swisscom

Cybersecurity Threat Radar 2025

La cyberrésilience face aux défis géopolitiques

Table des matières

Cybersecurity Threat Radar

La cyberrésilience face aux défis géopolitiques

Dans le monde de la cybersécurité, qui évolue rapidement, il est indispensable pour les entreprises de revoir et d'adapter en permanence leurs stratégies de défense. Les cybercriminels sont de plus en plus habiles et changent constamment leurs méthodes d'attaque, ce qui exige de trouver des solutions innovantes et flexibles pour se défendre. Dans le présent Cybersecurity Threat Radar, nous vous donnons un aperçu des thématiques centrales et défis actuels dans le domaine de la cyberrésilience auxquels nous nous consacrons intensivement chez Swisscom.

Dans la lutte contre les cybermenaces concrètes, nous donnons la priorité au développement ciblé de nos Detection & Response Capabilities. Cela s'appuie sur les enseignements pratiques tirés des exercices Red Team, des expériences de réponse aux incidents et des informations actuelles de Threat Intelligence.

On ne saurait trop insister sur l'importance des pratiques de sécurité de base, souvent qualifiées de «cyberhygiène». Ces bases constituent le fondement d'une stratégie de cybersécurité fiable et sont décisives pour se défendre efficacement contre un grand nombre de menaces. Nous attachons une grande importance à l'implémentation et à l'amélioration continue de ces mesures de sécurité de base. Cela inclut également des mises à jour de sécurité régulières, des méthodes d'authentification fortes et la formation régulière de nos collaboratrices et collaborateurs afin de promouvoir la sensibilisation générale à la sécurité.

L'évolution de la situation géopolitique place les entreprises face à de nouveaux défis dans le domaine de la cybersécurité. L'influence croissante des milliardaires de la technologie, les changements politiques en Europe et le durcissement des réglementations requièrent une stratégie de sécurité flexible et anticipative.

Pour relever ces défis, Swisscom mise aussi de manière ciblée sur une étroite collaboration avec des partenaires nationaux et internationaux. Notre Computer Security Incident Response Team (CSIRT) échange régulièrement avec d'autres exploitants d'infrastructures critiques et prestataires de services de sécurité afin d'avoir une vue d'ensemble de l'état actuel des menaces.

Si nous nous projetons vers l'avenir, nous constatons que nous serons confrontés à de nouveaux développements technologiques qui recèlent à la fois des opportunités et des risques. Nous avons par exemple le cas de l'IA générative utilisée dans la cybersécurité, qui nécessite une approche équilibrée: d'une part, nous devons utiliser cette technologie pour améliorer notre détection des menaces et, d'autre part, nous devons nous prémunir contre son utilisation abusive par les cybercriminels.

Le concept de l'architecture «Zero Trust» gagne par ailleurs en importance. Il remet systématiquement en question la confiance inhérente à l'infrastructure informatique et vérifie chaque accès individuel. Ainsi, les entreprises augmentent non seulement leur sécurité, mais font aussi avancer la transformation numérique.

En résumé, le renforcement de la cyberrésilience est un processus continu qui nécessite de la vigilance, de la flexibilité ainsi qu'une capacité d'innovation. Chez Swisscom, nous essayons de miser sur une approche globale qui tient tout autant compte des menaces réelles, des pratiques de sécurité de base et des technologies d'avenir. Ce n'est qu'ainsi que nous pourrons faire face efficacement aux diverses cybermenaces et façonner un avenir numérique sûr pour nos clientes et nos clients ainsi que nos partenaires.

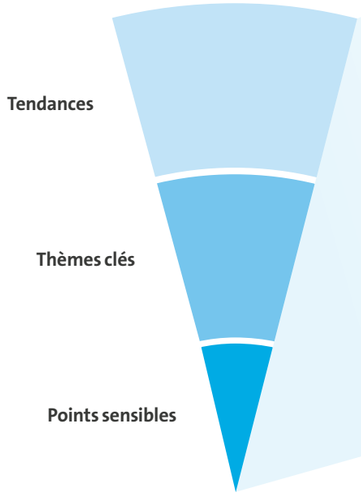
« L'évolution de la situation géopolitique place les entreprises face à de nouveaux défis dans le domaine de la cybersécurité. L'influence croissante des milliardaires de la technologie, les changements politiques en Europe et le durcissement des réglementations requièrent une stratégie de sécurité flexible et anticipative. »

Marco Wyrsch
Head of Group Security & Chief Security Officer

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-là 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 saisir de façon systématique. Pour faire le point sur le niveau de menace et son évolution, nous nous appuyons sur le Cybersecurity Threat Radar.



