swisscom

Cyber Security Threat Radar
2022/2023

Vivre la Security by Design

Table des matières

« Security by Design et Human Centered Security. Autrement dit : une approche de la sécurité déployée dès le stade de la conception et axée sur les collaborateurs. Ce n'est qu'ainsi que nous pourrons continuer à garantir la sécurité de nos entreprises. »

Cyber Security Threat Radar

Cyberrisques – une implantation durable ?

Le danger qu'impliquent les cyberrisques reste très élevé. Pour améliorer la cyberrésilience de son entreprise, il convient impérativement de développer une approche globale de la cybersécurité et de la sécurité informatique. Attendre que les crises passent ou espérer un rapide retour à la normale de l'état des menaces n'est pas recommandé. Il est plus judicieux de se préparer pleinement à d'éventuels scénarios de crise, afin de pouvoir réagir de manière adéquate et limiter les dommages en cas d'urgence. Les multirisques et les cyberrisques auxquels nous sommes actuellement confrontés sont durablement implantés. Leur impact est palpable et visible dans de nombreux pays du monde. Les dommages collatéraux risquent par ailleurs de les rendre encore plus imprévisibles.

Il est désormais évident que la cybersécurité ne relève pas uniquement de la responsabilité des services informatiques, mais qu'elle concerne tous les secteurs d'une entreprise. Un dispositif de gestion des risques intègre à la fois un Business Continuity Management solide et un service informatique stable. Parallèlement aux précautions techniques, il est essentiel de disposer d'un personnel bien formé et attentif. Seule l'association de ces deux aspects permet d'atteindre une résilience maximale.

Le présent Cyber Security Threat Radar vise à aider les entreprises à identifier les principaux cyberrisques auxquels elles sont exposées et à les combattre de manière adaptée. Il sert de fil rouge pour développer une approche uniforme de la cybersécurité et pour définir un concept de sécurité global.

Ce guide interorganisationnel jette les bases d'une cybersécurité performante, et par là même du succès de toute entreprise dans l'univers numérique.

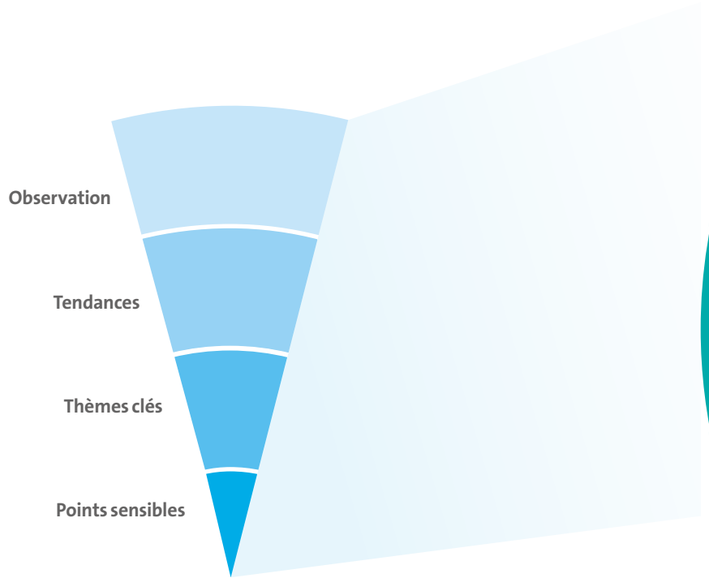
Marco Wyrsch
Head of Group Security
Swisscom (Schweiz) AG

« La guerre en Europe bouleverse notre monde », a déclaré mon prédécesseur en tant que Head of Group Security chez Swisscom, Philippe Vuilleumier, dans son introduction au Cyber Security Threat Radar de l'année dernière. Un an plus tard, tandis que la guerre continue à exercer son emprise sur le monde, ses propos n'ont rien perdu de leur validité. Son impact est perceptible à bien des égards : menace de pénurie d'électricité et de gaz, migration du champ de bataille dans le cyberespace, actes de sabotages sur des infrastructures critiques, déluge de fake news et couverture médiatique intensive sur tous les canaux. La situation actuelle le montre clairement : lors de crises multiples, la sécurité logique et la sécurité physique sont indissociables. D'où la nécessité d'être pleinement conscient des risques. En période d'incertitude, l'interaction entre les personnes, les processus et les technologies constitue la base de la résilience et de la stabilité des entreprises.

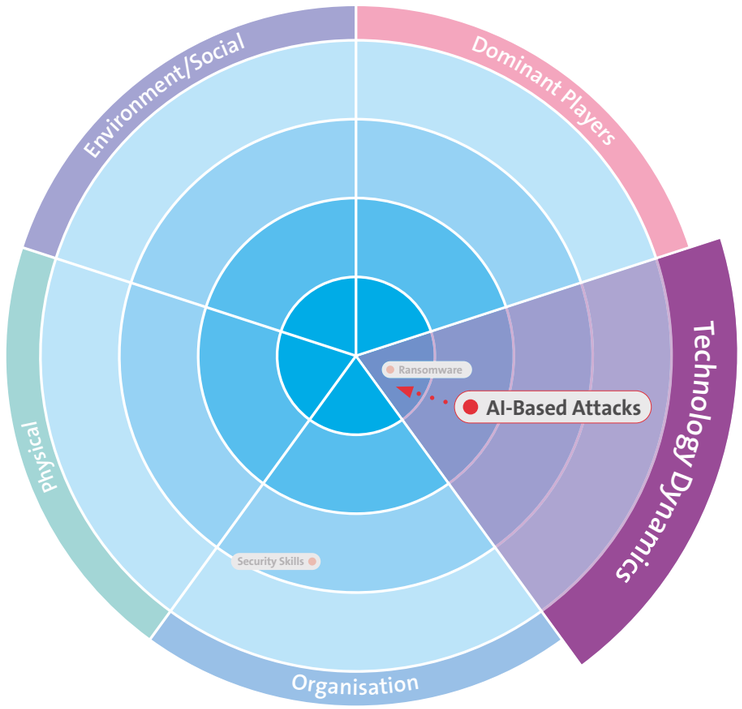
État des lieux – radar des menaces

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 encore faut-il 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.



