidées et éprouvées nous aide à faire face aux événements imprévisibles, aussi appelés «cygnes noirs». Lorsque celles-ci s'accompagnent d'une culture de la sécurité rigoureuse, de transparence sur les erreurs et d'une formation adéquate du personnel, les bases de la résilience organisationnelle sont jetées.

Mais faut-il encore identifier en amont les menaces potentielles et les observer de façon systématique. Pour faire le point sur le niveau de menace et son évolution, nous nous appuyons sur le Cyber Security Threat Radar.





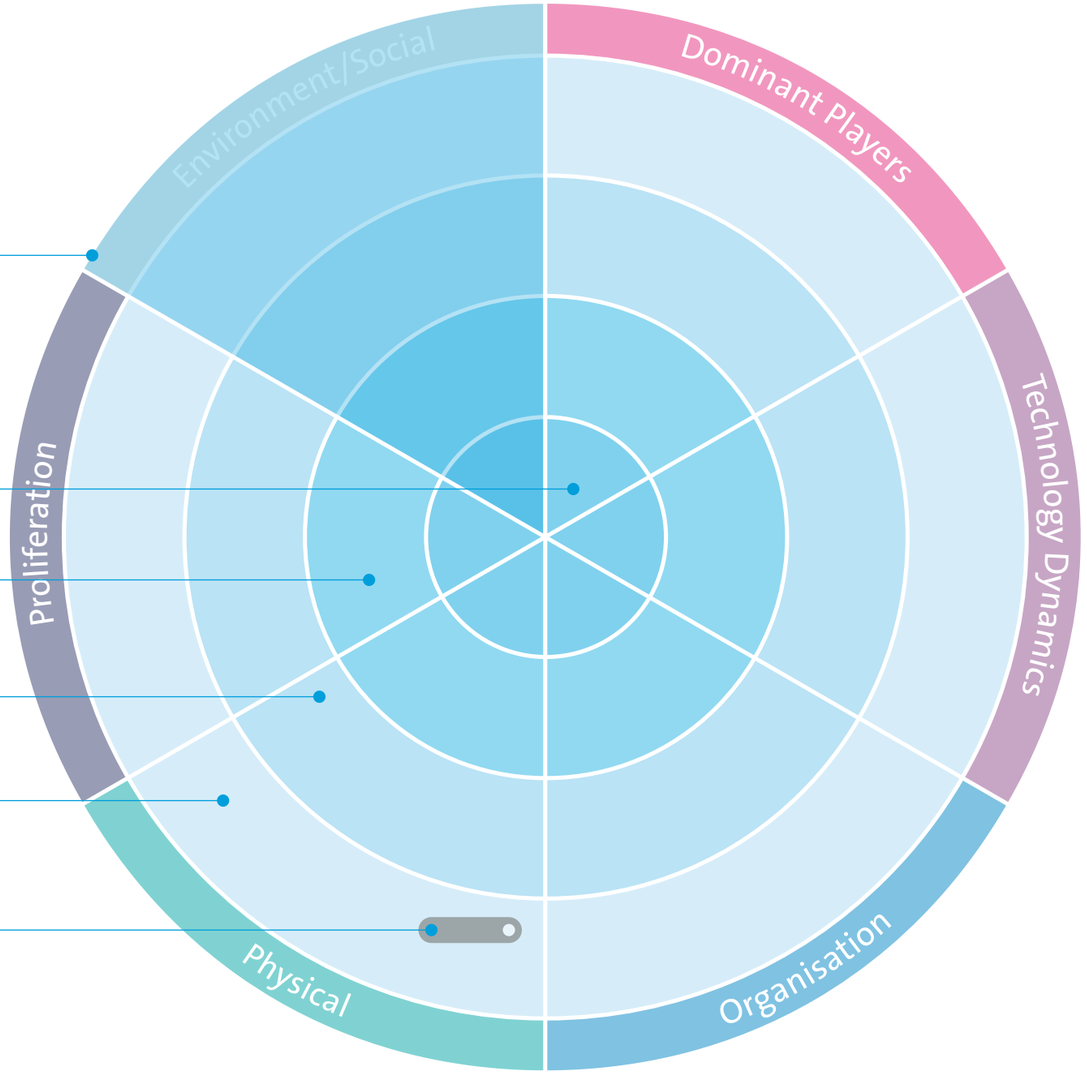
Méthodologie

Le radar des menaces se divise en six **segments** délimitant les différents domaines de menace. Dans chaque **segment**, les menaces associées peuvent être affectées à l'un des quatre cercles concentriques, qui indiquent si la menace en question est actuelle et le degré d'incertitude quant à son évaluation. Plus la menace se rapproche du centre du cercle, plus elle est concrète et plus il est important de prendre les mesures préventives adéquates.

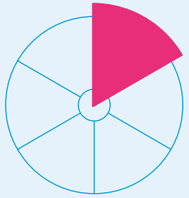
Ces cercles mettent en évidence:

- Des **points sensibles** pour les menaces déjà réelles dont la gestion nécessite de mobiliser des ressources relativement importantes.
- Des **thèmes clés** pour les menaces survenant de manière ponctuelle et dont la gestion nécessite de mobiliser des ressources normales. Il existe souvent des processus bien définis pour gérer efficacement les menaces de ce genre.
- Un besoin de **détection précoce** pour les menaces non encore survenues ou dont l'impact reste très faible à ce stade. Des projets ont été lancés pour pouvoir réagir très tôt à ces menaces, qui vont gagner en importance dans le futur.
- Un besoin **d'observation** pour les menaces qui ne devraient pas survenir avant quelques années. Aucune mesure concrète n'est définie pour gérer ces menaces.