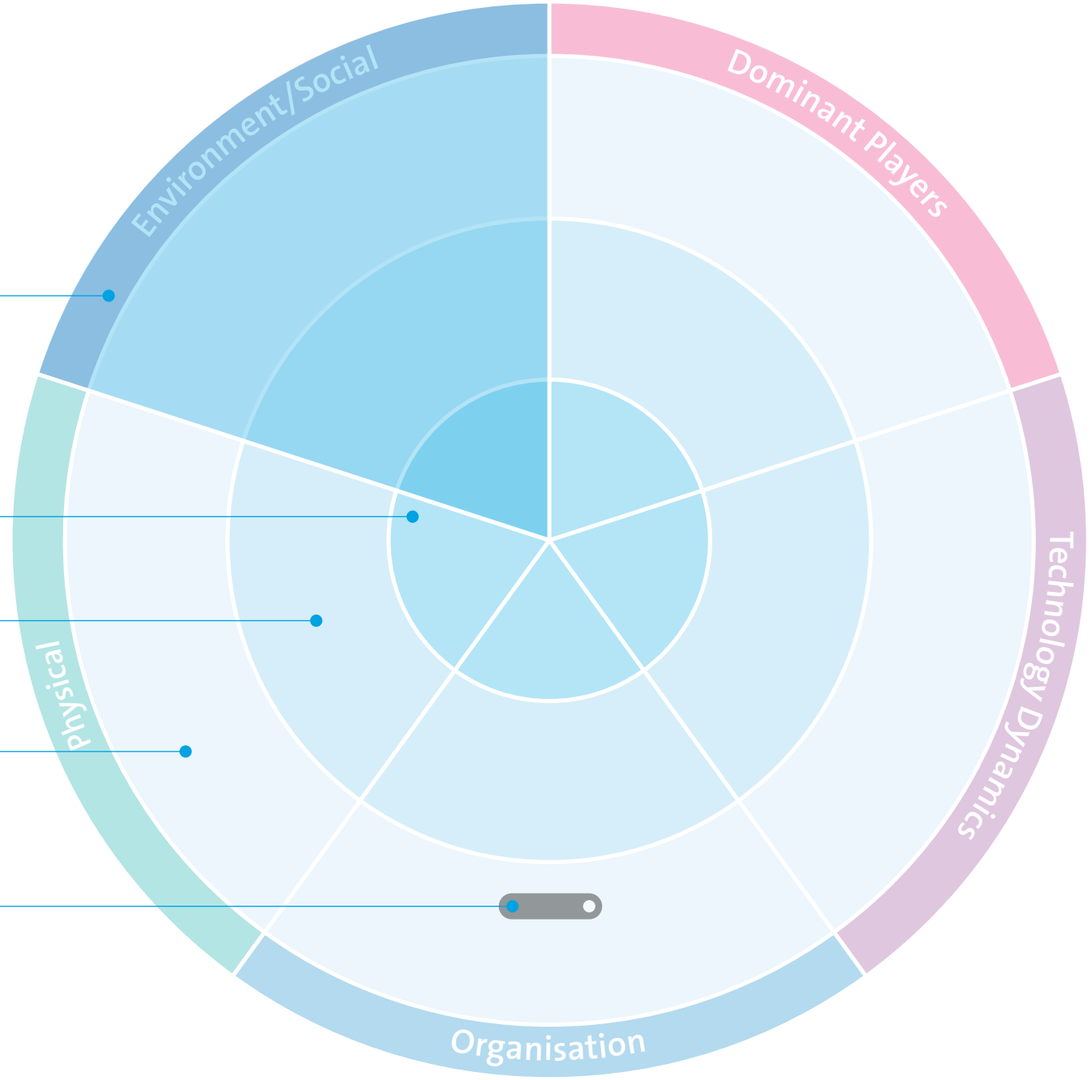
Méthodologie

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 trois 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.

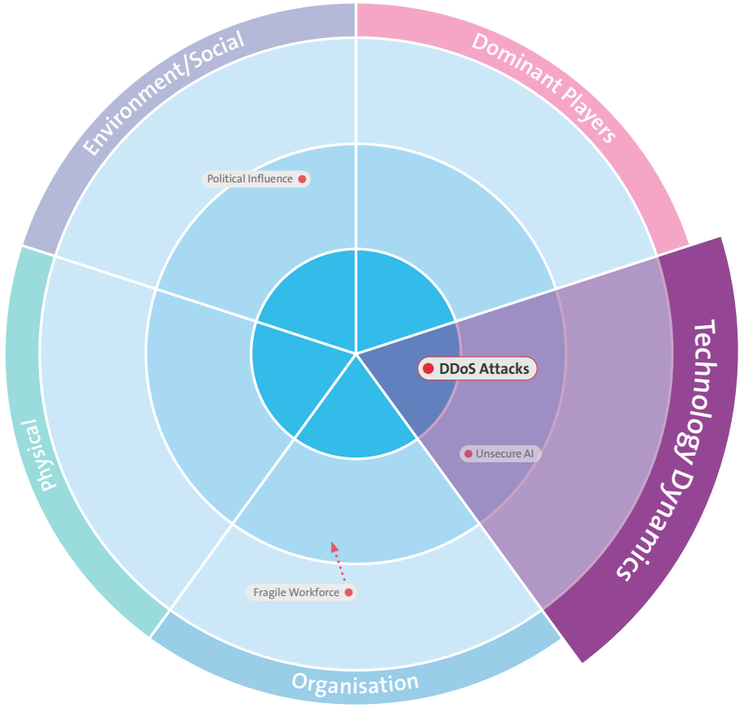
Ces cercles mettent en évidence:

- 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.

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.



Attaques DDoS: «Détruisez ce qui vous détruit»



Dans un contexte commercial de plus en plus numérisé, les attaques DDoS (Distributed Denial of Service) représentent une menace sérieuse et croissante pour les entreprises. Ces attaques visent à rendre inaccessibles des services en ligne, des sites Internet ou des réseaux par une avalanche de trafic de données, ce qui peut avoir de lourdes conséquences pour les entreprises concernées. L'attaque DDoS contre Swisscom en août 2024 a même attiré l'attention des médias.

Le nombre d'attaques DDoS[1] ciblées réalisées contre des prestataires de services financiers, des administrations publiques, des fournisseurs d'hébergement, des fournisseurs d'énergie, des opérateurs de télécommunications, des boutiques en ligne, etc. a doublé en Suisse entre 2023 et 2024. Selon le NETSCOUT Cyber Threat Horizon Report, 56 200 attaques DDoS de toutes sortes ont été enregistrées en 2023 contre environ 107 000 en 2024. Au cours de l'année écoulée, il y a eu 293 attaques par jour. Le secteur suisse des télécommunications a également été pris pour cible.

Scénario de menace

L'exécution d'attaques DDoS devient de plus en plus simple. Sur Internet, les places de marché criminelles proposent depuis des années de réaliser des attaques DDoS contre une somme modique (à partir de 15 dollars américains par mois), comme une sorte de «Cybercrime as a Service», ou comme test de résistance. Et ces offres se multiplient. Il faut donc s'attendre à ce que le nombre d'attaques DDoS continue d'augmenter.

De plus, grâce à l'essor de l'intelligence artificielle (IA), il devient de plus en plus facile pour les cybercriminels de rendre leurs attaques DDoS plus dangereuses et plus efficaces.

Pour la gestion des risques, la protection des immobilisations incorporelles telles que les données, les réseaux ou la propriété intellectuelle passe donc au premier plan. Une sécurité informatique insuffisante doit être considérée comme un risque pour l'entreprise si des unités entières peuvent être paralysées par des cyberattaques.

[1] Une attaque DDoS (Distributed Denial of Service) est une forme de cyberattaque au cours de laquelle les adresses IP accessibles publiquement sur Internet sont inondées de manière ciblée d'un très grand nombre de demandes provenant d'ordinateurs, de téléviseurs, de webcams et de nombreux autres appareils IP infectés. L'objectif des assaillants est de mettre hors ligne le plus longtemps possible les services électroniques accessibles via les adresses IP attaquées.

Pourquoi les attaques DDoS sont-elles dangereuses pour les entreprises?

1. **Interruption de l'exploitation:** les attaques DDoS peuvent perturber considérablement le fonctionnement normal de l'entreprise en paralysant des sites Internet, des services en ligne ou des réseaux internes.
2. **Pertes financières:** les entreprises, en particulier celles qui dépendent fortement du trafic en ligne, peuvent subir d'importantes pertes de chiffre d'affaires si leurs services ne sont pas disponibles.
3. **Atteinte à la réputation:** des pannes répétées ou de longue durée peuvent ébranler la confiance des clientes et clients dans la fiabilité et la sécurité de l'entreprise.
4. **Coûts de remise en état élevés:** les coûts de remise en état des services et du renforcement de l'infrastructure de sécurité après une attaque peuvent être considérables.
5. **Manœuvre de diversion:** les attaques DDoS peuvent servir de diversion pour détourner l'attention d'autres activités malveillantes, telles que le vol de données.