Défis et tendances :
AI-Based Attacks – la face sombre du progrès technologique



De quoi s’agit-il ?

Les AI-Based Attacks sont des cyberattaques qui ont recours aux technologies de l’intelligence artificielle (IA) pour gagner en performance et en efficacité ou pour contourner les mesures de défense existantes.

Les attaques basées sur l’IA alimentent les conversations depuis longtemps déjà. Ces derniers mois, les outils disponibles ont toutefois fait une véritable avancée. Des outils tels que ChatGPT, le grand modèle de langage d’intelligence artificielle lancé en novembre 2022, illustrent par exemple à quel point les attaques par hameçonnage peuvent être considérablement améliorées ou utilisées pour détecter des failles dans des codes de programme. Le thème de l’IA est actuellement omniprésent dans les médias, et son utilisation abusive pour la création de malwares/codes malveillants et de campagnes de phishing va très certainement s’intensifier dans l’avenir. Nous observons et analysons cette évolution, mais elle ne constitue à l’heure actuelle pas encore un sujet sensible.

Comment ce défi va-t-il évoluer ?

L’un des premiers développements prévisibles est une convergence croissante entre les attaques ciblées et les e-mails de phishing générés par l’IA. À partir d’un historique d’e-mails, une IA de modèle de langage peut créer un scénario convaincant pour poursuivre une conversation et la relier habilement à une attaque de phishing ou d’ingénierie sociale. Une automatisation adaptée permet ainsi de rédiger des campagnes de phishing ciblées avec des e-mails entièrement personnalisés et adaptés au contexte.

À l’avenir, la capacité des IA de modèle de langage pourrait également être utilisée à des fins malveillantes afin d’analyser des codes de programme sur des failles et de programmer des malwares en vue d’exploiter ces failles, y compris les vecteurs d’attaque adaptés. L’expertise dont les hackers ont besoin pour organiser des attaques complexes continue ainsi à diminuer.

En outre, l’évolution rapide des IA génératrices d’images et de vidéos permet toujours de mener des attaques de type « deepfake » et des campagnes de désinformation quasiment impossibles à détecter avec les moyens traditionnels.

Comment relever efficacement ce défi ?

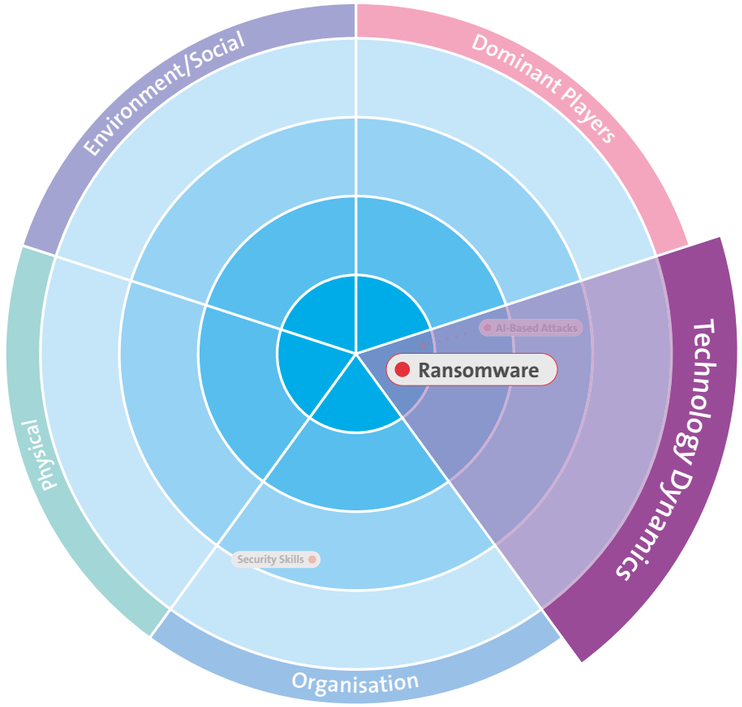
De la même manière que les technologies d'IA peuvent être utilisées par les hackers, l'IA offre également aux défenseurs de meilleures possibilités d'identification et de défense contre les cyberattaques, par exemple pour identifier des textes ou images et vidéos générés par l'IA. Des concepts tels que Zero Trust pour l'accès granulaire et authentifié aux données et aux ressources contribuent à réduire la surface d'attaque des entreprises. Les Security Best Practices établies, telles que l'authentification multifacteur, les DevSecOps, le Vulnerability & Patch Management et la sensibilisation des collaborateurs à la sécurité, contribuent par ailleurs à prévenir les cyberattaques – basées sur l'IA et en général.