En outre, chacune des **menaces** représentées affiche une **tendance,** dont la criticité peut être en hausse, en baisse ou stable. La longueur du faisceau de la tendance symbolise la rapidité avec laquelle le niveau de criticité de la menace va évoluer.

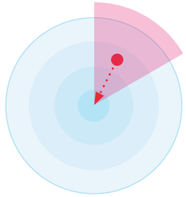


Zoom sur les tendances et évolution sur un an



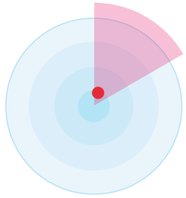
Dominant Players

Ce segment inclut les menaces résultant des interdépendances entre les principaux fabricants, services ou protocoles.



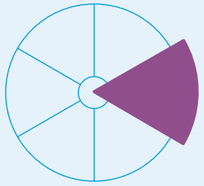
Concentration des Data & Cloud Services
La forte centralisation au sein de la structure de l'Internet induit des risques cumulés. La défaillance d'un service majeur peut avoir des répercussions dans le monde entier.

▲ Croissant (note: pour en savoir plus, rendez-vous à la page 28)



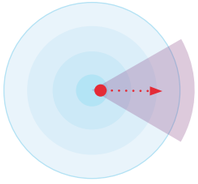
Infrastructure Integrity
Des vulnérabilités peuvent avoir été intégrées délibérément ou par négligence dans des composants essentiels des infrastructures critiques, compromettant ainsi la sécurité du système.

► Inchangé



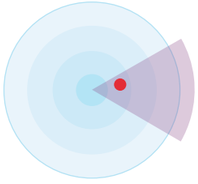
Technology Dynamics

Ce terme fait référence aux menaces résultant de l'innovation technologique fulgurante, qui offrent aux hackers de nouvelles opportunités et créent de nouvelles menaces inhérentes au développement.



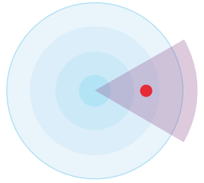
5G Security
La 5G est une technologie mobile encore jeune. Son déploiement crée de nombreuses opportunités, mais s'accompagne aussi de menaces encore inconnues.

▼ Décroissant



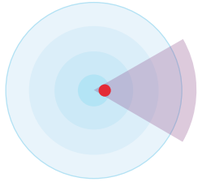
Automatisation & Scaling
L'automatisation accrue des processus d'exploitation techniques aura un plus fort impact en cas d'attaques réussies ou de défauts de configuration.

► Inchangé



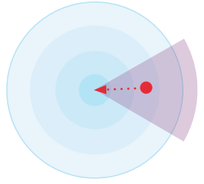
Quantum Computing
Les ordinateurs quantiques peuvent rendre inutiles les procédés cryptographiques actuels, compte tenu de leur capacité à les contourner en un rien de temps.

▼ Décroissant



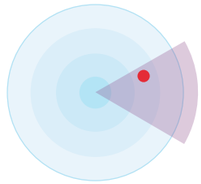
Ransomware
Les données critiques sont cryptées en masse, puis (éventuellement) décryptées moyennant le paiement d'une rançon.

▲ Croissant (note: pour en savoir plus, rendez-vous à la page 32)



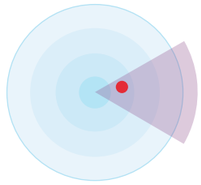
Increased Complexity
La complexité des systèmes ne cesse de croître, notamment hors du cadre technologique de l'entreprise. Les paysages IT se complexifient d'autant plus dans un environnement hybride/multicloud avec de nombreux fournisseurs de cloud. Cela augmente l'exposition aux risques et complique la recherche d'erreurs.

▲ Niveau croissant



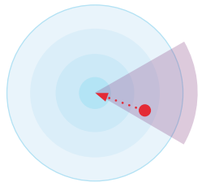
AI-Based Attacks
Les attaques au moyen de l'intelligence artificielle (IA) sont plus ciblées et donc plus difficiles à détecter. L'IA les rend plus efficaces sur les vecteurs d'attaque classiques, tels que le ransomware, l'hameçonnage et le spear phishing, ainsi que sur de nouveaux modes opératoires moins répandus comme les deepfakes et la désinformation.

► Inchangé



Targeted Attacks (APTs)
Des attaques ciblées et complexes poursuivant un objectif concret. Les personnes clés sont identifiées et ciblées directement ou indirectement (lateral movement) afin d'obtenir des informations sensibles ou de causer un préjudice maximal. La persistance est un aspect essentiel, c'est-à-dire que les hackers opèrent aussi longtemps que possible sans se faire repérer.

► Inchangé



Supply Chain Attacks
Les attaques sur la chaîne d'approvisionnement ont pour objectif de tirer parti des relations de confiance et commerciales entre une entreprise et des parties externes. Il peut s'agir de partenariats, de relations avec les fournisseurs ou de l'utilisation de logiciels tiers.

▲ Croissant (note: pour en savoir plus, rendez-vous à la page 36)

Organisation

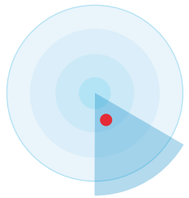
Cette tendance désigne les menaces résultant des changements dans les organisations ou consistant à exploiter les failles de ces dernières.

