swisscom

Cybersecurity Threat Radar 2026

La géopolitique et la technologie disruptive comme vecteurs de menace

Table des matières

« **La confiance n’est pas une promesse ponctuelle, c’est une responsabilité que nous devons assumer chaque jour. En tant qu’Innovators of Trust, nous protégeons non seulement les données, mais aussi la fiabilité et la souveraineté numériques de la Suisse.**

Cybersecurity Threat Radar

La géopolitique et la technologie disruptive comme vecteurs de menace

Chez Swisscom, nous ne protégeons pas seulement les systèmes, nous encourageons aussi la numérisation de la Suisse. Des millions de personnes comptent sur des réseaux stables, une communication sécurisée et une résilience numérique. En tant que CSO, je constate quotidiennement l'impact direct des tensions géopolitiques et des avancées technologiques sur la sécurité. Les menaces apparaissent aujourd'hui à l'échelle mondiale, mais leurs conséquences peuvent aussi nous toucher localement à tout moment.

Le Cybersecurity Threat Radar est notre instrument d'alerte précoce. Il nous renseigne sur l'évolution des menaces, les nouveaux schémas qui apparaissent et les domaines où il est urgent d'agir. Cette année, j'ai été particulièrement préoccupé par l'intégration d'un nouveau vecteur de menace: la guerre hybride, autrement dit le mélange de moyens militaires classiques et de cyberattaques, de désinformation et d'influence numérique et politique. Cette évolution montre clairement à quel point la sécurité physique et la sécurité numérique sont désormais étroitement liées.

Les incertitudes géopolitiques et les conflits d'intérêts économiques entraînent une augmentation des cyberattaques d'origine étatique: des attaques qui mettent à l'épreuve les entreprises, mais aussi la stabilité numérique de toute la Suisse. En tant qu'opérateur de télécommunications, nous sommes pleinement conscients que la capacité d'adaptation et la résilience sont devenues essentielles.

Les technologies disruptives changent également la donne. L'intelligence artificielle, l'informatique quantique et les appareils connectés ouvrent à la fois des opportunités d'innovation considérables et de nouvelles surfaces d'attaque. La protection de la Suisse numérique et des personnes qui comptent sur nous chaque jour reste la priorité absolue de Swisscom.

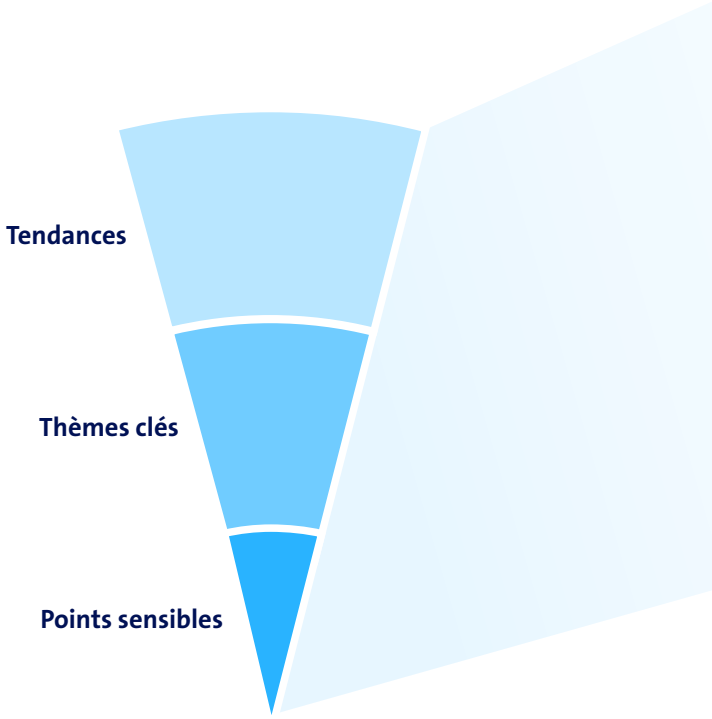
Le constat est évident: la sécurité est loin d'être garantie. Elle repose sur un processus continu qui requiert une démarche proactive, une analyse constante des nouvelles menaces et une culture de la sécurité partagée dans toute l'entreprise. Seuls le développement continu de nos mesures de protection et leur mise en œuvre cohérente pourront nous permettre de faire face aux risques complexes de notre époque et de renforcer de manière fiable la Suisse numérique.

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.




Environment/Social
Dominant Players
Technology Dynamics
Organisation
Physical
Security Job Market
Geopolitical Situation / State Level Attacks
Data-Centric Risks
Identity Theft & Impersonation
Disinformation & Destabilisation
Political Influence
Hybrid Warfare
Environmental Influence
Targeted Sabotage
Unsecure IoT/OT
Digital Transformation Risks
UAS Threats
Energy Instability
Security Skills
Infrastructure Misconfiguration
Fragile Workforce
Workplace Heterogeneity
Decentralised Development & Operations
Fraud
Insider Threat
Manipulated Generative AI
Cloud Ecosystem Dependencies
Legacy Protocols
Infrastructure Integrity
Subscriber Compromise
Agentic AI
Increased Complexity
DDoS Attacks
Ransomware
AI-Based Attacks
Supply Chain Attacks
Targeted Attacks
Unsecure AI
Residential Proxies
Quantum Computing
Défis
Today
Tendency