« À l'heure où les technologies d'IA connaissent un développement très rapide, il nous faut comprendre qu'elles ne sont pas intrinsèquement bonnes ou mauvaises. Il s'agit plutôt d'un outil qui peut être utilisé à ces deux fins. Le défi consiste à renforcer les processus de défense de manière à pouvoir repousser efficacement les attaques basées sur l'IA, en recourant à l'avenir de plus en plus à une ‹ bonne › IA. »

Florian Leibenzeder
Responsable Swisscom Security Operation Center

Défis et tendances :

Ransomware – chantage au vol de données plutôt qu'un « simple » cryptage



De quoi s'agit-il ?

Le ransomware est un type de malware (logiciel malveillant) qui vise, après avoir infecté un ordinateur, un serveur ou un réseau, à crypter les données de la victime et ainsi à les rendre inutilisables pour celle-ci. Pour obtenir la clé nécessaire au décryptage et à la récupération de ses données, la victime doit impérativement payer une rançon («ransom»). Cette forme d'attaque a déjà été identifiée l'année dernière comme un défi urgent et abordée spécifiquement dans le Cyber Security Threat Radar.

Depuis, de nombreuses entreprises et organisations ont évolué et se sont équipées techniquement, de sorte que le nombre de rançons versées à la suite d'attaques de ransomware tend désormais à diminuer. Les hackers se retrouvent bloqués dès la tentative de cryptage ou les données peuvent être restaurées d'une autre manière. Souvent, les hackers ne parviennent plus à rendre les sauvegardes de données inutilisables. Aussi tentent-ils de plus en plus d'exfiltrer les données avant de lancer une menace de publication. Contrairement aux données cryptées, qui peuvent être récupérées à partir de la sauvegarde, il est quasiment impossible d'empêcher la publication de données exfiltrées sans payer une rançon.

Les motivations des hackers sont financières. Les attaques par ransomware et le vol de données associé constituent pour eux la méthode la plus simple et la plus directe pour tirer un profit financier d'une infrastructure d'entreprise compromise. La somme demandée varie en fonction de la taille de l'entreprise et s'élève à environ 3% de son chiffre d'affaires. Il convient toutefois de noter que le montant de la rançon payée ne constitue qu'une infime partie des coûts engendrés par l'attaque.

S'il n'existe pas de statistiques officielles sur les montants effectivement versés, on estime que le paiement moyen par attaque réussie est de l'ordre de 950 000 francs suisses. Au niveau mondial, le dommage économique causé par les attaques de ransomware devrait dépasser 240 milliards de francs suisses d'ici 2031.

La perspective d'un important gain pécuniaire lors de ces attaques amène de plus en plus les hackers à se professionnaliser. C'est ainsi que le ransomeware « Unicorn » a vu le jour. Selon diverses sources, parmi lesquelles les Conti Leaks, de nombreux hackers disposent de moyens financiers équivalents à ceux de start-up informatiques bien financées.

Ils emploient ainsi parfois des développeurs et des pirates à plein temps et offrent à leurs victimes un « support client » à plusieurs niveaux. Les hackers utilisent des méthodes de développement agiles et ne cessent de développer leur propre modèle d'affaires et leur infrastructure. Ils gèrent par ailleurs leurs programmes Bug Bounty, qui aident les cybercriminels à identifier la présence d'éventuelles failles dans leur propre infrastructure informatique.

Certains groupes de hackers sont en outre très soucieux de leur notoriété. Le groupe Lockbit a ainsi lancé une action de guérilla marketing proposant de se faire tatouer le logo de Lockbit pour la somme de 1000 dollars US. Après cet appel, de nombreuses photos de personnes arborant leur tout nouveau tatouage à l'effigie de Lockbit ont circulé sur Internet.

Comment ce défi va-t-il évoluer ?

Le ransomware reste un sujet d'actualité. Nous prévoyons une nette augmentation de l'extorsion multiple, à savoir la combinaison de plusieurs formes d'attaque telles que le ransomware, le vol de données et le Denial-of-Service, cette forme d'attaque par ransomware étant déjà largement utilisée par les cybercriminels. Les hackers ciblent par ailleurs de plus en plus les fournisseurs de services gérés. L'expérience montre en effet que ces derniers sont prêts à payer une rançon. Leurs clients peuvent en outre également faire l'objet d'une attaque directe afin de générer encore plus de profit.

La spécialisation grandissante des hackers, et donc la complexité de leurs attaques, constitue le futur défi majeur. La plus grande menace émane dès à présent des offres dites de ransomware-as-a-service. Les groupes de ransomware ne pénètrent plus eux-mêmes dans l'entreprise mais louent leur logiciel malveillant de cryptage ainsi que leur infrastructure de serveur et de support à d'autres hackers. La rançon obtenue est ensuite partagée «fraternellement» entre les hackers et le groupe de ransomware. Certains «initial access brokers» sont spécialisés dans l'intrusion dans des entreprises et la vente des possibilités d'accès obtenues.

L'accès initial peut être obtenu au niveau humain ou au niveau de l'infrastructure : au niveau de l'infrastructure, les serveurs accessibles au public sont attaqués par le biais de vulnérabilités déjà connues ou de «zero day exploits». Ces derniers ne sont généralement pas conçus en interne mais achetés auprès d'autres parties.