Workplace Heterogeneity
Malgré les nombreuses opportunités qu'offrent les nouveaux modèles de travail comme le «Bring Your Own Device» (BYOD) et le recours accru au télétravail, la mise en place incontrôlée de ce type de modèles expose davantage aux risques.

► Inchangé

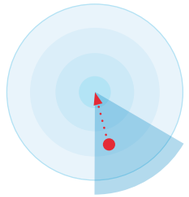
Decentralised Development & Operations
Les départements de développement classiques périclitent; le développement d'applications est confié davantage aux Business Units, avec des cycles de release toujours plus courts. De quoi compliquer le contrôle/la gestion de la sécurité.

► Inchangé



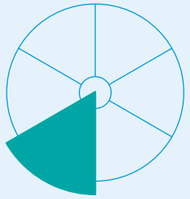
Insider Threat
Des partenaires ou des collaborateurs manipulent, détournent ou vendent des informations par négligence ou de façon intentionnelle.

► Inchangé



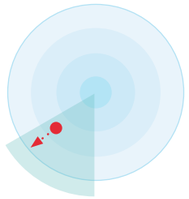
Infrastructure Misconfiguration
Exploitation d'éléments de l'infrastructure mal configurés et/ou de vulnérabilités identifiées et corrigées tardivement.

▲ Niveau croissant



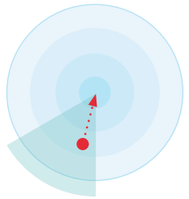
Physical

Ce terme regroupe les attaques sur l'infrastructure du cyberespace et causant davantage de dégâts dans le monde physique. Mais cela inclut aussi les menaces liées à l'environnement physique et davantage axées sur des cibles physiques en règle générale.



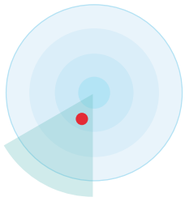
Device Theft
Le vol ou la perte de quelconque manière de terminaux comme des smartphones, des ordinateurs portables et des composants informatiques essentiels, peut entraîner la perte de données ou compromettre la disponibilité des services IT.

▼ Décroissant



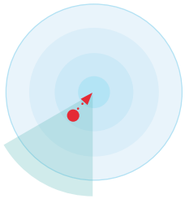
Energy Instability
Attaques ciblant des infrastructures critiques telles que celles des opérateurs de réseau électrique. La sûreté de fonctionnement est un élément important et le thème de la Business Continuity revient fréquemment dans les débats sur la cyberrésilience. Les pénuries d'électricité, les blackouts (panne générale d'électricité) et les blue-outs (défaillance générale de l'approvisionnement en eau), entre autres, sont des éléments importants. Les médias montrent que les infrastructures critiques sont nettement plus vulnérables aux cyberattaques.

▲ Niveau croissant



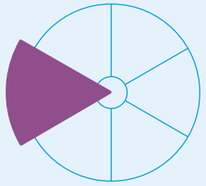
IoT Devices
Les appareils faiblement protégés peuvent être compromis et sabotés. Cela peut restreindre leur fonctionnement et avoir un impact, par exemple, en termes de disponibilité et d'intégrité des données.

► Inchangé



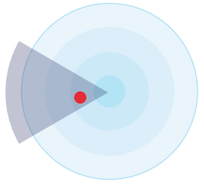
Technologie opérationnelle OT
La technologie opérationnelle (OT) consiste à utiliser du matériel et des logiciels pour surveiller et contrôler les processus, les appareils et les infrastructures physiques. Présente dans de nombreux secteurs d'activité, elle s'utilise à des fins diverses et variées, par exemple pour surveiller les infrastructures critiques ou encore pour piloter les robots sur les lignes de production. Il existe encore de nombreux systèmes de contrôle mal ou non protégés pour les éléments d'infrastructure critique.

▲ Niveau croissant



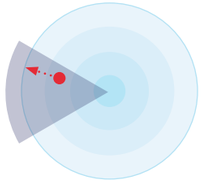
Proliferation

Ce segment inclut les menaces résultant de la disponibilité accrue et à moindre coût des connaissances et des supports IT. La propagation à large échelle augmente les surfaces d'attaque et accroît la disponibilité des outils d'attaque.



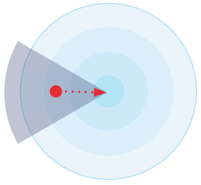
Digitalisation
L'interconnexion croissante du monde réel et virtuel dans la vie privée et professionnelle élargit l'éventail des vecteurs d'attaque. Le nouveau modèle «New Work» et le transfert opéré vers des environnements en télétravail exacerbent aussi les cyberrisques et la vulnérabilité de l'infrastructure IT en raison des terminaux non sécurisés.

► Inchangé



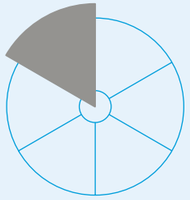
Subscriber Compromise
Des programmes malveillants se créent un accès aux données privées des utilisateurs mobiles ou servent à cibler les infrastructures IT et de télécommunication.