Dommages potentiels

Une entreprise peut subir un préjudice financier avant même qu'une attaque DDoS ne se produise. L'Office fédéral de la cybersécurité (OFCS) fait état de tentatives d'extorsion sur Internet, durant lesquelles des entreprises sont menacées d'attaques DDoS si elles ne sont pas prêtes à payer la somme demandée. Les maîtres-chanteurs n'ont pas toujours la capacité réelle de mettre à exécution une attaque DDoS, mais ils bluffent et espèrent que la seule menace suffira à obtenir une rançon.

Mesures de protection

Les attaques DDoS représentent une menace sérieuse en constante augmentation pour les entreprises de toutes tailles. Avec la numérisation croissante et une dépendance accrue aux services en ligne, disposer de mesures de protection solides va continuer de gagner en importance. Les entreprises doivent agir de manière proactive pour protéger leur infrastructure numérique et assurer ainsi la continuité de leurs activités. Comme on le constate aussi dans d'autres domaines, «mieux vaut prévenir que guérir».

« Les opportunités et les risques sont une constante sur Internet. Mais vous pouvez influencer consciemment ces deux paramètres. Attendre et espérer ne jamais être victime d'une attaque DDoS est définitivement déconseillé. Prenez des mesures ciblées et mettez-les en œuvre le plus rapidement possible. »

Beat Hunziker
Senior Product Manager Business Internet & Security Services

Les investissements dans des solutions complètes de protection contre les attaques DDoS, la formation continue et le développement de plans de réponse flexibles sont essentiels pour relever les défis d'un cyberenvironnement en constante évolution. Seule une approche globale et prévoyante peut permettre aux entreprises de renforcer leur capacité de résister aux attaques DDoS et limiter les dommages potentiels.

En fin de compte, la protection contre les attaques DDoS ne représente pas seulement un défi technique, c'est une nécessité stratégique pour toute entreprise moderne. La capacité à contrer efficacement de telles attaques constitue de plus en plus un avantage concurrentiel décisif dans l'économie numérique.

« La menace des attaques DDoS est omniprésente. Celles-là peuvent non seulement causer des dommages financiers, mais également nuire à la réputation d'une entreprise. »

Reto Friedl
Product Manager Managed Security Services

Équipe fragile: «Lorsque la pression devient trop forte»

Les équipes de cybersécurité subissent une énorme pression. Le paysage des menaces évolue constamment, allant des attaques par hameçonnage sophistiquées aux manipulations par deepfake en passant par les attaques ciblées de ransomware. Parallèlement, la complexité des infrastructures informatiques augmente, tandis que les surfaces d'attaque se multiplient grâce aux modèles de travail hybrides et aux appareils connectés.

Plus de 10 000 alertes par jour: pourquoi est-ce problématique?

Les messages d'alerte, les analyses d'incidents et l'évolution rapide des scénarios de menace conduisent à une «fatigue d'alarme», un état dans lequel les signaux d'alerte ne sont plus suivis avec l'attention requise parce que le système est surchargé. Une étude de Devo Technology montre que 42% des équipes de sécurité informatique ignorent régulièrement les alertes, car elles sont trop nombreuses et brouillonnes. L'inattention et les mauvaises décisions qui en résultent représentent un risque considérable pour la sécurité.

Le défi: gérer la charge cognitive et émotionnelle

Ces défis ont de graves conséquences pour les collaboratrices et collaborateurs: le stress chronique nuit non seulement à la santé, mais aussi aux performances de travail. Une récente étude sectorielle menée par SoSafe montre que jusqu'à 57% des professionnels de la sécurité dans la région DACH souffrent de burn-out. Les principales raisons sont les suivantes:

- **Forte pression sur la performance:** détection permanente des menaces et défense comme activité principale.
- **Surcharge de travail et heures supplémentaires:** le temps de travail normal est souvent dépassé.
- **Formation insuffisante:** l'absence de formation continue est source d'insécurité.
- **Manque de personnel:** le manque de main-d'œuvre qualifiée augmente encore la charge de travail.

Il en résulte en outre un «Cognitive Overload», c'est-à-dire une surcharge mentale, lorsque le cerveau doit lutter avec trop d'informations, de tâches et de décisions en même temps. Les distractions, le travail multitâche et le stress permanent aggravent le problème, et il devient de plus en plus difficile de prendre des décisions fiables. Les conséquences typiques sont les suivantes:

- Réactions différées aux menaces
- Erreurs de configuration et failles de sécurité
- Communication limitée en cas de stress
- Burn-out et forte fluctuation

En conséquence, ignorer la charge mentale, c'est risquer non seulement la sécurité de l'entreprise, mais aussi la santé des personnes qui la protègent.

Stratégies pour un travail sûr, efficace et équilibré

Une approche durable aborde les domaines principaux suivants: le leadership, la dynamique d'équipe et les compétences clés.

Les cadres comme barrière de sécurité contre la surcharge

Les cadres jouent un rôle essentiel en donnant l'exemple d'un travail vigilant, en menant des entretiens réguliers et en faisant de la santé mentale une priorité. Ils aident à créer des structures permettant de se concentrer et à limiter les interruptions inutiles. Parallèlement, ils peuvent favoriser la sécurité psychologique et éviter la surcharge de travail par des mesures préventives.

Les responsables RH devraient eux aussi être impliqués, par exemple en encourageant la gestion de la santé au travail. Il en résulte une culture d'entreprise dans laquelle la résilience mentale est considérée comme un facteur de réussite.

Sécurité psychologique: la base d'un travail d'équipe efficace

Une équipe de cybersécurité résiliente a besoin de sécurité psychologique. Partager les connaissances, parler ouvertement des erreurs et apporter un soutien collégial dans les situations de stress renforce la capacité de résistance de l'équipe. Les facteurs de réussite sont les suivants:

- **Promouvoir l'intelligence émotionnelle:** prise de conscience et soutien au sein de l'équipe.
- **Établir des programmes de mentorat:** échange d'expériences et développement individuel.
- **Faire appel aux groupes de pairs:** réfléchir aux bonnes pratiques et aux défis psychiques.

Compétences clés pour des équipes de cybersécurité résilientes

L'agilité mentale s'entraîne, et la maîtriser permet non seulement de réduire les erreurs, mais aussi le stress. La capacité de réagir rapidement aux menaces tout en prenant des décisions réfléchies est essentielle:

- L'agilité mentale permet de passer facilement de la pensée analytique à l'action rapide.
- La clarté mentale garantit que les informations pertinentes sont évaluées, même sous pression, au lieu de réagir de manière impulsive.

En quoi cela aide-t-il à lutter contre le stress?

Les professionnels de la cybersécurité doivent s'entraîner à passer consciemment d'un système de pensée à l'autre afin d'éviter les mauvaises décisions. En cas de forte pression ou de surcharge cognitive, c'est souvent la pensée intuitive, rapide, mais sujette aux erreurs qui prend le dessus, un concept que le psychologue Daniel Kahneman décrit comme le «système 1». Le «système 2», analytique et réfléchi, aide en revanche à prendre des décisions plus précises, mais nécessite davantage de ressources cognitives.