Le niveau humain est attaqué par certains hackers via des campagnes de (spear) phishing ciblées sur les utilisateurs finaux d'une entreprise. D'autres groupes de ransomware contactent directement les collaborateurs de leurs victimes et tentent de les corrompre via le versement d'importantes sommes d'argent. Ces attaques sur l'infrastructure privée des collaborateurs sont de plus en plus fréquentes, comme le montrent les attaques récentes de LastPass : le réseau domestique d'un administrateur système a dans un premier temps été piraté afin d'y dérober les données d'accès au VPN de l'entreprise.

Comment relever efficacement ce défi ?

La principale mesure de protection consiste à s'orienter sur les Best Practices établies, parmi lesquelles :

- Patch & Vulnerability Management
- utilisation de solutions de sauvegarde modernes de type « air gap », sauvegarde de données régulières (offline) et tests de récupération réguliers
- sensibilisation à la sécurité au sein d'une entreprise
- utilisation d'une authentification multifacteur (MFA) cohérente et protection contre la fatigue MFA
- surveillance globale de la sécurité informatique via Endpoint Detection & Response (EDR)
- équipes de sécurité spécialisées telles que Security Operation Centers (SOC) et Cyber Security Incident Response Teams (CSIRT)
- segmentation du réseau et concept de zones de sécurité
- définition de processus de réponse aux incidents et de communication de crise, formations régulières sur les scénarios de crise possibles.

« Compte tenu de la spécialisation grandissante des hackers, il peut être utile de solliciter des entreprises spécialisées et des équipes d'experts externes pour renforcer sa propre défense. »

Tim Trinkl
Senior Security Analyst & Incident Responder B2B

Défis et tendances :

Security Skills – prévenir une pénurie de personnel qualifié et une perte de savoir

De quoi s'agit-il ?

De nombreuses entreprises, quelle que soit leur taille, sont confrontées au même défi : leurs équipes de sécurité sont en sous-effectifs et/ou débordées. Les entreprises peuvent se trouver submergées par l'augmentation du nombre d'incidents de sécurité, leur difficile hiérarchisation par ordre de priorité et la pénurie de personnel qualifié, ce qui génère un risque accru. Pour résister aux cybercriminels, les entreprises n'ont pas forcément besoin d'un budget plus élevé, mais de collaborateurs qui disposent d'une expertise pertinente en matière de sécurité informatique. Le Cyber Security Threat Radar aborde les deux vecteurs d'attaque suivants : Security Skills et Infrastructure Misconfiguration. En raison d'un manque de compétences et de personnel, les cyberrisques augmentent de manière exponentielle en conséquence de l'exploitation de composants d'infrastructure mal configurés.

En Suisse, les universités, hautes écoles spécialisées et autres instituts de formation ont considérablement étendu leurs offres de cours ces dernières années, mais ne sont pas encore en mesure de satisfaire le besoin élevé en spécialistes de la cybersécurité.

Dans une lutte constante pour les talents, une entreprise pourra s'épuiser dans une quête de main-d'œuvre qualifiée sur un marché qui en est désormais dépourvu. Une autre approche consiste à miser sur ses ressources internes et à investir dans la formation initiale et continue de son propre personnel. Compte tenu de la multiplication des attaques dans les secteurs publics et privés et de leur complexité grandissante, la pénurie mondiale d'experts en cybersécurité se fait déjà lourdement sentir dans de nombreuses entreprises et organisations.

Autre problème : outre le manque de personnel qualifié dans le secteur de la cybersécurité, certains experts en sécurité souhaitent quitter ce domaine. Diverses études indiquent que de nombreux spécialistes de la cybersécurité envisagent de changer d'emploi.

Comment ce défi va-t-il évoluer ?

« Compte tenu des tensions géopolitiques, de l'instabilité macroéconomique, des violations de la protection des données largement médiatisées et des défis croissants dans le domaine de la sécurité physique, le thème cybersécurité est désormais au cœur de l'attention et s'accompagne d'une hausse de la demande en personnel qualifié dans ce secteur », déclare Clar Rosso, CEO de (ISC)² – l'International Information System Security Certification Consortium.

De nombreuses entreprises ont recours à des plateformes de formation pour cyberspécialistes afin de renforcer de manière ciblée la formation initiale et continue en interne. On constate toutefois souvent un manque d'intégration pertinente en termes de formation initiale et continue des collaborateurs, lesquels ont de plus en plus besoin de Security Skills dans leurs processus de développement, d'exploitation et d'innovation. Des questions telles que « Comment rendre la formation initiale et continue suffisamment attrayante pour qu'elle soit adoptée par les collaborateurs techniques et mise en œuvre dans leurs activités quotidiennes » ou « Quelles opportunités en résultent pour un programme de formation actif dans l'environnement spécialisé ? » restent souvent sans réponse. La question du cadre organisationnel adapté se pose par ailleurs également, en parallèle de l'offre de formation proprement dite.

À l'heure actuelle, de nombreux candidats et candidates déplorent régulièrement un manque de considération de la dimension humaine dans le processus de recrutement : longs temps de réaction aux candidatures de la part des entreprises, règles rigides et fourchettes salariales figées, manque de transparence dans le processus de recrutement, pour ne citer que quelques exemples négatifs. On peut donc supposer que certaines des entreprises critiquées appliquent des processus de recrutement non professionnels. Le processus de recrutement doit intégrer un Employer Journey rigoureux, afin que l'entreprise soit durablement perçue comme un employeur attractif par les cybertalents.

Comment relever efficacement ce défi ?