▼ Décroissant



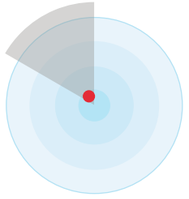
DDoS Attacks
Une attaque par déni de service distribué (DDoS) est une tentative malveillante de perturber le trafic normal d'un serveur, d'un service ou d'un réseau ciblé en submergeant la cible ou son infrastructure environnante avec un flot de trafic Internet. L'efficacité des attaques DDoS réside dans l'utilisation de plusieurs systèmes informatiques compromis comme sources de trafic hostile. Les machines exploitées peuvent être des ordinateurs et d'autres ressources situées sur le réseau, comme des appareils IdO. Une forte croissance combinée à une faible protection des appareils IoT accroît les prises de contrôle potentielles par le biais des réseaux de bots.

▲ Niveau croissant



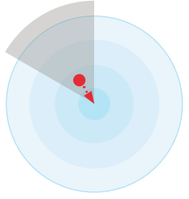
Environment/Social

Il s’agit des menaces émanant directement des changements sociaux et politiques ou consécutives à ces changements, qui simplifient la tâche des hackers et rendent donc les attaques plus profitables.



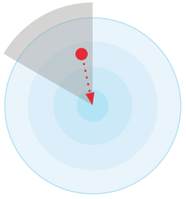
Security Job Market
Les besoins énormes en professionnels de la sécurité sont très difficiles à satisfaire. Il en résulte une perte de savoir-faire dans la lutte contre des attaques de plus en plus complexes et intelligentes.

► Inchangé (note: pour en savoir plus, rendez-vous à la page 24)



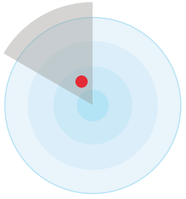
Digital Identity
Les identités numériques personnelles certifiées peuvent être usurpées ou volées, par exemple pour conclure des contrats sous le nom d’une tierce personne.

▲ Niveau croissant



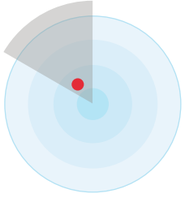
Desinformation & Destabilisation
La diffusion volontaire de fausses informations peut créer une instabilité économique et sociale et s’utilise de plus en plus de manière ciblée dans les situations de crise, notamment dans le cyberespace.

▲ Niveau croissant



Political Influence
Les forces politiques peuvent influer sur les décisions d’ordre technologique ou économique, notamment dans le choix des fournisseurs de technologie. Il peut en résulter de nouveaux risques

► Inchangé



Big Data Analytics
Le volume accru de données et les modèles d’analyse améliorés peuvent être utilisés abusivement pour influencer le comportement des gens. De plus en plus, la prise de décisions est confiée à des systèmes autonomes. Les données des «big data lakes» sont détournées à des fins de désinformation, de fake news et d’analyses sociétales et psychosociales, ainsi que pour créer des modèles de mouvement. Ce dernier point induit une violation de la sphère privée.

► Inchangé

Défis et tendances

Pénurie de main-d'œuvre qualifiée dans le Security Job Market

De quoi s'agit-il ?

Infrastructures IT hybrides de plus en plus décentralisées, environnements IoT et télétravail : les exigences sont toujours plus strictes pour les systèmes de sécurité informatique, les menaces se multiplient, mais les spécialistes se font rares. Les entreprises doivent prendre un ensemble de mesures pour protéger les réseaux et les données et développer le savoir-faire. L'automatisation, tout comme la formation initiale et continue, a aussi un rôle à jouer.

Le manque de personnel qualifié aggrave les difficultés actuelles dans le domaine de la sécurité IT. Le Global Risk Report 2022 du WEF met lui aussi en lumière la pénurie mondiale d'experts en cybersécurité. On estime qu'il manque environ trois millions de professionnels sur le marché du travail.

L'International Information System Security Certification Consortium (ISC)² a réalisé un sondage pour déterminer les possibles conséquences d'une pénurie de personnel dans la cybersécurité. 32 % des personnes interrogées évoquent comme possible conséquence la mauvaise configuration des systèmes. Elles sont presque autant à craindre que le temps manque pour une gestion des risques adéquate ou qu'un élément important soit négligé. 27 % d'entre elles pensent qu'il est impossible d'identifier toutes les menaces sur le réseau. De même, 27 % des répondants considèrent que l'installation et la configuration de logiciels à la hâte en raison du manque de personnel constituent un réel danger.

La Suisse aura besoin d'environ 118 000 spécialistes TIC supplémentaires d'ici 2028 si l'on en croit l'«Étude sur les besoins en spécialistes TIC d'ici 2028» menée par ICT-Formation professionnelle Suisse. Pour répondre à ce besoin, il faudrait former quelque 36 000 personnes de plus qu'actuellement. Un défi pour la politique de formation et sur le plan macroéconomique, lequel exige des mesures exceptionnelles. Les entreprises de tous les secteurs, ainsi que l'administration publique, sont appelées à créer de nouvelles places d'apprentissage et d'études dans l'informatique et la médiamatique.

Au vu de ces chiffres, il n'est pas étonnant que les entreprises aient du mal à trouver les candidats adéquats et à les garder. Il faut compter en moyenne six mois pour pourvoir un poste vacant dans l'informatique, sous réserve de multiplier les offres et les entretiens d'embauche. De plus, les petites et moyennes entreprises peinent déjà à trouver des spécialistes, mais aussi à les garder dans la durée, faute de pouvoir les challenger suffisamment.

Quelle sera l'évolution dans le futur?

Le recrutement de spécialistes en informatique constitue un défi lorsque les profils qualifiés et adéquats manquent. Bon nombre d'entreprises s'efforcent donc de garder leur personnel. Mais cela ne suffira pas à résoudre le problème. Il conviendra de garder les collaborateurs qualifiés et d'automatiser les tâches courantes.