- Passer consciemment du système 1 au système 2 permet de prendre des décisions plus fiables et de réduire le stress.
- Une gestion ciblée des systèmes de pensée évite les réactions impulsives et accroît la capacité de contrôle dans les situations critiques.
- Moins de surcharge cognitive réduit la pression mentale et améliore à long terme la résistance au stress.

« Slight destroyers: les ignorer, c'est compromettre la sécurité. »

Anja Peter
CEO & Co-Founder Human Empowerment Center AG

Focalisation et régénération

Travailler en permanence en mode de crise n'est viable ni sur le plan mental, ni sur le plan physique. Quand on passe constamment d'une tâche à l'autre et qu'on travaille sans faire de pauses, on épuise ses ressources cognitives. Des études montrent que la surcharge sensorielle permanente due au travail multitâche et aux interruptions constantes réduit considérablement la capacité de concentration et de résolution des problèmes. À l'inverse, une régénération ciblée augmente la résistance à long terme. Cela inclut:

- **Deep Work et Time Blocking:** des phases ciblées de travail sans perturbation afin d'utiliser efficacement les ressources cognitives.
- **Focus Sprints:** des phases de travail intensives avec des pauses clairement définies pour éviter la fatigue mentale.
- **Micropauses et techniques de respiration:** soulagement ciblé du système nerveux pour améliorer la concentration et la gestion du stress.

Alterner consciemment entre concentration et repos permet de préserver ses performances mentales. Travailler en pleine conscience signifie ne pas se laisser guider par les distractions, mais décider de manière ciblée sur quoi porter son attention. Sans ce contrôle conscient, le cerveau reste en permanence en mode d'alerte, ce qui entraîne à long terme un épuisement et de mauvaises décisions.

Conclusion: une cybersécurité durable commence par des équipes résilientes

Une équipe de sécurité résiliente est décisive pour la réussite en matière de cybersécurité. Réaliser durablement de hautes performances nécessite de faire preuve de résilience et de soutenir les personnes se trouvant derrière les écrans.

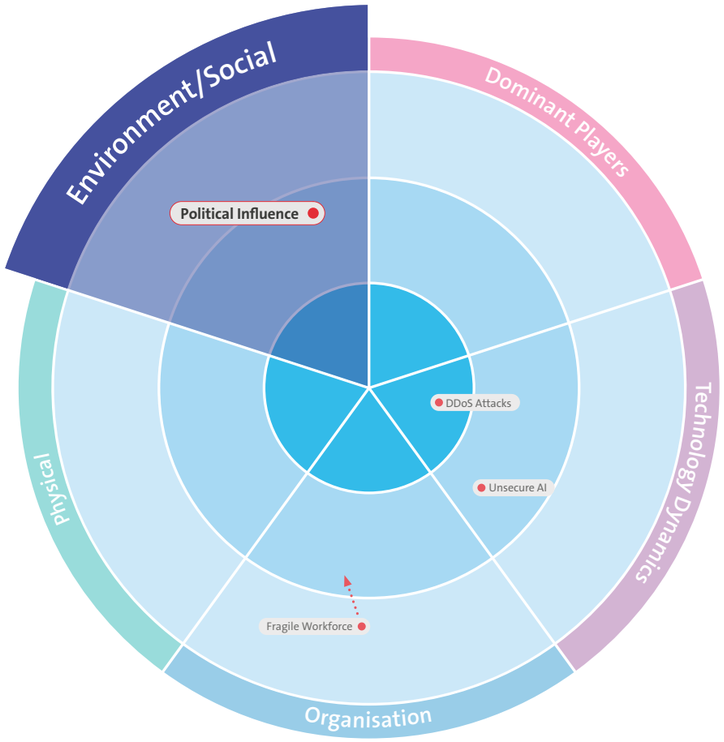
L'objectif doit être de créer un environnement dans lequel la pleine conscience, la sécurité psychologique et la gestion active du stress vont de soi. Ce n'est qu'ainsi que l'on pourra désamorcer la surcharge cognitive, la fatigue d'alarme et les «slight destroyers of strong cybersecurity», beaucoup montrés du doigt. De cette manière, l'entreprise ou l'organisation gagne non seulement un personnel motivé et en bonne santé, mais augmente également à long terme sa capacité de résistance globale aux cyberattaques. C'est la seule façon de constituer une équipe de travail forte et résistante, capable de relever les défis de demain.

En fin de compte, toute stratégie de sécurité dépend des personnes qui la mettent en œuvre. Une main-d'œuvre résiliente est la clé d'une cybersécurité robuste, pour les entreprises et pour la santé de ceux qui les protègent.

« Une équipe fragile réagit, une équipe résiliente agit. »

Martina Novo
Tribe Chief Security

Influence politique: «Plus de sécurité = plus de directives?»



Nous vivons une époque de profonds bouleversements, où les évolutions géopolitiques, économiques et technologiques peuvent engendrer des incertitudes générales. Cette tendance est appelée «Age of Disorder», soit l'«ère des troubles». En ces temps difficiles, il faut de la fiabilité, de la stabilité et du leadership. Les entreprises et l'État sont soumis à une pression considérable, car les menaces hybrides, telles que la désinformation ciblée, les cyberattaques et les actes de sabotage, visent à ébranler la confiance dans les institutions politiques, à attiser les craintes de la société et à affaiblir la cohésion sociale.

Les entreprises et les États doivent donc se concentrer sur une transformation numérique durable afin de pouvoir garantir la stabilité économique. Les stratégies de résilience, telles que la diversification et la cybersécurité, sont essentielles pour atténuer les crises futures. L'«ère des troubles» exige d'agir en amont pour anticiper les changements disruptifs et les gérer activement. Seuls ceux qui font avancer les innovations avec flexibilité et participent courageusement au changement peuvent s'affirmer face à la concurrence mondiale.

La transformation numérique présente non seulement des défis, mais aussi de nombreuses opportunités. Les entreprises capables de s'adapter rapidement aux nouvelles réalités et de développer des solutions innovantes se démarqueront avec succès face à la concurrence mondiale. Cela nécessite toutefois une culture de l'ouverture et de l'apprentissage continu, dans laquelle les erreurs sont considérées comme des opportunités d'apprendre et où les nouvelles idées sont encouragées.

Dans cet environnement qui évolue rapidement, les entreprises sont confrontées au défi de garantir la cybersécurité tout en restant innovantes. Des réglementations telles que NIS2, DORA, le Cyber Resilience Act (CRA), des normes telles que ISO 27001 ou encore des directives nationales, comme la loi suisse sur la sécurité de l'information (LSI), doivent y contribuer.

Mais la multiplication des réglementations s'accompagne aussi des risques d'un «paradoxe réglementaire»: les entreprises et les organisations se croient dans une sécurité apparente et donnent la priorité au fait de remplir les exigences réglementaires au lieu de réfléchir à la sécurité de manière globale.