Améliorer les conditions de travail : l'argent ne fait pas le bonheur, mais il y contribue grandement. Outre une rémunération adéquate, les entreprises peuvent également se distinguer en termes d'environnement de travail et de conciliation entre la vie professionnelle et la vie privée. Les possibilités sont nombreuses : horaires de travail flexibles, modèle de travail à domicile, temps de travail réduit pour un salaire identique, etc. Les entreprises doivent analyser et décider elles-mêmes quelles options sont réalistes pour elles.

Adapter ses attentes en fonction des candidats : les postes de débutants ou juniors exigeant à la fois un diplôme universitaire et au moins cinq ans d'expérience sont très éloignés de la réalité. Certaines entreprises doivent revoir leurs attentes, faute de quoi la recherche de collaborateurs de qualité pourrait s'avérer très difficile.

Proposer des formations continues et développer les compétences en interne : des formations initiales et continues allant des formations en cours d'emploi aux enseignements universitaires, en passant par les Bootcamps DevSecOp, les collaborateurs peuvent acquérir les compétences nécessaires en matière de sécurité et ainsi assumer de nouvelles tâches. Pour s'assurer que son personnel profite de cette opportunité, une entreprise doit proposer des incitations correspondantes, par exemple une participation aux frais de formation continue.

Miser sur l'externalisation et réduire le volume de travail : l'externalisation de certaines tâches auprès de prestataires externes et spécialisés permet de réduire le volume de travail dans le domaine de la sécurité. Les prestataires externes peuvent contribuer à combler certaines lacunes dans le savoir-faire de l'entreprise (Knowledge Gap).

« Nous devons impérativement combler la pénurie de talents dans le domaine de la cybersécurité. Pour y parvenir, il nous faut supprimer les barrières à l'entrée, fidéliser les collaborateurs en leur confiant un travail intéressant dans le domaine de la cybersécurité, et veiller à ce qu'ils restent durablement en poste. La formation adaptée aux groupes cibles dans l'environnement DevSecOp interne soutient également activement la ‹lutte pour les talents›. »

Marcus Beyer
Security Awareness Officer

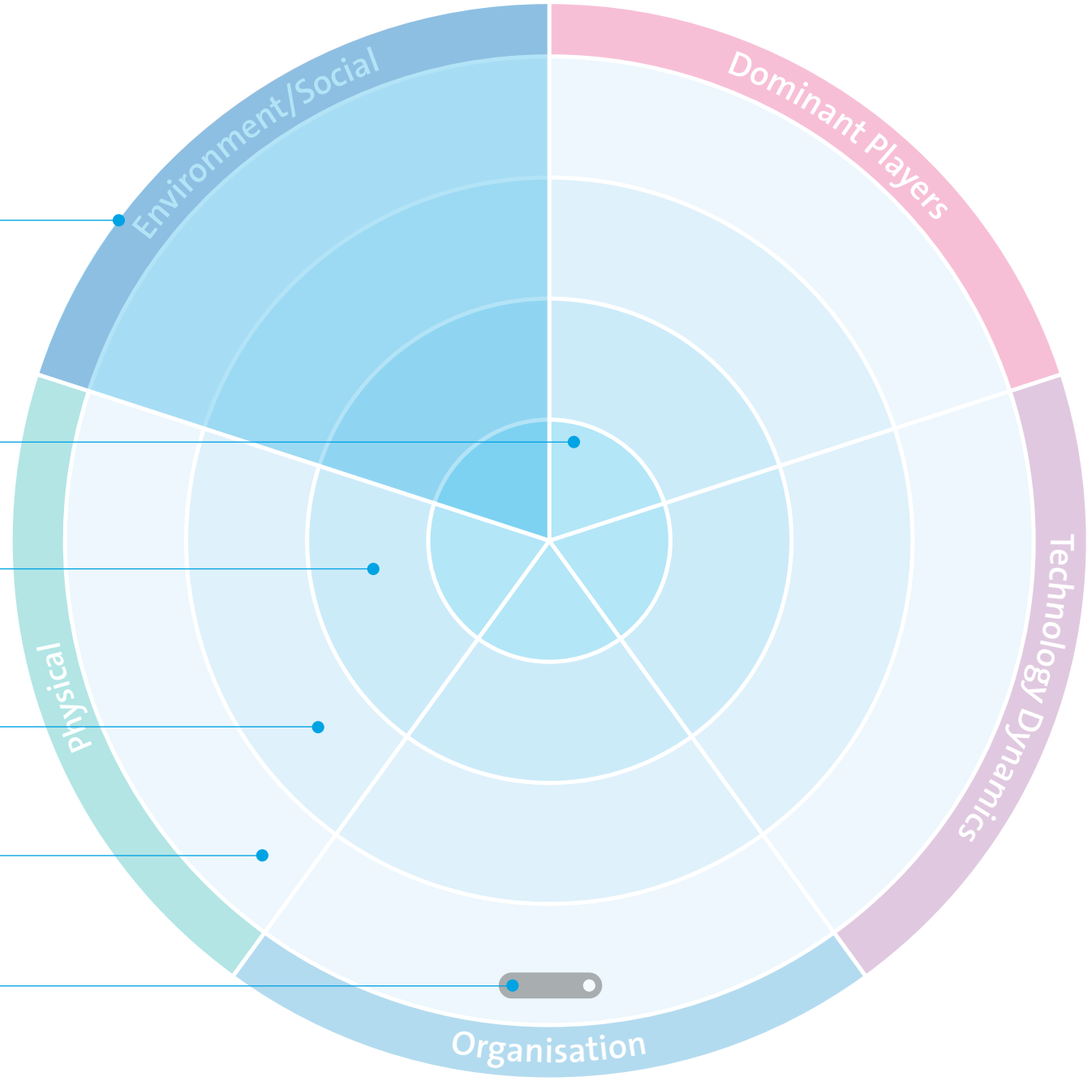
Méthodologie

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

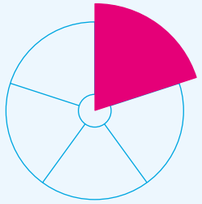
Ces cercles mettent en évidence :