Il sera de plus en plus laborieux pour les entreprises de trouver des professionnels formés à la sécurité IT, d'autant plus qu'elles seront toujours plus nombreuses – petites structures incluses – à avoir besoin d'experts. L'évolution démographique sur le marché du travail ne fera qu'aggraver la situation. Les entreprises trouveront de moins en moins de nouveaux et jeunes professionnels. La «guerre des talents» va s'intensifier et les besoins de sécurité vont croître de manière générale. Les situations de crise, à l'instar de la guerre en Ukraine, auront pour effet d'accentuer la prise de conscience des entreprises et des organisations en matière de sécurité.

Ainsi, la pénurie de spécialistes en cybersécurité se fera sentir de deux manières. D'une part, les experts du numérique manqueront pour développer des solutions de sécurité IT, alors que les attaques de cybercriminalité seront de plus en plus sophistiquées et ciblées. D'autre part, les entreprises manqueront de responsables de la sécurité IT qualifiés et à même de lutter contre la menace croissante de la cybercriminalité en prenant les mesures appropriées.

La pénurie de spécialistes IT touche surtout les petites et moyennes entreprises (PME), car les collaborateurs qualifiés leur préfèrent souvent les grands groupes, qui proposent des modèles de rémunération et des avantages sociaux plus attrayants.

Afin de désamorcer cette pénurie de personnel, les universités proposent de plus en plus des cursus dédiés à la cybersécurité. Il reste à voir si cela permettra de pallier rapidement les problèmes structurels. Développer le savoir-faire requis prendra beaucoup de temps. Par ailleurs, la formation purement théorique devra s'accompagner d'une certaine expérience pratique. Il y aurait une approche potentiellement plus prometteuse: les entreprises pourraient s'engager dans la recherche et l'enseignement axés sur la pratique en mettant à contribution leurs départements spécialisés et leurs spécialistes. Par ailleurs, elles auraient intérêt à se concentrer davantage sur les collaborateurs intéressés par la cybersécurité en assurant leur formation continue. Mais cela ne suffira pas, du moins à moyen et à court terme, à combler le manque béant de personnel et de sécurité en résultant. Dans les départements de sécurité en sous-effectif, le manque de connaissances techniques se cumule aux experts souvent surmenés, ce qui n'est pas une base saine pour leur propre cybersécurité.

Comment faire face efficacement à ce défi?

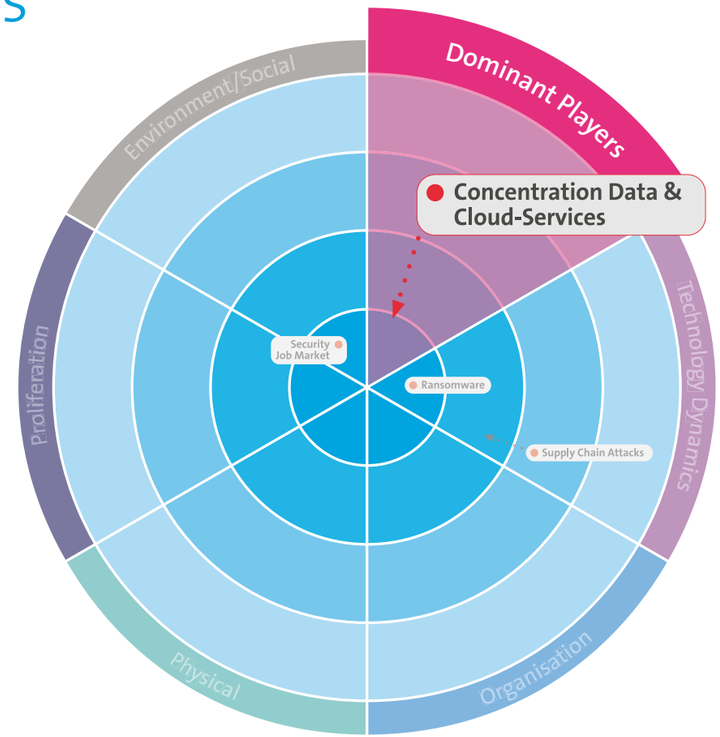
- Maintenir l'attractivité de l'employeur et fidéliser les collaborateurs
- Proposer aux talents un challenge axé sur la pratique
- Investir dans la formation technique interne et créer des programmes de formation attrayants
- Offrir des possibilités d'évolution dans l'entreprise et assurer une forte employabilité
- Recourir davantage aux médias sociaux pour recruter et être présent lors d'événements professionnels
- Tirer parti du brand marketing de l'employeur et du réseau des collaborateurs
- Encourager les opportunités pour les juniors, p. ex. la mise en place de programmes dédiés (pour former les futurs collaborateurs)
- Repérer les talents grâce aux programmes Bug Bounty internes
- Automatiser les processus standard et l'assistance logicielle, même pour les tâches complexes
- Intégrer un MSSP externe (Managed Security Service Provider)

«Nul besoin d'avoir des experts entièrement formés. Nous avons de bonnes expériences avec des professionnels issus de domaines d'expertise connexes (développeurs, administrateurs réseau, etc.) et des jeunes sortant de formation qui veulent se perfectionner sur le sujet.»

Dimosthenis Georgokitsos
Program Manager Cyber Security,
Recruiting & Education, Swisscom (Suisse) SA

Défis et tendances

Cloud hybride et multicloud dans la concentration des Data & Cloud Services



De quoi s'agit-il ?