Pour contrer cette tendance, les entreprises doivent trouver un équilibre entre la conformité et une gestion proactive de la sécurité. Elles doivent adopter une approche axée sur les risques en se concentrant sur les menaces réelles plutôt que sur le simple respect des réglementations. Des examens réguliers de la situation en matière de sécurité au-delà des exigences réglementaires sont nécessaires pour pouvoir réagir de manière flexible aux nouvelles menaces. Il est essentiel que les organisations assument leur propre responsabilité en matière de sécurité et ne s'appuient pas uniquement sur des directives externes. Ce n'est qu'en combinant le respect des réglementations, une gestion de la sécurité forte et autogérée ainsi qu'une culture de la sécurité durable et efficace que les entreprises peuvent devenir résilientes face aux cybermenaces.

Dans un monde en constante évolution, il est indispensable que les entreprises et les États ne se contentent pas de réagir aux menaces actuelles, mais prennent également des mesures proactives pour faire face aux défis futurs. Une adaptation et une amélioration continues des stratégies de sécurité, une collaboration étroite entre les différents acteurs et une bonne compréhension de la situation sont cruciales. Ce n'est qu'en conjuguant nos efforts que nous pourrons façonner un avenir numérique sûr et stable.

La résilience et la disponibilité des services et des infrastructures sont également essentielles. Les entreprises doivent veiller à ce que leurs systèmes restent opérationnels même en temps de crise et puissent être rétablis rapidement. Une collaboration étroite entre les différentes unités et une communication claire sur les responsabilités et les mesures à prendre en cas d'incident sont alors nécessaires.

Le contrôle des processus numériques clés et des infrastructures qui les rendent possibles est décisif pour garantir la souveraineté numérique. Les entreprises doivent s'assurer de garder le contrôle sur leurs données et leurs systèmes et de ne pas dépendre de fournisseurs externes. Cela nécessite une planification et une mise en œuvre minutieuses des mesures de sécurité ainsi qu'une surveillance et une adaptation continues aux nouvelles menaces. Les entreprises doivent s'assurer que leurs systèmes et leurs données sont protégés contre tout accès non autorisé et qu'elles sont en mesure de réagir rapidement et efficacement aux incidents de sécurité.

Souveraineté numérique

L'accès à des informations dignes de confiance est un autre aspect important de la souveraineté numérique. Les entreprises et les gouvernements doivent s'assurer de disposer d'informations fiables et actualisées pour pouvoir prendre des décisions en toute connaissance de cause. Cela nécessite une collaboration étroite avec différentes sources d'information et la capacité de traiter et d'analyser les informations rapidement et efficacement.

« La politique sociale et l'innovation transforment notre monde plus rapidement que jamais. Mais l'avenir n'est pas inéluctable, il est construit par ceux qui avancent avec résilience, agilité et clairvoyance. »

Florian Kässberger
Experience Innovation Expert

Dans l'ensemble, il est essentiel que les entreprises et les États adoptent une approche globale pour relever les défis de la transformation numérique. Cela demande une collaboration étroite entre les différents acteurs, une adaptation et une amélioration continues des stratégies de sécurité ainsi qu'une culture de l'ouverture et de l'apprentissage continu. Ce n'est qu'en conjuguant nos efforts que nous pourrons façonner un avenir numérique sûr et stable.

La cybersécurité reste encore et toujours un élément central de la souveraineté numérique des entreprises et des organisations, à savoir:

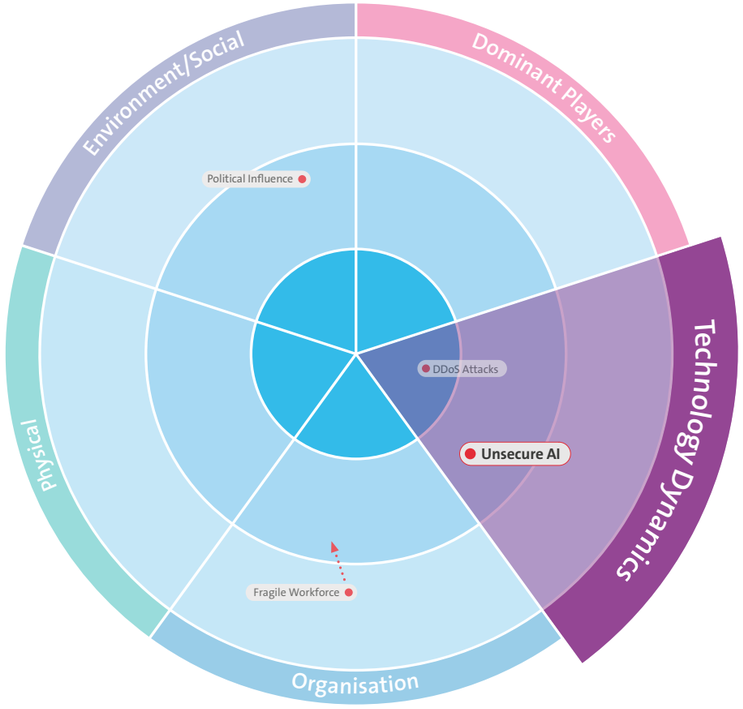
- Résilience et disponibilité des services et des infrastructures.
- Contrôle des données et des flux de données.
- Contrôle des processus numériques clés ainsi que des infrastructures et organisations qui les rendent possibles.
- Accès à des informations dignes de confiance.
- Cybersécurité.
- Compétences numériques.
- Chaînes d'approvisionnement diversifiées.

Et nous sommes tous appelés à contribuer à la souveraineté numérique. L'économie est prête à engager le dialogue et à apporter sa contribution. La voix de la branche est particulièrement importante pour la faisabilité et la mise en œuvre de la souveraineté numérique.

« La souveraineté numérique n'est pas un objectif en soi, mais un processus continu qui nécessite une approche globale. »

Karin Stöckli
Public Affairs Delegate of
Federal Administration and NGO

Shadow AI: «Là pour rester – l'IA à tout prix?»



Dans l'économie actuelle où tout va très vite, les entreprises misent de plus en plus sur l'intelligence artificielle (IA) pour rester compétitives. Mais à côté des systèmes d'IA officiellement implémentés se profile un phénomène moins connu: **le Shadow AI.**

Cette «IA fantôme» touche les entreprises de toutes tailles et de tous secteurs. Tout comme le «Shadow IT», le phénomène du «Shadow AI» fait référence à l'utilisation d'outils et de modèles d'IA au sein d'une entreprise sans l'autorisation de l'équipe informatique ou de l'équipe de sécurité. Cela peut sembler anodin, mais cette pratique comporte des risques considérables. Selon une étude de Gartner, plus de 50% des membres du personnel utilisent pour leur travail des modèles d'IA ou des applications d'apprentissage automatique dont le service informatique n'a pas connaissance. Dans certaines circonstances, cela peut entraîner des incidents graves, tels que:

- Violations de la protection des données et risques pour la sécurité.
- Violations de la conformité, en particulier dans le domaine de la protection des données et de la confidentialité, ou encore en ce qui concerne la loi européenne sur l'IA (dans la mesure où elle est applicable aux entreprises en Suisse).
- Inefficacités dues à des doubles dépenses et à des processus incohérents.
- Atteintes potentielles à la réputation en cas de divulgation d'abus.