- des **points sensibles** pour les menaces déjà réelles dont la gestion nécessite de mobiliser des ressources relativement importantes.
- des **thèmes clés** pour les menaces déjà survenues 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.
- des **tendances :** détection précoce des menaces qui ne sont pas 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.
- une **observation** pour les menaces qui ne surviendront que dans quelques années. Il n'existe encore aucune mesure concrète pour la gestion de ces menaces.

Par ailleurs, les différentes **menaces** identifiées par ces points suivent une **tendance** dont la criticité est en progression, 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.

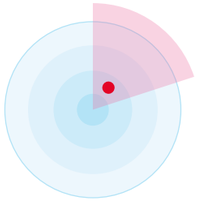


Détails, y compris tendances et comparaison par rapport à l’année précédente



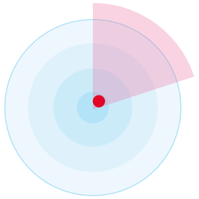
Dominant Players

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



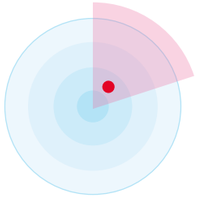
Concentration Data & Cloud Services
La forte centralisation des données dans le cloud induit des risques cumulés. La défaillance d’un service ou d’un service centralisé peut avoir des répercussions dans le monde entier.

▲ Croissant



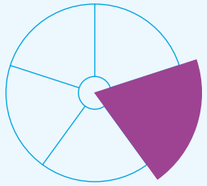
Infrastructure Integrity
Des vulnérabilités peuvent avoir été intégrées délibérément ou par négligence dans des composants essentiels des infrastructures critiques, compromettant ainsi la sécurité du système.

► Inchangé



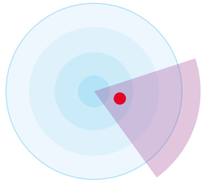
Legacy Protocols
En raison des dépendances logicielles, des protocoles totalement obsolètes et vulnérables (p. ex. NTLMv1, SMBv1, RC4) sont encore utilisés. Quelques applications viennent ainsi compromettre la sécurité d’infrastructures complètes.

► Inchangé



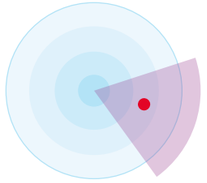
Technology Dynamics

On entend par là les menaces qui découlent d'une innovation technologique fulgurante et profitent de la disponibilité de plus en plus simple et bon marché des supports et de l'expertise informatiques. Conséquence : davantage de surfaces d'attaque, disponibilité accrue des outils correspondants et nouvelles opportunités pour les hackers de créer de nouvelles menaces inhérentes au développement.



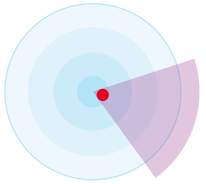
5G Security
La 5G est une technologie mobile encore récente. Son déploiement génère de nombreuses opportunités, mais s'accompagne aussi de menaces encore inconnues.

► Inchangé



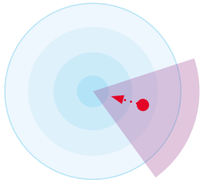
Quantum Computing
Les ordinateurs quantiques peuvent rendre inutiles les procédés cryptographiques actuels car ils sont en mesure de les contourner en très peu de temps.

▼ Décroissant



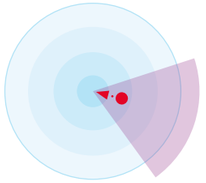
Ransomware
Les données critiques sont cryptées en masse puis (éventuellement) décryptées moyennant le versement d'une rançon.

▲ Croissant



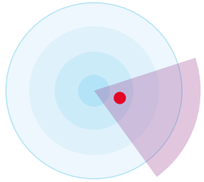
Increased Complexity
La complexité des systèmes, en particulier au-delà des limites des technologies et des entreprises, ne cesse de croître. Les paysages IT se complexifient d'autant plus dans un environnement hybride/multicloud intégrant de nombreux fournisseurs de cloud. L'exposition aux risques augmente d'autant et la recherche d'erreurs devient plus difficile.

▲ Croissant



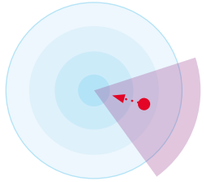
AI-Based Attacks
Les attaques basées sur l'intelligence artificielle (IA) sont plus ciblées et donc plus difficiles à détecter. L'IA les rend plus efficaces sur les vecteurs d'attaque classiques tels que le ransomware, le phishing, le spear phishing, ainsi que sur de nouveaux modes opératoires moins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

▲ Croissant



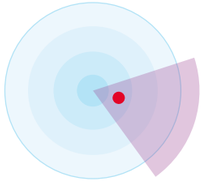
Targeted Attacks
Attaques ciblées et complexes poursuivant un objectif concret. Des personnes clés sont identifiées et ciblées directement ou indirectement (Lateral Movement, méthodes d'ingénierie sociale) afin d'obtenir des informations sensibles ou de causer un maximum de dommages. L'une des principales caractéristiques de ces attaques est la persistance : les hackers agissent le plus longtemps possible sans se faire repérer et un changement est opéré au niveau des canaux d'attaque (du mail au SMS et même au courrier).