Dans une solution multicloud, une entreprise utilise plusieurs services cloud différents, souvent de plusieurs fournisseurs. Le multicloud offre flexibilité et choix, mais s'avère aussi complexe. Pour la plupart des entreprises, la solution cloud «adéquate» se trouve non pas dans le public ou dans le privé, mais dans la combinaison des deux.

Le multicloud fait partie de la transition vers le cloud. Après avoir réussi une migration ou un onboarding de services cloud, le besoin d'avoir un autre cloud se transforme en nécessité. Plusieurs raisons à cela, p. ex. le risque, l'effet de verrouillage, les services, les projets, les équipes DevOps décentralisées utilisant des plateformes de cloud différentes. Bien souvent, il s'agit d'un environnement multicloud Azure, GCP ou AWS. Les services sous-jacents requièrent une gestion multiple, ce qui est inefficace. Une solution faîtière pour plusieurs clouds peut offrir des solutions, mais cela pose un nouveau défi de par la complexité globale accrue. Une stratégie multicloud comprend au moins deux plateformes ou prestataires de cloud computing. Pour certains spécialistes, le multicloud implique qu'une entreprise utilise des services aux fonctions identiques de différents prestataires, par opposition à une stratégie dans laquelle une organisation sélectionne le meilleur chez chaque fournisseur.

La plupart des études/experts soulignent les défis suivants:

- Gestion centralisée des identités et des accès tout au long du cycle de vie
- Compliance
- Manque de visibilité et de contrôle (E2E)
- Sécurité des données
- Complexité accrue
- Manque de connaissances et de compétences
- Manque d'uniformité dans les possibilités de journalisation et de surveillance
- Sécurité dans la chaîne d'approvisionnement
- Transfert de la responsabilité de sécurité

Quelle sera l'évolution dans le futur?

La gestion centralisée des identités et des accès (Identity and Access Lifecycle Management) gagnera encore en importance au vu des besoins croissants en matière de sécurité des données et de compliance. L'aspect de la «visibilité de bout en bout» doit être clarifié en préparation à l'Incident Detection & Response.

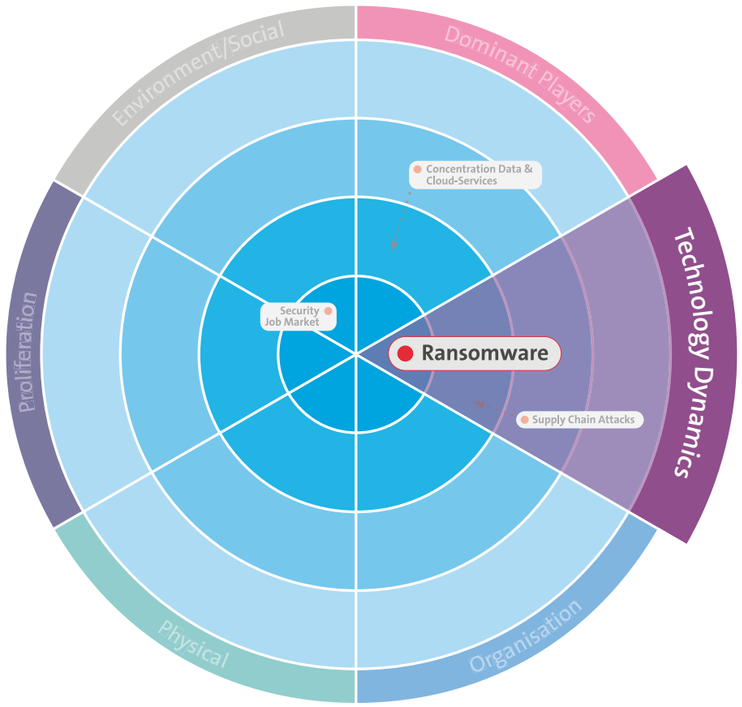
Comment faire face efficacement à ce défi?

- Réfléchir en amont au multicloud
- Disposer d'une architecture globale permettant une transition du cloud au multicloud
- Mettre en place un système de contrôle de la sécurité (Security Posture) et de la compliance sur l'ensemble des clouds
- Surveiller les infrastructures cloud dans leur globalité et créer une vue d'ensemble centralisée de tous les événements liés à la sécurité

«Un environnement multicloud offre des avantages indéniables. Toutefois, la complexité en résultant nécessite une gestion adéquate pour maîtriser les risques liés à l'augmentation de la surface d'attaque.»

Duilio Hochstrasser
Security Specialist, Swisscom (Suisse) SA

Défis et tendances
Ransomware



De quoi s'agit-il ?

Un ransomware est un logiciel malveillant conçu pour empêcher un utilisateur ou une organisation d'accéder à ses propres fichiers. En cryptant les données et en exigeant le paiement d'une rançon pour obtenir la clé de décryptage, les cybercriminels mettent les entreprises dans une position, où le paiement de la rançon semble être le moyen le plus simple et le moins onéreux d'accéder de nouveau à leurs fichiers. À cela s'ajoute parfois le vol de données pour exercer une pression supplémentaire sur les victimes du ransomware et les pousser à payer la rançon.