La loi européenne sur l'IA est une loi de l'UE, mais elle peut également s'appliquer aux entreprises en Suisse dans certaines conditions. La loi sur l'IA imposera des exigences supplémentaires aux entreprises:

- Catégorisation des systèmes d'IA basée sur les risques. Plus le risque est élevé, plus les exigences sont strictes.
- Contrôles pour les modèles d'IA à haut risque.
- Obligations de transparence pour certains systèmes d'IA.
- Amendes élevées en cas de non-respect (jusqu'à 30 millions d'euros ou 6% du chiffre d'affaires annuel mondial selon l'infraction).

Formes de l'IA fantôme

- **Chatbots basés sur l'IA:** ceux-là sont souvent utilisés sans autorisation pour traiter les demandes de clients, ce qui peut conduire à des réponses inexactes.
- **Modèles d'apprentissage automatique:** les collaboratrices et collaborateurs utilisent des plateformes externes pour analyser les données, ce qui peut mettre en danger les données confidentielles.
- **Outils d'automatisation pour le marketing:** ceux-là augmentent certes la productivité, mais peuvent enfreindre les règles de conformité et nuire à la confiance des clients.
- **Fonctionnalité d'IA dans les logiciels d'entreprise:** une fonctionnalité d'IA supplémentaire est activée après la mise à jour d'une application existante sans vérification en plus, et divulgue des données sensibles à des personnes non autorisées.

Opportunités et défis

L'intégration de l'IA dans les processus d'entreprise offre un énorme potentiel d'innovation. L'IA peut contribuer à optimiser les processus commerciaux, à développer de nouveaux produits et services et à augmenter la satisfaction de la clientèle. L'analyse de grands volumes de données permet aux entreprises d'obtenir des informations précieuses et de prendre des décisions éclairées. L'automatisation basée sur l'IA peut améliorer l'efficacité et soulager le personnel des tâches répétitives, ce qui lui permet de se concentrer sur des activités stratégiques.

L'intelligence artificielle est devenue incontournable dans le monde du travail actuel. Elle sert de moteur d'innovation et, si elle est correctement utilisée, elle peut augmenter la productivité. Toutefois, les entreprises doivent limiter les risques en donnant des directives claires et en effectuant une surveillance.

Pour relever les défis de l'IA fantôme, il est essentiel que les entreprises encouragent une culture de la transparence et de la collaboration entre les services informatiques et les services spécialisés. Des formations et des audits réguliers permettent d'identifier et de corriger les risques potentiels à un stade précoce. C'est le seul moyen d'intégrer l'IA fantôme dans un écosystème d'IA contrôlé et sécurisé.

« Toute entreprise qui utilise des outils d'IA devrait à l'avenir mettre en place une gouvernance de l'IA globale, non seulement pour prévenir les risques de réputation, mais aussi pour se conformer aux réglementations actuelles et futures. Les technologies d'IA évoluent rapidement. Il est donc d'autant plus important de suivre le rythme et de garantir une utilisation responsable. »

Anne-Sophie Morand
Data Governance Counsel

Mesures d'intégration de l'IA fantôme et innovation par l'IA

Pour s'attaquer à l'IA fantôme et se préparer à la loi européenne sur l'IA, les entreprises devraient prendre les mesures suivantes:

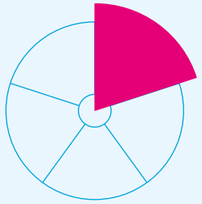
- **Inventaire et évaluation des risques:** identifiez tous les systèmes d'IA de l'entreprise et évaluez leurs risques au regard des dispositions légales applicables (p. ex. droit de la protection des données ou loi européenne sur l'IA, le cas échéant).
- **Gouvernance et directives:** développez des directives claires sur l'utilisation de l'IA et établissez un processus d'autorisation pour les nouveaux outils d'IA.
- **Contrôles techniques:** mettez en place la surveillance du réseau et des systèmes DLP.
- **Formation et sensibilisation:** organisez régulièrement des formations spécifiques à l'IA pour votre personnel et encouragez une culture de la communication ouverte sur les thèmes de l'IA.
- **Déploiement de solutions d'IA autorisées:** évaluez et déployez des outils d'IA officiels.
- **Gestion de la conformité:** mettez en place un comité d'éthique de l'IA ainsi que des processus de suivi et de documentation continus.
- **Collaboration et expertise:** établissez un centre de compétences en matière d'IA et collaborez étroitement avec des experts en droit et en conformité.

Ces mesures permettent aux entreprises de gérer efficacement l'IA fantôme tout en respectant les exigences légales. Il est important d'adopter une approche proactive afin d'à la fois exploiter les opportunités de l'IA et limiter les risques qui y sont liés.

« Lors de l'utilisation d'outils d'IA, les utilisatrices et utilisateurs ainsi que les entreprises se préoccupent encore trop peu des violations de la protection des données et des risques pour la sécurité. Outre les opportunités offertes par l'IA associée au traitement de grands volumes de données, c'est justement cela qui présente des risques potentiellement importants. »

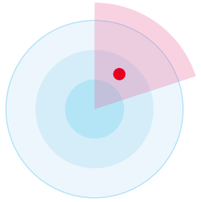
Marc Scheidegger
Solution Security Architect pour Data, Analytics & AI

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



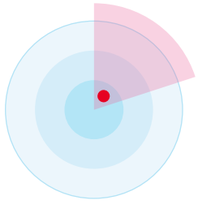
Dominant Players

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



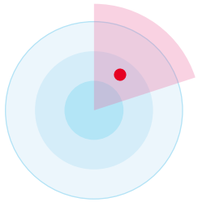
Cloud Ecosystem Dependencies
La forte centralisation des données dans le Cloud induit des risques cumulés. La défaillance d’un service notamment centralisé peut avoir des répercussions dans le monde entier.

► Inchangé



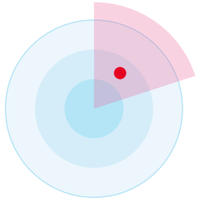
Infrastructure Integrity
Des vulnérabilités peuvent avoir été intégrées délibérément ou par négligence dans des composants essentiels des infrastructures critiques, compromettant ainsi la sécurité du système.

► Inchangé



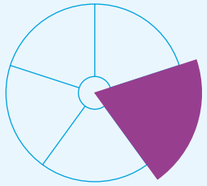
Legacy Protocols
En raison de dépendances logicielles, des protocoles totalement obsolètes et vulnérables (p. ex. NTLMv1, SMBv1, RC4) sont encore utilisés. Quelques applications peuvent ainsi compromettre la sécurité d’infrastructures complètes.