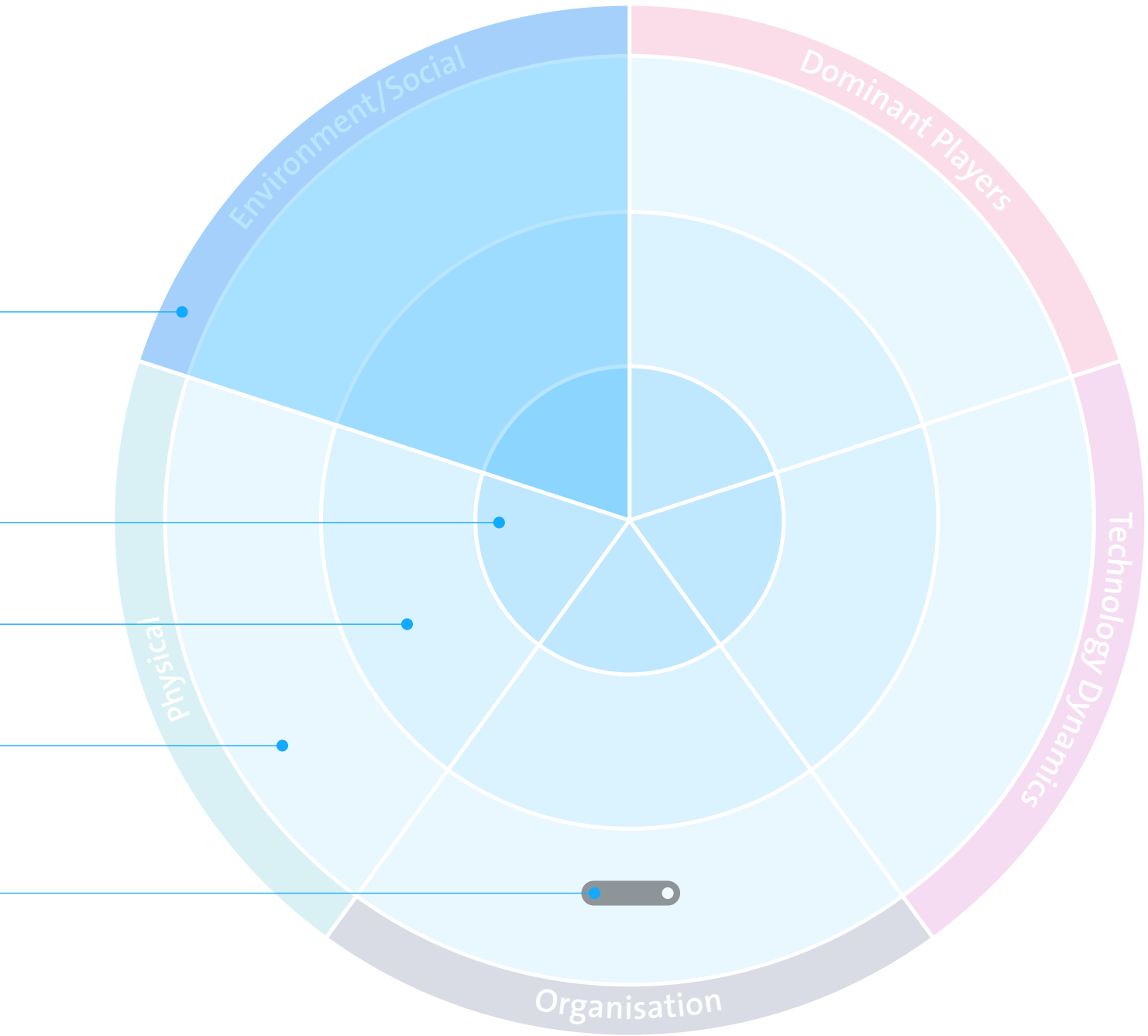
Méthodologie

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 l'actualité de la menace en question 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.

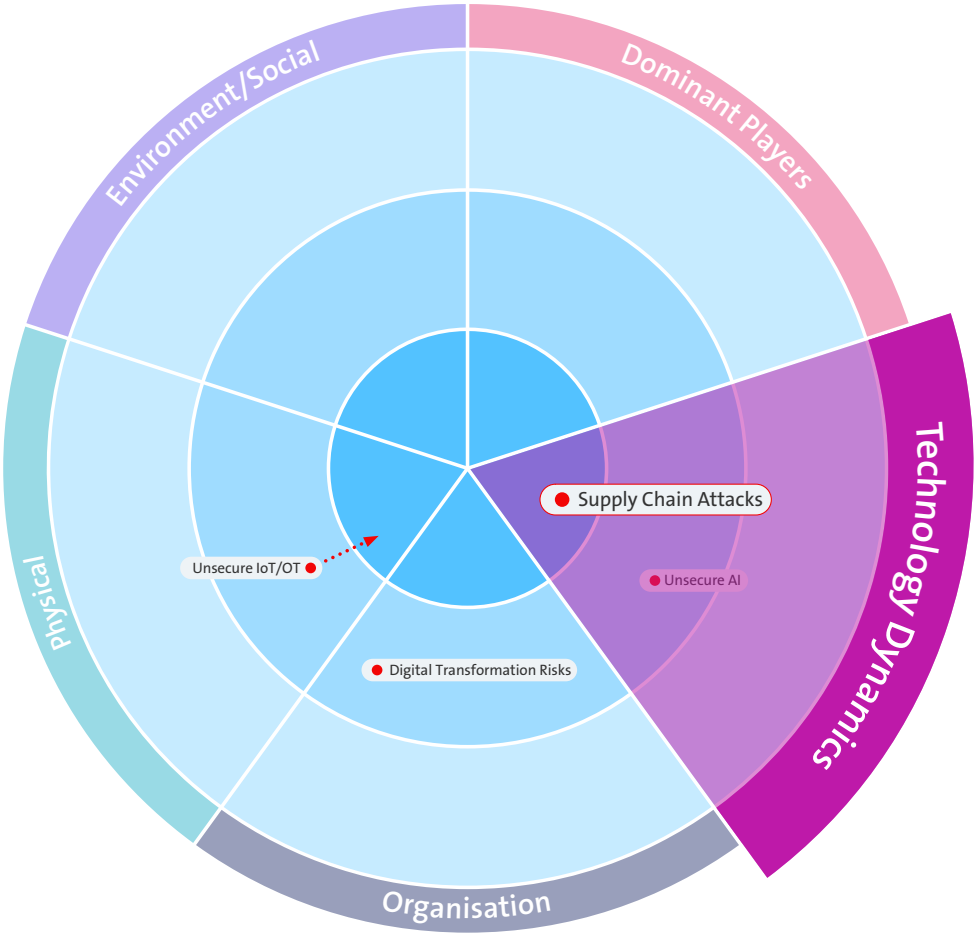
Ces cercles mettent en évidence:

- 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.