En très peu de temps, le ransomware est devenu le type de programme malveillant le plus connu et le plus visible, avec un préjudice financier annuel de plus d'un milliard de dollars américains à l'échelle mondiale (Gartner). Compte tenu du caractère lucratif des ransomwares pour les cybercriminels et de la sophistication croissante des méthodes d'attaque, les coûts engendrés par ces attaques continueront à augmenter. Il n'y a encore pas si longtemps, les attaques par ransomware faisaient surtout trembler les grandes entreprises, mais elles ciblent de plus en plus les PME ces dernières années.

Au-delà des coûts directs – lorsque l'entreprise paie la rançon – qui s'élèvent à environ 710 000 francs suisses en moyenne pour les attaques contre de petites entreprises, il y a aussi des coûts indirects liés à l'arrêt d'activité tout le temps où les systèmes sont verrouillés. Sans compter les éventuels frais de réparation et de restauration des systèmes et le préjudice en termes d'image. Une mauvaise réputation peut rapidement plonger une entreprise dans une situation mettant en péril son existence. Rétablir sa réputation nécessite des efforts considérables dans la durée, en plus de coûter très cher.

Quelle sera l'évolution dans le futur?

La tendance ne faiblira pas. Tant que des systèmes non patchés ou des accès RAS/VPN sans authentification à facteurs multiples (MFA) seront accessibles sur Internet et que des collaborateurs installeront des logiciels malveillants comme Quakbot, le risque d'une attaque par ransomware sera bien réel. Les tentatives d'hameçonnage avec des logiciels malveillants étant faciles à mettre en œuvre et souvent fructueuses, les cybercriminels n'auront pas besoin de développer davantage d'attaques par ransomware. Il se peut qu'à l'avenir, les attaques soient davantage automatisées ou organisées sur le modèle «as a service». Les technologies de deepfake et le recours à l'intelligence artificielle (IA) compliqueront encore la détection de ces attaques. En outre, il semblerait que les auteurs d'attaques ne se contentent plus de crypter les données, ils menacent également de les rendre publiques («double extorsion»).

À compter de la mi-2023, les entreprises basées dans l'Union européenne devront signaler les attaques par ransomware. Il faudra donc s'attendre à une explosion du nombre d'attaques rendues publiques, ce qui donnera l'impression à la population que le nombre d'attaques a augmenté. Il restera à voir si cela aura une influence sur le nombre effectif d'attaques. Une chose est sûre, les ransomwares ne constituent pas un «cas de force majeure». Il est légitime de s'attendre à ce que des services cloud se retrouvent sous «la coupe» des cybercriminels dans l'avenir.

Tout comme les industries comparables, nous travaillons d'arrache-pied à améliorer notre gestion des ransomwares.

Comment faire face efficacement à ce défi?

- S'assurer que l'administration des systèmes IT et des applications logicielles est appropriée dans toute l'organisation
- Patcher tous les services d'accès à Internet (surtout si les vulnérabilités ont déjà été exploitées) dans les meilleurs délais
- Faire des sauvegardes régulières (en local) des systèmes et des données (et tester le processus de récupération)
- Élaborer un plan de communication de crise tenant compte des prestataires tiers, des fournisseurs, des partenaires, des collaborateurs et des autres parties prenantes importantes
- Évaluer la capacité de l'entreprise (et du service informatique) à réagir à une attaque et à gérer les éventuelles défaillances système à l'aide de plans de réponse
- S'assurer que les collaborateurs sont bien informés sur la cybersécurité et le risque d'attaque par ransomware
- Protéger les services RAS/VPN avec l'authentification à facteurs multiples (MFA)/l'accès conditionnel
- Investir dans le déploiement à vaste échelle de la technologie EDR et du monitoring (p. ex. de l'infrastructure Active Directory) pour espérer détecter les attaques à temps et pouvoir les neutraliser
- Réduire la surface d'attaque

«Les auteurs d'attaques par ransomware agissent par opportunisme. Dès lors qu'une voie d'accès s'ouvre à eux, ils saisissent l'occasion.»

Thomas Röthlisberger
Senior Security Analyst & Tech Lead Red Team, Swisscom CSIRT

Défis et tendances

Écosystème des fournisseurs et dépendances/Sécurité de la chaîne d'approvision-nement

De quoi s'agit-il ?

Toutes les organisations doivent – dans une certaine mesure – faire confiance aux autres entreprises lorsqu'elles installent leurs logiciels sur leurs réseaux et qu'elles travaillent ensemble. Les attaques sur la chaîne d'approvisionnement exploitent justement ces relations de confiance, mais aussi la perte de contrôle résultant des dépendances entre les différentes organisations.

Elles ciblent alors le maillon le plus faible au sein de la chaîne de confiance. En d'autres termes, si une organisation dispose d'un système de cybersécurité robuste, mais qu'elle collabore avec un prestataire vulnérable, celui-ci sera pris pour cible par les assaillants. Dès lors qu'ils ont un pied dans le réseau du prestataire, les hackers peuvent se jouer de cette relation de confiance pour accéder au réseau plus sécurisé. Les dérangements chez les prestataires entravent la fourniture de nos propres prestations, par exemple par l'absence de prestations préalables (rupture de SLA de notre côté) ou par une mise en danger directe (par exemple en compromettant des appareils tiers dans nos réseaux ou logiciels).

En effet, les Managed Service Providers (MSP) sont souvent la cible d'attaques au sein de la chaîne d'approvisionnement. Ils ont un accès intégral aux réseaux de leurs clients, ce qui vaut son pesant d'or pour les auteurs d'attaques. Une fois infiltrés chez le MSP, les pirates peuvent facilement étendre leurs méfaits aux réseaux des clients. En exploitant les vulnérabilités de la chaîne d'approvisionnement, ils renforcent leur influence et peuvent accéder à des réseaux bien plus difficiles à attaquer autrement. C'est ce procédé qui a permis aux auteurs de l'attaque de Kaseya d'infecter autant d'organisations avec des ransomwares.