► Inchangé



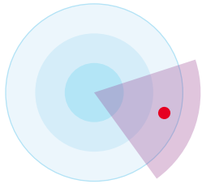
Manipulated Generative AI
Des manipulations ciblées permettent de modifier les résultats d’un système d’IA. L’objectif est alors d’introduire des données malveillantes, fausses ou corrompues dès la phase d’entraînement, de voler des modèles LLM, ou de générer des prompts qui peuvent avoir des effets indésirables et juridiquement contraignants. Nous parlons ici des risques de sécurité liés à l’IA et non des risques liés à l’utilisation de l’IA (voir AI-Based Attacks).

► Inchangé



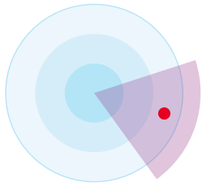
Technology Dynamics

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.



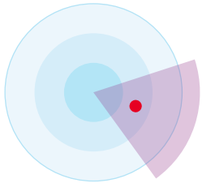
5G Security
La 5G est une technologie mobile encore récente. Son déploiement génère de nombreuses opportunités, mais s'accompagne aussi de menaces encore inconnues.

► Inchangé



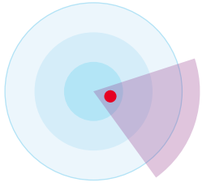
Quantum Computing
Les ordinateurs quantiques peuvent rendre inutiles les procédés cryptographiques actuels, car ils sont en mesure de les contourner en très peu de temps.

► Inchangé



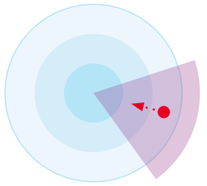
Unsecure AI
Les systèmes d'IA non sécurisés mettent en danger les chaînes d'approvisionnement et la protection des données, car les modèles génératifs peuvent divulguer des données confidentielles de manière incontrôlée. Cela peut non seulement porter atteinte à la continuité des activités, mais aussi nuire considérablement à la réputation d'une entreprise. En outre, des conséquences réglementaires risquent d'être encourues, notamment à travers la loi sur l'IA, si les décisions prises en matière d'IA enfreignent les prescriptions en vigueur.

► Inchangé



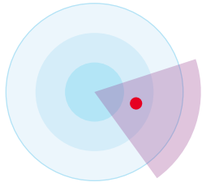
Ransomware
Les données critiques sont cryptées en masse puis (éventuellement) décryptées moyennant le versement d'une rançon.

► Inchangé



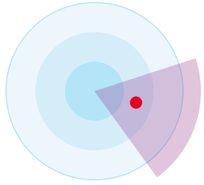
Increased Complexity
La complexité des systèmes, en particulier au-delà des limites des technologies et des entreprises, ne cesse de croître. Les paysages IT se complexifient d'autant plus dans un environnement hybride/multicloud intégrant de nombreux fournisseurs de cloud. L'exposition aux risques augmente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

▲ Croissant



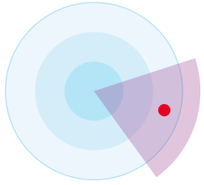
AI-Based Attacks
Les attaques basées sur l'intelligence artificielle (IA) sont plus ciblées et donc plus difficiles à détecter. L'IA les rend plus efficaces sur les vecteurs d'attaque classiques tels que le ransomware, le phishing, le spear-phishing, ainsi que sur de nouveaux modes opératoires moins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

► Inchangé



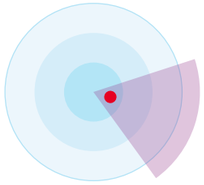
Agentic AI
L'IA agentique est proactive et capable de prendre des décisions et d'adapter des stratégies de manière autonome. Cela augmente la surface d'attaque, car les systèmes d'autoapprentissage et adaptatifs peuvent développer des comportements imprévisibles et interagir de manière indépendante avec les systèmes périphériques. La compromission de ces agents peut entraîner des accès non autorisés à des composants de système et données sensibles, ce qui augmente considérablement la probabilité d'escalade et de fraude. Même un Copilot apparemment inoffensif peut causer des dommages considérables en raison d'instructions erronées ou de manipulations de la part d'assaillants.

► Inchangé



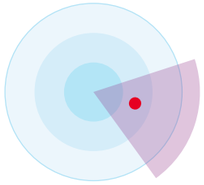
Subscriber Compromise
Des logiciels malveillants se créent un accès aux données privées des utilisatrices et utilisateurs mobiles ou sont utilisés pour cibler les infrastructures IT ou de télécommunication. Les attaques de phishing, smishing, vishing et MFA Bypass ciblent les Subscriber Credentials.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

► Inchangé



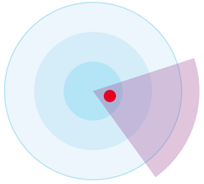
DDoS Attacks
Une attaque par Distributed Denial of Service (DDoS) est une tentative malveillante visant à perturber le trafic de données normal d'un serveur, d'un service ou d'un réseau cible en inondant la cible ou son infrastructure d'un flot de trafic Internet. L'efficacité des attaques DDoS repose 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.

► Inchangé



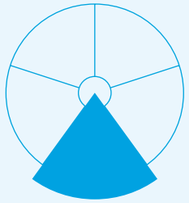
Targeted Attacks
Attaques ciblées et complexes poursuivant un objectif concret. Des personnes clés sont identifiées et attaquées de manière ciblée, directement ou indirectement (Lateral Movement, méthodes d'ingénierie sociale) afin d'obtenir des informations pertinentes ou de causer un maximum de dommages. L'une des principales caractéristiques de ces attaques est la persistance: les assaillants 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



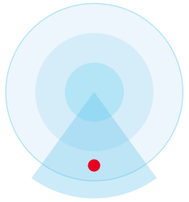
Supply Chain Attacks
Les attaques contre la chaîne d'approvisionnement visent à exploiter les relations de confiance et d'affaires entre une entreprise et des parties externes. Il peut s'agir de partenariats, de relations avec les fournisseurs ou de l'utilisation de logiciels de tiers.

► Inchangé



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 contrôle et la gestion de la sécurité deviennent ainsi compliqués.

► Inchangé

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

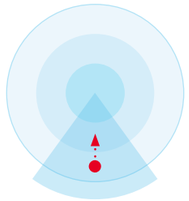
► Inchangé

Digital Transformation Risks
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 lié 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.

► Inchangé



Fragile Workforce
Une organisation de travail fragile décrit la vulnérabilité des équipes de cybersécurité et de cyberdéfense face à la charge psychique et à l'absence de prévention du stress et du burn-out. Lorsqu'une personne est psychologiquement instable et ne peut pas agir correctement sous pression, la probabilité d'erreurs humaines augmente. Il en résulte un risque accru de failles de sécurité et de points d'attaque susceptibles de mettre en péril la stabilité de l'ensemble de l'entreprise.

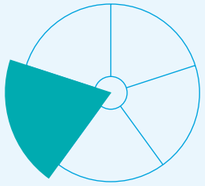
▲ Croissant

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.