► Inchangé



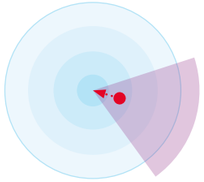
Attaques DDoS
Une attaque par Denial-of-Service (DDos) est une tentative malveillante visant à perturber le trafic de données normal d'un serveur, d'un service ou d'un réseau cible en inondant la cible ou son infrastructure d'un flot de trafic Internet. L'efficacité des attaques DDos repose sur l'utilisation 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 telles que les appareils IoT. Une croissance forte associée à une faible protection des appareils IoT accroît les prises de contrôle potentielles par le biais des botnets.

▲ Croissant



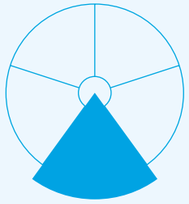
Supply Chain Attacks
Les attaques sur la chaîne d'approvisionnement visent à tirer parti des relations de confiance et d'affaires entre une entreprise et des parties externes. Il peut s'agir de partenariats, de relations avec les fournisseurs ou de l'utilisation de logiciels de tiers.

▲ Croissant



Subscriber Compromise
Des logiciels malveillants se créent un accès aux données privées des utilisateurs mobiles ou sont utilisés pour cibler les infrastructures IT ou de télécommunication. Les attaques de phishing, Smishing, Vishing et MFA-Bypass ciblent les Subscriber Credentials. Des identités numériques complètes sont dérobées et reprises aux cours des attaques consécutives.

▲ Croissant



Organisation

Menaces résultant des changements dans l'organisation ou exploitant les failles qui y sont présentes.

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 tandis que le développement des applications est davantage confié aux Business Units, avec des cycles de release de plus en plus courts. Le contrôlee / la gestion de la sécurité devient ainsi compliqué.

► Inchangé

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

► Inchangé

Digitalisation
L'interconnexion croissante entre le monde réel et le monde virtuel dans la vie privée et professionnelle multiplie l'éventail des vecteurs d'attaque. Le nouveau modèle « New Work » et la transposition opérée dans des environnements de télétravail renforcent également les cyberrisques et la vulnérabilité de l'infrastructure IT en raison des équipements terminaux non sécurisés.

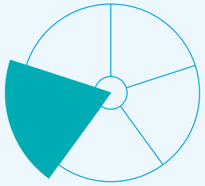
► Inchangé

Security Skills
La complexité des cyberattaques et la progression de la numérisation rendent les Security Skills et le recours à des cyberprofessionnels indispensables dans l'organisation. Une menace de « Downskilling », à savoir le désapprentissage des connaissances, liée à l'automatisation dans l'informatique peut générer de nouveaux vecteurs d'attaque, par exemple si les installations SCADA ne peuvent plus être utilisées et entretenues par le personnel qualifié.

▲ Croissant

Infrastructure Misconfiguration
Exploitation de composants de l'infrastructure mal configurés et/ou de vulnérabilités identifiées et corrigées tardivement. L'automatisation renforcée des processus d'exploitation techniques aura des conséquences plus importantes en cas d'attaques efficaces ou de configurations erronées.

▲ Croissant



Physical

Ce terme désigne les attaques sur l'infrastructure du cyberespace et qui causeront de plus en plus de dommages dans le monde physique. Il inclut également les menaces émanant de l'environnement physique et généralement davantage axées sur des cibles physiques.

Device Theft
Le vol ou toute autre forme de perte d'équipements terminaux tels que les smartphones, les ordinateurs portables, mais aussi de composants informatiques importants, peut entraîner une perte de données ou compromettre la disponibilité des services IT.

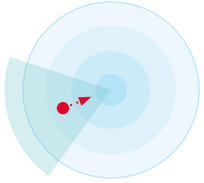
▼ Décroissant

Energy Instability
Attaques sur des infrastructures critiques telles que celles des exploitants du réseau électrique. La sûreté de fonctionnement est essentielle et la Business Continuity alimente de plus en plus le débat sur la cyberrésilience. La pénurie d'électricité, le blackout (panne générale d'électricité) ou même blue-out (défaillance générale de l'alimentation en eau), entre autres, sont des points importants. Selon les médias, les infrastructures critiques sont nettement plus vulnérables aux cyberattaques.

▲ Croissant

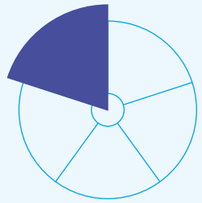
Unsecure IoT/OT Devices
Qu'il soit déployé dans des technologies opérationnelles (OT) pour la surveillance et la gestion de processus, des appareils et infrastructures physiques ou dans des appareils IoT, l'Internet des objets est omniprésent. Des tâches très variées – des plus simples au plus complexes – y sont exécutées, des applications de Home Entertainment à la surveillance d'infrastructures critiques (CI), en passant par le pilotage de robots dans les ateliers de production. Les appareils faiblement protégés, quelle que soit leur nature, peuvent être compromis et sabotés. Ils peuvent ainsi voir leurs propres fonctions restreintes, par exemple leur disponibilité ou l'intégrité des données.