Environment/Social
Dominant Players
Technology Dynamics
Organisation
Physical

La chaîne d’approvisionnement logicielle dans la supply chain: un château de cartes bâti sur un code inconnu



Dans un monde des affaires de plus en plus numérisé, les entreprises sont tributaires d'une multitude de solutions et de services logiciels. L'intégration de composants et modules externes est depuis longtemps devenue la norme – et c'est précisément là que réside l'un des plus grands défis de la sécurité informatique actuelle: les «supply chain attacks», autrement dit les attaques visant la chaîne d'approvisionnement logicielle. Il suffit d'un seul maillon faible pour que tout le château de cartes s'effondre.

Les logiciels modernes sont constitués de centaines de composants externes et de pipelines de construction automatisés. L'origine et la qualité de ce code tiers sont souvent difficilement traçables, ce qui complique considérablement l'identification des vulnérabilités. C'est précisément ce manque de transparence qui fait de la chaîne d'approvisionnement une cible privilégiée pour les attaquants: une seule bibliothèque compromise ou un système CI/CD manipulé peut déjà impacter des milliers d'entreprises.

Le risque majeur vient du fait que de nombreuses entreprises s'appuient sur des composants dont elles ne peuvent pas vérifier elles-mêmes le niveau de sécurité.

État actuel des menaces: exemples et tendances de développement

En 2025, des incidents dans l'écosystème npm (le plus grand registre pour les paquets JavaScript) tels que «Shai-Hulud» ont mis en évidence une nouvelle réalité: les attaquants ciblent le code open source et exploitent la chaîne de confiance des paquets populaires pour propager des logiciels malveillants via des mises à jour apparemment légitimes. Les mises à jour étant souvent prises en charge sans vérification de sécurité supplémentaire ni contrôle manuel, puis diffusées sous forme de dépendances, ces attaques peuvent se propager très rapidement tout au long de la chaîne d'approvisionnement logicielle.

De plus, des défaillances ou compromissions de services ou fournisseurs centraux, appelés Single Points of Failure, peuvent – comme récemment chez CrowdStrike, Microsoft ou Cloudflare – entraîner des répercussions considérables pour de nombreuses entreprises.

Perte de données, interruption d'exploitation et atteintes à la réputation

Les attaques réussies contre la chaîne d'approvisionnement logicielle ont de graves conséquences: outre la perte de données sensibles, il existe un risque d'interruption de l'exploitation qui, dans le pire des cas, peut conduire à l'arrêt de processus critiques pour l'entreprise. Les atteintes à la réputation causées par des incidents de sécurité rendus publics ne doivent pas non plus être sous-estimées, car elles sont susceptibles d'ébranler durablement la confiance des clients, partenaires et investisseurs.

Renforcer la vérifiabilité et la résilience
Relever les défis de la chaîne d'approvisionnement logicielle moderne requiert des mesures techniques et organisationnelles, parmi lesquelles:

- Documentation et suivi systématiques de tous les modules utilisés et de leurs actualisations
- Contrôles de sécurité (audits) et tests d'intrusion réguliers tout au long de la chaîne d'approvisionnement
- Établissement de processus clairs pour la sélection, l'évaluation et la validation de composants logiciels externes
- Utilisation de solutions de surveillance qui détectent et signalent précocement les activités suspectes
- Développement et mise en œuvre de stratégies de mise à jour afin de remédier rapidement aux vulnérabilités connues

Sur le plan réglementaire, le **Cyber Resilience Act (CRA)** et la **Network and Information Security Directive 2 (NIS2)** de l'Union européenne marquent un tournant: les fabricants doivent désormais prouver comment leur logiciel a été développé et les exploitants sont tenus de vérifier ces preuves. Les SBOM (Software Bill of Materials), les builds reproductibles, les signatures et la gestion documentée des vulnérabilités deviennent ainsi obligatoires. L'intégrité et l'origine ne sont plus supposées, mais démontrées techniquement.

Deux concepts sont essentiels à cet égard:

- **Intégrité:** une mise à jour est-elle authentique et inchangée?
- **Provenance:** comment, où et avec quoi a-t-elle été construite?

Des standards tels que les SLSA (Supply-chain Levels for Software Artifacts) ou les SBOM signés fournissent pour la première fois des preuves infalsifiables.

« La base d'une véritable confiance n'est créée que lorsque chaque artefact logiciel est signé par cryptographie et que son origine peut être prouvée de manière irréfutable.

Florian Lukavsky
Chief Innovation Officer, SignPath

Ces contrôles n'étant guère possibles manuellement, des plateformes spécialisées en sécurité de la chaîne d'approvisionnement logicielle prennent en charge les attestations automatisées et sécurisées par cryptographie, directement dans le processus de construction. La sécurité devient ainsi vérifiable et ne repose plus uniquement sur la confiance.

Un changement d'approche est également nécessaire sur le plan organisationnel. Les entreprises doivent surveiller en permanence leur chaîne d'approvisionnement, gérer activement les vulnérabilités et imposer à leurs partenaires des normes minimales pour rester résilientes face aux attaques de la chaîne d'approvisionnement. La sensibilisation de ses propres effectifs aux risques et la création d'une culture de la sécurité sont également des éléments essentiels.