► Inchangé

Fraud
La fraude désigne des actes frauduleux basés sur la tromperie et l'enrichissement illicite. Elle se manifeste par des transactions falsifiées, des vols d'identité ou la manipulation de documents. Pour les entreprises et les particuliers, la fraude représente un danger considérable, car elle peut entraîner des pertes financières et nuire à la réputation.

► Inchangé



Physical

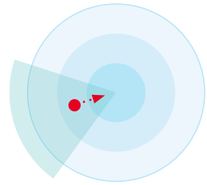
Ce terme désigne les attaques sur l'infrastructure du cyberespace qui causeront de plus en plus de dommages dans le monde physique. Il inclut également les menaces émanant de l'environnement physique et généralement davantage axées sur des cibles physiques.

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 black-out (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.

► 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.

► Inchangé

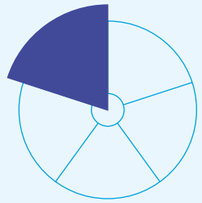


Unsecure IoT/OT Devices
Qu'il soit déployé dans des technologies opérationnelles (OT) pour la surveillance et la gestion de processus, des appareils et infrastructures physiques ou dans des appareils IoT, l'Internet des objets est omniprésent. Des tâches très variées – des plus simples au plus complexes – 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.

▲ Croissant

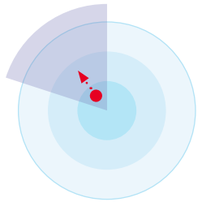
Environmental Influence
La crise climatique entraîne une augmentation des phénomènes et des influences météorologiques imprévisibles (chaleur, fortes pluies, tornades, grêle, éclairs de forte intensité, etc.), qui peuvent occasionner des dommages à l'infrastructure des organisations et des entreprises et ainsi avoir un fort impact sur l'environnement externe et interne d'un système d'information ou d'un réseau.

► Inchangé



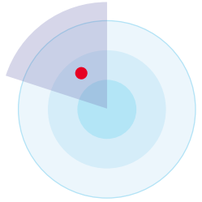
Environment/Social

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.



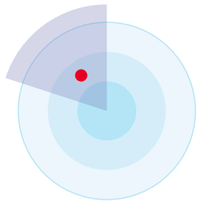
Security Job Market
Les besoins énormes en professionnels de la sécurité sont très difficiles à satisfaire. Il en résulte une perte de savoir-faire dans la lutte contre des attaques de plus en plus complexes et intelligentes.

▼ Décroissant



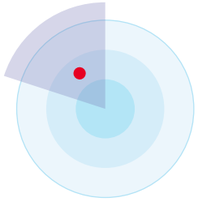
Digital Identity
Les identités numériques personnelles certifiées peuvent être usurpées ou volées, par exemple dans le but de conclure des contrats au nom de tiers.

► Inchangé



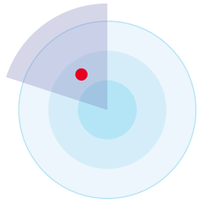
Disinformation & Destabilisation
La diffusion intentionnelle d’informations erronées peut entraîner une déstabilisation économique et sociale. Son utilisation ciblée dans les scénarios de crise, y compris via le cyberespace, se développe de plus en plus.

► Inchangé



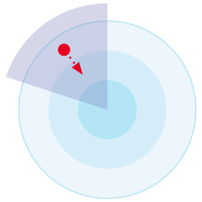
Political Influence
Les forces politiques, mais aussi les réglementations et les directives, peuvent influencer les décisions d’ordre technologique ou économique, par exemple dans le choix des fournisseurs de technologie. Il peut en résulter de nouveaux risques.

► Inchangé



Data-Centric Risks
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



Geopolitical Situation / State Level Attacks
En périodes de guerres, de terreur et d'instabilité politique au sein des pays et des sociétés, les conséquences négatives dans le cyberespace tendent à s'accentuer. Il s'agit de piratages commandités par différents pays et groupes de hacktivistes à motivation politique, d'acteurs étatiques et de réseaux de criminalité organisée, qui exercent une pression accrue sur les entreprises et les organisations par le biais de travaux sur commande. Les dommages collatéraux qu'entraînent les stratégies de «hack back» suscitent également une attention accrue.

▲ Croissant

Conclusion

La transformation numérique pose de nombreux défis aux entreprises et aux institutions.

La transformation numérique pose de nombreux défis aux entreprises et aux institutions. La situation géopolitique, à laquelle nous devons faire face au quotidien, a également une influence directe sur les décisions d'ordre technologique et économique. Il s'agit par exemple de la gestion des modèles d'IA non contrôlés, de la garantie de la cybersécurité générale et de la protection des équipes de cybersécurité contre le surmenage. Les entreprises ont donc tout intérêt à développer des stratégies de résilience afin d'anticiper les changements disruptifs et de pouvoir s'imposer avec succès face à la concurrence mondiale. Il est essentiel de trouver un bon équilibre entre la conformité et une gestion proactive de la sécurité. Une méthode de travail durable nécessite une culture de la transparence, une sécurité psychologique et des formations continues régulières. Les cadres jouent un rôle central dans la prévention de la surcharge mentale et dans la création d'un environnement de travail résilient.

C'est pourquoi les entreprises et les institutions devraient agir de manière proactive dans ce monde numérique en pleine évolution afin d'exploiter les opportunités de la transformation numérique tout en réduisant activement les risques qui y sont liés. Cela demande une collaboration étroite entre les différents acteurs, une adaptation et une amélioration continues des stratégies de sécurité ainsi qu'une culture de l'ouverture et de l'apprentissage continu.

Miser sur des solutions innovantes dans les entreprises et les organisations, c'est encourager une culture d'entreprise transparente et consciente de la sécurité et investir dans la formation continue régulière des équipes. Il est ainsi possible de créer un avenir numérique sûr permettant aux entreprises, organisations et États de gagner en résilience face aux menaces de sécurité. Nous pouvons tous y contribuer et montrer l'exemple. Saisissons ensemble les opportunités de l'avenir numérique.

#BeTheStrongestLink

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	© Avril 2025 by Swisscom (Suisse) SA, Group Security, Alte Tiefenaustrasse 6, 3048 Worblaufen, swisscom.ch
Édition	OK DIGITALDRUCK AG, Zurich
Tirage	140 exemplaires

En tant qu'«Innovator of Trust», Swisscom permet et façonne l'avenir numérique. Ses produits et services innovants associés à la confiance de sa clientèle créent une expérience unique pour cette dernière et ont un impact durable sur l'environnement et la société. En Suisse et dans le monde entier.

De plus amples informations sur nos produits, nos services et notre engagement pour la sécurité en Suisse sont disponibles sur swisscom.ch/securite

Un emploi dans le secteur de la sécurité chez Swisscom t'intéresse-t-il ? Alors jette un coup d'œil ici et dépose ta candidature: swisscom.com/securityjobs

#BeTheStrongestLink