D'autres attaques sur la chaîne d'approvisionnement reposent sur un logiciel qui envoie des malwares aux clients d'une entreprise. À l'exemple des assaillants de SolarWinds, qui ont réussi à accéder aux serveurs build de l'entreprise pour ajouter une porte dérobée dans les mises à jour du produit de surveillance du réseau de SolarWinds Orion. Une fois le code installé chez les clients, les pirates ont pu accéder à leurs réseaux. Par ailleurs, Log4J a indiqué que bon nombre d'entreprises ne maîtrisaient pas suffisamment l'utilisation des bibliothèques et des frameworks dans les solutions. Cela va au-delà des prestataires directs et inclut les sous-traitants et les sous-traitants des sous-traitants.

Quelle sera l'évolution dans le futur?

Nous tablons sur une recrudescence de ce phénomène en raison de l'interconnexion accrue avec les fournisseurs (assistance à distance, bibliothèques de logiciels, SaaS) et des attaques visant à perturber les chaînes d'approvisionnement. De plus, les pirates sont désormais capables d'exploiter bien plus rapidement les failles.

Comment faire face efficacement à ce défi?

- Se concentrer sur les fournisseurs principaux/critiques
- Intégrer des techniques DevSecOps dans le cycle de développement
- Minimaliser les données lors des échanges avec les partenaires
- Répertorier les relations avec les fournisseurs et évaluer leur impact
- Observer en continu les fournisseurs importants et élaborer des plans de continuité
- Mettre en place des alternatives et des solutions de repli pour les fournisseurs importants

«Les «Software Bills of Materials» (SBOM) permettent effectivement de vérifier la composition des livrables jusqu'aux niveaux fonctionnels – et même sur plusieurs niveaux. Il faut faire la même chose au niveau du matériel, peu importe qu'il soit sur mesure ou standard. Cela existe d'ores et déjà dans certaines technologies.»

Oliver Jäschke
Security Governance Manager, Swisscom (Suisse) SA

Conclusion

Alors que nous pensions avoir un peu de répit au vu du recul progressif de la pandémie, la guerre en Ukraine a montré une nouvelle fois la vulnérabilité de notre monde. Aujourd'hui, tant de choses paraissent encore plus fragiles et hors de contrôle.

À cela s'ajoute le manque de ressources de plus en plus perceptible dans de nombreux départements informatiques et de sécurité. Le monde est confronté à des problèmes pernicieux. En raison d'exigences lacunaires, contradictoires et changeantes, ceux-ci ne sont pas toujours prévisibles, planifiables et compensables, ce qui les rend généralement difficiles ou impossibles à résoudre.

Tout cela semble bien compliqué et légèrement déprimant. Pour autant, nous ne devons pas nous laisser décourager. La numérisation progresse ardemment dans les entreprises et les organisations. Elles prévoient toutes, ou presque, de migrer leurs composants et leurs services IT vers le cloud en 2022, si ce n'était pas déjà à l'ordre du jour durant ces dernières années. Les thématiques comme le métavers, le Web 3.0, les NFT et la blockchain marquent l'évolution actuelle du cyberespace et donnent des raisons d'espérer. Il convient de prendre du recul, de tout mettre en balance et d'opérer une gestion active des risques.

Dans un monde toujours plus volatil, incertain, complexe et ambigu, nous devons nous concentrer davantage sur notre propre gestion des risques. Quels sont les éléments sensibles? Qu'est-ce qui menace nos valeurs et nos ressources dans l'organisation? Quel rôle les services et composants critiques de tiers (fournisseurs, prestataires SaaS, services cloud, etc.) jouent-ils?

Nous devons faire de nos collaborateurs des alliés, exiger des responsables de conduite qu'ils assument cette fonction d'exemple si souvent évoquée, veiller au respect systématique des directives et des règles et nouer des alliances entre les départements. Être capable d'opposer une défense adéquate aux risques et aux dangers en constante évolution nécessite une sécurité plus agile.

«L'être humain est la clé de voûte du dispositif de sécurité.»

Remarques

Colophon

Éditeur	Swisscom (Suisse) SA, Group Security
Conception/réalisation	Agence Nordjungs, Zurich
Rédaction	Swisscom (Suisse) SA Marcus Beyer (Group Security) Manuel Bühlmann (Group Communications) Claudia Lehmann (B2B Communications)
Traduction	Textraplus AG
Copyright	© Mai 2022 by Swisscom (Suisse) SA, Group Security, Alte Tiefenaustrasse 6, 3048 Worblaufen, swisscom.ch
Édition	OK DIGITALDRUCK AG, Zurich
Tirage	200 exemplaires

L’esprit tranquille dans le monde interconnecté

Nous plaçons les besoins de nos collaborateurs, clients et partenaires au cœur de toutes les problématiques de sécurité. Notre infrastructure IT et nos réseaux modernes nous permettent de développer des solutions, des produits et des services sécurisés.

Tu cherches un emploi dans le domaine de la sécurité chez Swisscom ?
Alors, jette un coup d’œil à ce lien et inscris-toi :

swisscom.com/securityjobs

#talkingaboutsecurity

swisscom.ch/security