Résilience et contrôle continu: les facteurs clés

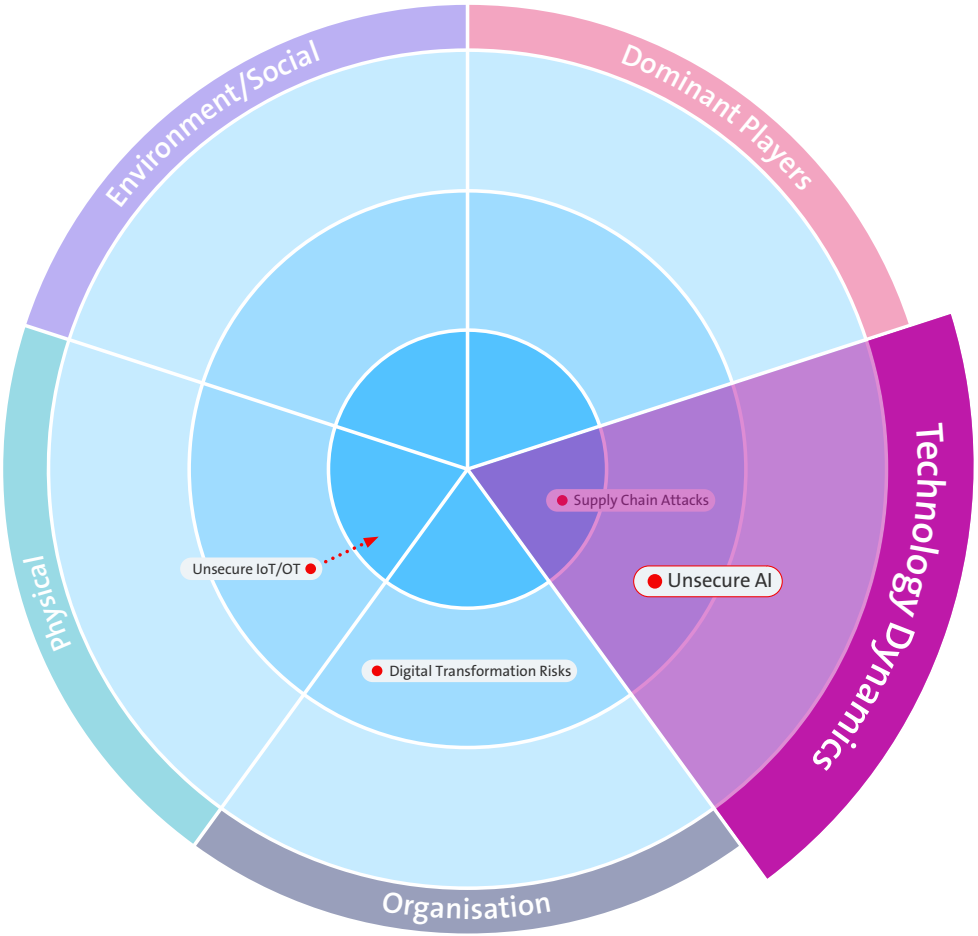
La menace des attaques de la chaîne d'approvisionnement continuera à l'avenir à peser sur les entreprises et gagnera en importance. Miser sur les avantages des logiciels modernes et modulaires impose d'avoir conscience des risques et d'investir systématiquement dans sa propre résilience. Contrôle continu, transparence et gestion globale des risques sont les piliers qui permettent de maintenir la stabilité de son château de cartes informatique, y compris en période de turbulences, et d'éviter la «roulette russe» dans la chaîne d'approvisionnement logicielle.

> « La confiance reste indispensable aujourd'hui. Il est toutefois impératif d'identifier les éventuelles vulnérabilités de la chaîne d'approvisionnement logicielle, par exemple par une modélisation ciblée des menaces couvrant l'ensemble de la chaîne d'approvisionnement.

Simon Röthlisberger
Security Architect

Défis et tendances

L’IA à plein régime – un multiplicateur de risques



L'intelligence artificielle s'est propagée à une vitesse remarquable dans de nombreux domaines de notre société et de notre économie. L'engouement pour les technologies IA est tel que des questions critiques relatives à la sécurité, à la transparence et à la durabilité peuvent passer au second plan. Le vecteur de menace «Unsecure AI», en particulier, montre à quel point l'ignorance peut rapidement conduire à une architecture système dangereuse, avec des conséquences qui dépassent largement le cadre de l'informatique.

Cet article explique pourquoi nous devons nous intéresser à l'IA non sécurisée, comment ces risques se développent, et quelles mesures concrètes les acteurs peuvent adopter pour y faire face de manière constructive et responsable.

Pourquoi l'Unsecure AI devient un risque

L'engouement pour l'IA conduit souvent à introduire des innovations sans compréhension approfondie ou sans réflexion suffisante en matière de sécurité. Les systèmes IA sont utilisés «à plein régime», sans savoir où et comment ils influencent les décisions opérationnelles, avec quelles données ils ont été entraînés ou qui a été impliqué dans le processus de développement. On a souvent recours à des solutions low-code et no-code dont l'origine et l'architecture ne sont pas compréhensibles pour les utilisateur·trice·s. L'intégration de l'IA par les entreprises partenaires constitue un point particulièrement critique en raison des risques de chaîne d'approvisionnement (voir page 10) difficilement contrôlables qui en résultent. À cela s'ajoute le fait que les logiciels malveillants sont de plus en plus souvent introduits directement dans les systèmes lors du codage, par exemple par l'IA générative.