► Inchangé



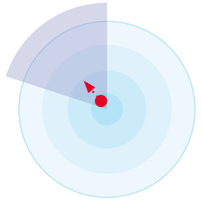
Targeted Sabotage
Attaques ciblées contre des infrastructures, des installations d'approvisionnement et des connexions, qui peuvent restreindre de manière considérable le fonctionnement d'Internet. Le sabotage ciblé des câbles à fibre optique sensibles se développe actuellement et constitue un danger qui doit être surveillé. Compte tenu de la difficile mise en œuvre des contre-mesures, il convient de miser sur une détection rapide et sur des solutions alternatives.

▲ Croissant



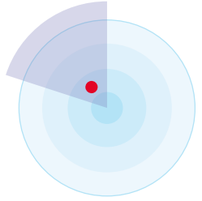
Environment/Social

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.



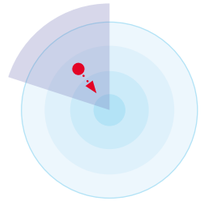
Security Job Market
Les besoins énormes en professionnels de la sécurité sont très difficiles à satisfaire. Il en résulte une perte de savoir-faire dans la lutte contre des attaques de plus en plus complexes et intelligentes.

► Inchangé



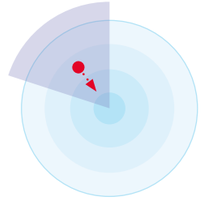
Digital Identity
Les identités numériques personnelles certifiées peuvent être usurpées ou volées, par exemple dans le but de conclure des contrats au nom de tiers.

▲ Croissant



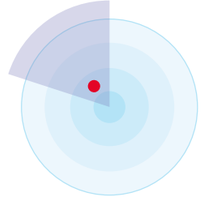
Disinformation & Destabilisation
La diffusion intentionnelle d'informations erronées peut entraîner une déstabilisation économique et sociale. Son utilisation ciblée dans les scénarios de crise, y compris via le cyberespace, se développe de plus en plus.

▲ Croissant



Political Influence
Les forces politiques peuvent influencer les décisions d'ordre technologique ou économique, par exemple 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 individus. Les décisions sont de plus en plus souvent confiées à des systèmes autonomes. Les données des « Big Data Lakes » sont utilisées de manière ciblée à des fins de désinformation, de fake news, d'analyses sociétales et psychosociales, ainsi que pour créer des modèles de mouvement. Ce dernier point induit une violation de la sphère privée.

► Inchangé

Conclusion

Le concept de «Security by Design», qui consiste à prendre en compte et à intégrer de manière systématique les aspects de la sécurité dans toutes les phases du développement logiciel – à savoir de l'idée au lancement et à l'utilisation des produits –, ne fait pas que gagner en importance : il constitue l'épine dorsale d'une cybersécurité stable au sein des entreprises et des organisations.

En association avec une approche de la sécurité axée sur l'humain, autrement dit la sensibilisation pertinente des collaborateurs aux questions de sécurité, les entreprises peuvent renforcer leur protection et se préparer aux situations de crise imminentes.

Si l'on prend le temps d'analyser les risques potentiels, on constate rapidement qu'il existe toutes sortes de scénarios de crise susceptibles de mettre une entreprise en difficulté. Ces dangers doivent être abordés et analysés. La politique de l'autruche n'est assurément pas une option durable et n'est pas recommandée.

La gestion des cyberrisques est une mission difficile. Il est toutefois impératif de toujours garder un œil sur le dispositif de risque et d'avoir conscience des risques généraux en matière de cybersécurité, y compris des risques de défaillances associés.

Lorsque les schémas de pensée, concepts et technologies existants n'apportent plus de réponses satisfaisantes, il convient d'essayer, d'introduire et de mettre en place de nouveaux modes de pensée, de nouvelles approches, de nouveaux rôles et de nouvelles technologies. Cette démarche requiert une vision éclairée, une stratégie, du courage et une bonne dose de persévérance.

Cet investissement dans l'avenir constitue donc un énorme défi pour les entreprises. Réexaminer et repenser les schémas de pensée et processus existants au sein des départements informatiques est une démarche souvent très difficile qui exige beaucoup de travail et de patience. Ces changements sont cependant parfois indispensables pour protéger son entreprise contre les menaces. Car il ne fait aucun doute que les cyberrisques évoluent à un rythme très rapide. Seules les entreprises qui suivent le rythme et disposent d'une sécurité agile pourront maintenir une protection efficace contre la cybercriminalité.

« En période d'incertitude, l'interaction entre les personnes, les processus et les technologies constitue la base de la résilience et de la stabilité des entreprises. »

Remarques

Impressum

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	Apostroph Bern AG
Copyright	© Mai 2023 by Swisscom (Suisse) SA, Group Security, Alte Tiefenaustrasse 6, 3048 Worblaufen, swisscom.ch
Édition	OK DIGITALDRUCK AG, Zurich
Tirage	200 exemplaires

Swisscom montre la voie et développe des innovations sur lesquelles on peut s'appuyer en toute confiance. En tant qu'« Innovators of Trust ».

Tu recherches un emploi dans le secteur de la sécurité chez Swisscom? Alors jette un coup d'œil ici et dépose ta candidature : swisscom.com/securityjobs

Tu trouveras de plus amples informations sur nos produits, nos services et notre engagement pour la sécurité en Suisse sous swisscom.ch/fr/about/securite.html

#BeTheStrongestLink