Le danger n'émane cependant pas seulement de la technique. Le manque de savoir-faire des utilisateur·trice·s et des cyperexpert·e·s aggrave le problème. La conclusion erronée selon laquelle les spécialistes juniors pourraient être remplacés par l'IA conduit à une lacune de compétences susceptible d'affaiblir à moyen terme l'ensemble de la structure de la sécurité, y compris des domaines tels que la gestion de la qualité des données ou la gestion de la chaîne d'approvisionnement.

D'où viennent les faiblesses?

Une IA insuffisamment sécurisée résulte de la négligence des processus de sécurité, de l'ignorance des exigences de transparence et du non-respect des règles de gouvernance. Les modèles d'IA sont utilisés dans des systèmes productifs sans que leur fonctionnement, leur base de données ou leur logique de décision aient été vérifiés et documentés.

Les outils et les plateformes low-code permettent à des personnes moins expérimentées de créer des applications IA. Si l'on se fie à 100% aux résultats de l'IA, cet avantage en matière d'innovation renforce parallèlement la surface d'attaque. Dans la chaîne d'approvisionnement, les modèles et les données de tiers sont souvent repris sans conscience des risques de sécurité et sans implémentation préalable des normes de sécurité uniformes.

L'utilisation de l'IA dans la gestion du Bug Bounty, où les signalements sont automatisés et donc plus nombreux mais de moindre qualité, montre clairement à quel point il est difficile de faire la distinction entre les véritables vulnérabilités et les faux signalements. Il en résulte un patchwork de systèmes dans lesquels plus personne ne sait comment, où et avec quelle intégrité l'IA est utilisée.

Stratégies positives pour plus de sécurité

Les risques sont importants, mais de nombreuses approches permettent aux entreprises et aux particuliers de relever ces défis de manière constructive:

- **Créer de la transparence:** chaque application IA doit être documentée, y compris l'origine des données, les algorithmes utilisés et la logique de décision. C'est le seul moyen de comprendre et de contrôler les risques.
- **Formations et sensibilisation:** la formation continue de toutes les personnes impliquées est essentielle. Les compétences en matière d'IA ne doivent pas être réservées aux seul·e·s expert·e·s, mais doivent être ancrées à l'échelle de l'organisation.
- **Équipes pluridisciplinaires:** des équipes en charge de l'informatique, du droit, de l'éthique et d'autres domaines spécialisés doivent également être impliquées dans le développement et l'implémentation de l'IA. Différentes perspectives et compétences sont ainsi exploitées pour identifier les risques à un stade précoce.
- **Responsabilité et gouvernance:** Il convient de définir des responsabilités claires pour les systèmes IA et de établir des règles pour leur utilisation. Des audits et des révisions doivent parallèlement être réalisés par des organismes indépendants.
- **Culture de l'erreur et échanges:** les erreurs et les failles de sécurité doivent être communiquées ouvertement afin d'en tirer des enseignements et d'améliorer continuellement les processus. Une gestion transparente des faiblesses renforce l'ensemble de l'organisation.

> « Dans un monde livré au chaos du low code et à l'automatisation de l'IA, un programme Bug Bounty fait office de sismographe des risques réels.

Antoine Neuenschwander
Head Bug Bounty

- **Éthique et durabilité:** outre des critères techniques et économiques, toute application IA doit également être évaluée sous l'angle éthique et sociétal.
- **Promotion de la relève:** la promotion de la relève dans le domaine Security reste essentielle. Les juniors et les seniors doivent collaborer à la recherche de solutions – l'IA peut compléter les compétences, mais non les remplacer.

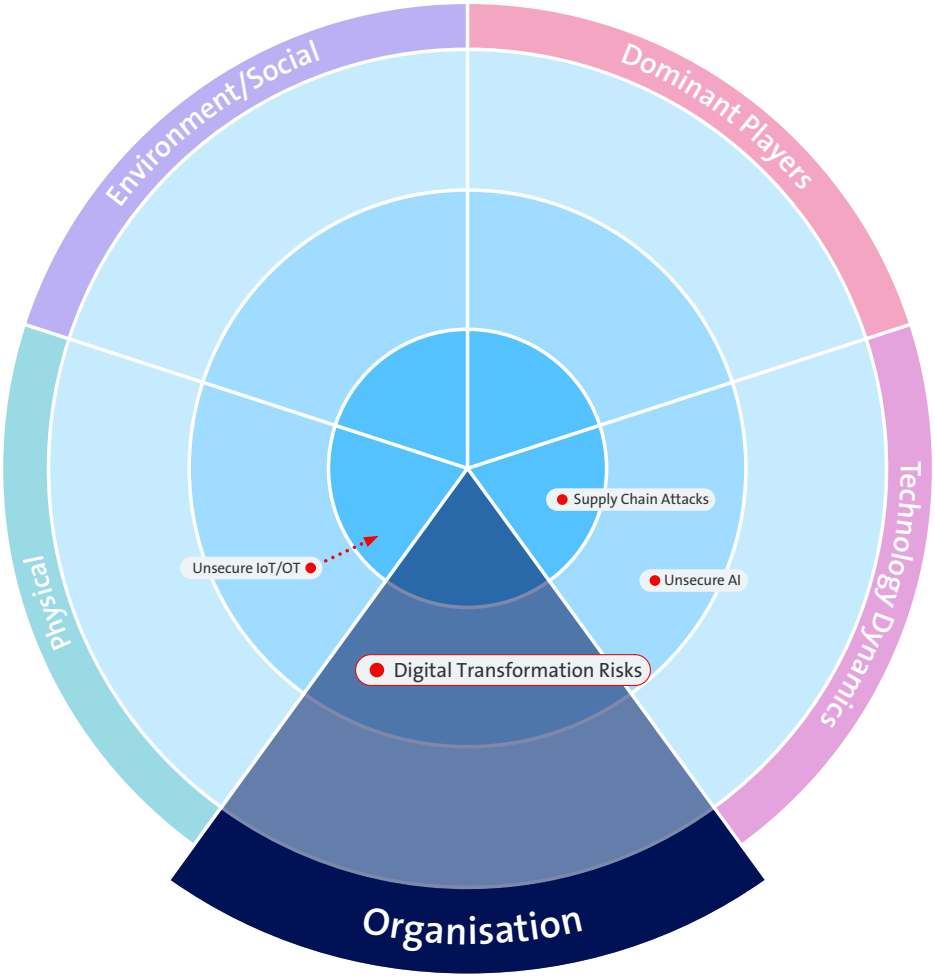
Implication des collaborateur·trice·s
Il est important d'aborder ouvertement les aspects d'ordre éthique, moral et durable que soulève le thème de l'IA. Pour que collaborateur·trice·s puissent suivre l'évolution fulgurante de l'IA, il convient de créer un environnement approprié. Les compétences des collaborateur·trice·s peuvent ainsi être renforcées par des formations ciblées, par exemple au moyen de formats de sensibilisation tels que les promptathons.

Cette approche constitue une gestion active et consciente du changement.

« Si nous voulons faire tourner l'IA à plein régime dans les entreprises, il faut avant tout une direction qui place l'humanité avant la vitesse dans le domaine de la numérisation. La culture ne naît pas d'outils, mais de modèles. Avant de développer l'IA, nous devons d'abord développer les compétences humaines.

Marcus Beyer
Security Awareness Officer

Souveraineté numérique: qui détient la dernière bouée de sauvetage dans le tourbillon de la transformation?



Au quotidien comme au travail, la transformation numérique est devenue omniprésente et implique de toutes nouvelles règles du jeu pour les entreprises suisses. Les données sont de plus en plus importantes, l'informatique migre vers le cloud et de nombreux processus sont désormais exécutés en externe. C'est précisément pour cette raison que le thème de la souveraineté numérique est actuellement sur toutes les lèvres. L'urgence est en outre accentuée par les évolutions géopolitiques. Les entreprises doivent plus que jamais garder une vue d'ensemble de leurs données et de leurs processus numériques, ce qui n'est pas une mince affaire dans un monde connecté.

Mais qu'entend-on exactement par souveraineté numérique et pourquoi est-elle si importante aujourd'hui pour les entreprises suisses? Tandis que la numérisation ne cesse de progresser et que de plus en plus de processus sont transférés des entreprises vers le cloud ou vers des prestataires de services externes, la question se pose de savoir comment les organisations peuvent garantir leur capacité d'action et leur contrôle. Il est donc nécessaire de comprendre clairement ce qu'impliquent la souveraineté numérique et les défis et opportunités qui en découlent concrètement.

En principe, les entreprises et les organisations doivent toujours être en mesure de contrôler, de piloter et de protéger leurs ressources numériques, en particulier leurs données et leurs infrastructures informatiques, de manière autonome et indépendante. La dépendance vis-à-vis de prestataires de services étrangers externes, notamment en ce qui concerne les services de cloud et d'externalisation, ne doit pas dépasser un niveau raisonnable.

Pour les entreprises suisses, la souveraineté numérique est importante à plusieurs titres:

- Les lois sur la protection des données, telles que la loi suisse révisée sur la protection des données (nLPD) et le RGPD européen, exigent que les entreprises sachent où leurs données sont stockées et qui y a accès.
- Le contrôle des données et des systèmes constitue un facteur central de la sécurité de l'information. Plus les dépendances vis-à-vis de tiers sont nombreuses, plus la surface d'attaque est importante.
- Les entreprises qui ne contrôlent pas leurs données peuvent, dans le pire des cas, perdre l'accès à leur capital le plus important et voir leur capacité d'innovation et leur position sur le marché s'affaiblir.

Externalisation et cloud: risque de perte de contrôle – l'illusion de la souveraineté des données?

L'externalisation des services informatiques et l'utilisation de plateformes cloud offrent des avantages considérables en termes d'évolutivité, de coûts et de flexibilité. Pour les entreprises suisses en particulier, l'externalisation à des prestataires spécialisés est souvent judicieuse d'un point de vue économique. Parallèlement, une partie du contrôle des données et des processus est perdue à chaque étape d'externalisation.

De nombreuses entreprises sous-estiment les risques liés à la transmission de données à des prestataires tiers:

- **Dépendance vis-à-vis du prestataire:** les coûts de changement et les obstacles techniques compliquent le changement de fournisseur ou le retour en arrière («Vendor Lock-in»).
- **Perte de transparence:** on ignore souvent précisément où et comment les données sont effectivement traitées, en particulier chez les opérateurs de cloud internationaux.
- **Insécurité juridique:** des espaces juridiques différents (p. ex. en raison de l'enregistrement dans l'UE ou aux États-Unis) compliquent l'application de ses propres exigences en matière de protection des données et de sécurité.
- **Risques de cybersécurité:** la concentration de données sensibles dans de grandes plateformes cloud en fait des cibles d'attaque de choix pour les cybercriminels.

La souveraineté des données tant invoquée reste souvent illusoire dans la pratique, en particulier lorsque les entreprises ne disposent pas des mécanismes de contrôle et des compétences nécessaires pour gérer leurs flux de données et leurs dépendances.

Avec la loi révisée sur la protection des données (nLPD), la Suisse dispose depuis septembre 2023 de l'une des réglementations en matière de protection des données les plus modernes d'Europe. Les entreprises suisses doivent appliquer les principes «Privacy by Design» et «Privacy by Default», respecter les droits des personnes concernées, et remplir les obligations de déclaration en cas de violation de la protection des données.

La question de savoir si et comment les données peuvent être transférées à l'étranger est particulièrement importante. Des directives strictes s'appliquent pour la transmission à des pays tiers, en particulier lorsque ceux-là ne présentent pas un niveau de protection des données approprié. De nombreuses entreprises s'interrogent ainsi sur l'opportunité de recourir à des partenaires cloud et d'externalisation basés en Suisse ou à l'étranger.

« Maîtriser et piloter activement sa souveraineté numérique est aujourd'hui un impératif pour toutes les entreprises.

Lukas Hebeisen
Senior VP Cloud & Datacenter Solutions

De grands fournisseurs suisses tels que Swisscom se positionnent explicitement comme des partenaires de confiance pour les infrastructures numériques et proposent des solutions cloud avec stockage des données en Suisse. Ils répondent ainsi aux exigences spécifiques en matière de protection des données et de souveraineté, lesquelles sont décisives pour de nombreuses entreprises.

Outre la conservation des données en Suisse, il est également important de connaître le droit auquel le fournisseur est soumis. Il faut savoir que les fournisseurs américains sont soumis au droit américain, même si les données se trouvent dans des centres de données suisses.

«Plus AI ou Minus AI?» – conséquences sur la souveraineté numérique

Le débat actuel autour de l'intelligence artificielle est de plus en plus marqué par un champ de tension que l'on peut globalement diviser en deux camps: Plus AI – regard optimiste sur les possibilités technologiques – et Minus AI – regard réaliste à critique sur les risques, les dépendances et la perte de contrôle. Ce champ de tension est particulièrement important pour les entreprises suisses, car il influence la question de la souveraineté numérique dans des proportions inédites.

D'une part, l'utilisation de l'IA offre des avantages considérables: automatisation des tâches répétitives, augmentation de l'efficacité, prise de décision basée sur des données et nouveaux modèles d'innovation. Les entreprises qui utilisent l'IA de manière systématique et responsable se créent un net avantage concurrentiel et peuvent renforcer leur résilience numérique. Dans ce contexte, l'IA peut même être un moteur de souveraineté, à condition que les entreprises conservent la maîtrise de leurs données, de leurs modèles et de leurs chaînes de valeur.

> « La souveraineté numérique naît de l'identification des données et applications critiques et du choix de solutions locales fiables. Cela n'exclut pas l'utilisation de services globaux innovants pour des domaines moins critiques.

Thomas Stemmler
Head of Regulatory & Policy

D'un autre côté, les technologies IA renforcent les risques liés à la transformation numérique. Chaque nouvelle génération de systèmes d'IA accroît la dépendance vis-à-vis de grands fournisseurs technologiques, souvent internationaux. Les modèles, les données d'entraînement, l'infrastructure et la maintenance échappent souvent au contrôle direct des entreprises. Le risque de «Shadow AI», soit l'utilisation d'outils d'IA non autorisés ou non contrôlés dans le quotidien professionnel, prend de l'ampleur et affaiblit les structures de gouvernance existantes. À cela s'ajoute la complexité croissante des prescriptions réglementaires, qui rend encore plus difficile l'utilisation conforme au droit de l'IA. Dans ce scénario «Minus AI», la souveraineté numérique devient rapidement un défi, voire une illusion.

L'impact de l'IA sur la souveraineté numérique ne dépend pas de la technologie en tant que telle, mais plutôt de l'usage qu'en font les entreprises. Un choix conscient des partenaires, des flux de données transparents, une gouvernance claire de l'IA, des compétences internes et des mécanismes de protection techniques déterminent dans une large mesure si l'IA génère un gain de souveraineté ou une perte de contrôle. Les entreprises qui investissent dans ces compétences peuvent utiliser l'IA comme un levier stratégique, non seulement à des fins d'efficacité et d'innovation, mais aussi de préservation de leur souveraineté numérique.

Recommandations d'action: que peuvent faire les entreprises pour conserver leur souveraineté numérique?

Pour que la souveraineté numérique ne devienne pas illusoire, les entreprises suisses doivent adopter les mesures suivantes:

- **Pilotage stratégique:** définissez une stratégie claire en matière de numérisation et de données, qui régit également les relations avec les prestataires externes et les services cloud.
- **Évaluation et gestion des risques:** analysez régulièrement les risques liés à l'externalisation et à l'utilisation du cloud et développez des plans d'urgence en cas de perte ou d'utilisation abusive des données. Évaluez également les conséquences d'une perte d'accès à court terme à vos systèmes informatiques ou d'un changement soudain des conditions-cadres par un fournisseur.
- **Mesures techniques et organisationnelles:** utilisez le cryptage, la gestion des accès et la surveillance pour rendre les flux de données et les accès transparents et contrôlables.
- **Couverture contractuelle:** veillez à définir des règles contractuelles claires en matière de protection des données, d'accès aux données, de portabilité des données et de stratégies de sortie en cas de changement de prestataire.
- **Choix judicieux du partenaire:** privilégiez des prestataires qui garantissent la conservation et le traitement des données en Suisse. Vérifiez régulièrement le respect des normes convenues.

- **Formation et sensibilisation:** formez régulièrement vos collaborateur·trice·s à la gestion des données sensibles et aux risques de la transformation numérique.
- **Monitoring réglementaire:** suivez l'évolution de la protection des données et adaptez en permanence vos processus aux nouvelles exigences légales.

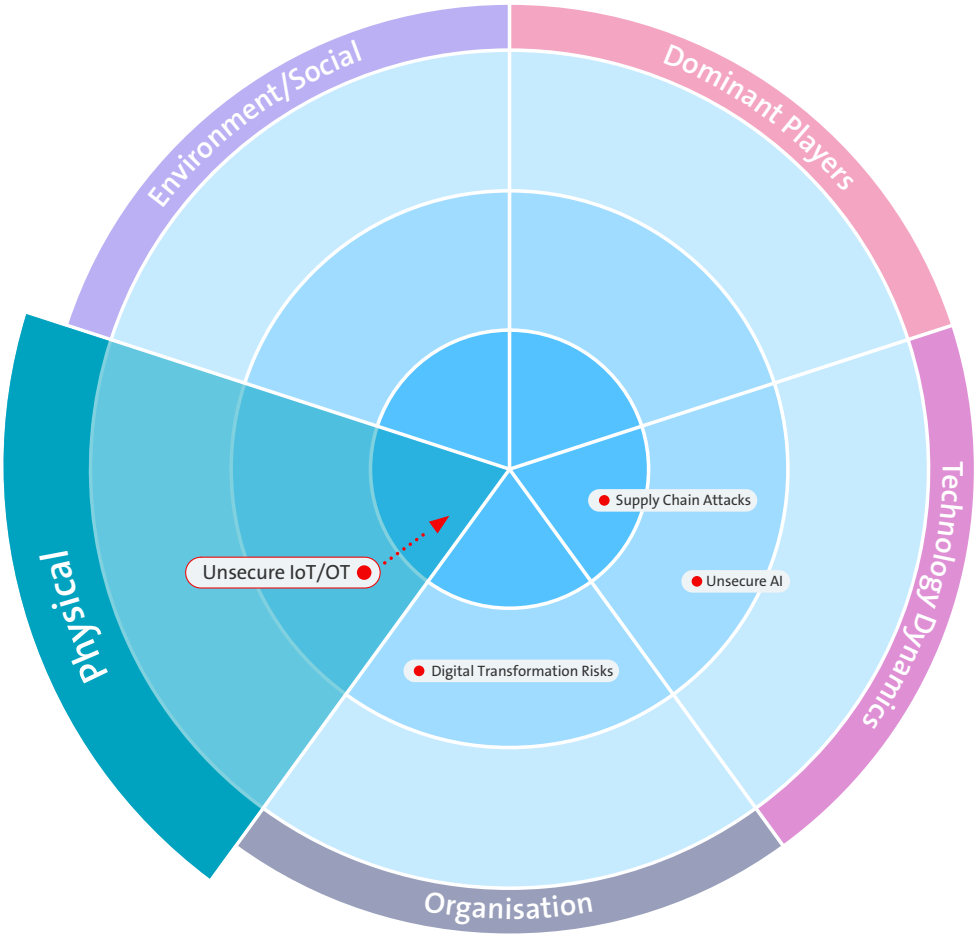
La souveraineté comme objectif

Dans une économie mondialisée et numérisée, le contrôle total de tous les processus et données numériques n'est guère réaliste. La souveraineté numérique reste un objectif ambitieux dont les entreprises ne peuvent se rapprocher qu'en combinant pilotage stratégique, compétence technique et choix rigoureux des partenaires. L'externalisation et l'utilisation du cloud n'impliquent pas nécessairement une perte de contrôle, à condition que les entreprises prennent les bonnes mesures et gèrent activement leurs risques. Cette tâche est complexe et nécessite des connaissances très spécialisées. Il est essentiel de définir de manière réfléchie quelles compétences sont développées en interne et lesquelles sont externalisées.

La connaissance des risques, une action proactive et le choix de partenaires dignes de confiance permettent d'organiser la transformation numérique avec succès et en toute sécurité – pour ne pas se laisser engloutir dans le tourbillon de la transformation mais en ressortir plus solide.

Défis et tendances

La sécurité OT: le sujet tabou qu'on ne peut plus ignorer



Quel est le point commun entre les installations de production, les infrastructures d'approvisionnement, les systèmes de transport, les appareils médicaux et la domotique? Ces dernières années, bon nombre de ces systèmes essentiels à l'exploitation des entreprises ont été fortement négligés du point de vue de la cybersécurité et sont désormais davantage exposés aux menaces. Les attaques contre les infrastructures critiques ont augmenté sous l'effet de la numérisation croissante de la production, de l'intérêt croissant des cybercriminels pour les «proies faciles» et de l'évolution de la situation mondiale en matière de sécurité.

Les risques qui en résultent pour les entreprises sont multiples: coûts élevés dus à des machines endommagées, production inutilisable, atteintes à la réputation, dommages environnementaux, voire dangers immédiats pour la vie et l'intégrité physique des collaborateur·trice·s. Ces risques ont longtemps été un sujet tabou que personne ne voulait aborder. Cette période est désormais révolue: les risques sont de plus en plus évidents et ne peuvent plus être ignorés.

L'Operational Technology (OT) englobe tous les systèmes qui commandent, surveillent, automatisent et interagissent avec le monde réel: de la technique du bâtiment aux appareils médicaux hospitaliers en passant par les chaînes de production et les réseaux d'approvisionnement en énergie. Les frontières entre IT et OT s'estompent progressivement sous l'effet de la montée en puissance de la connectivité (industrie 4.0 et IoT). L'interface entre IT et OT constitue le point le plus critique des architectures d'installations modernes. Alors que le paradigme de la confidentialité domine dans l'informatique, l'OT met l'accent sur la disponibilité et le temps de réaction immédiat. Un redémarrage du système après une mise à jour de sécurité, procédure courante en informatique, peut entraîner un arrêt de la production dans l'OT et impacter directement le bilan.

Les principaux défis sont les suivants:

- **Diversité des protocoles:** les systèmes OT utilisent souvent des protocoles propriétaires ou obsolètes qui n'ont à l'origine pas été conçus pour être connectés à Internet.
- **Différents cycles de vie:** alors que le matériel informatique est renouvelé tous les 3 à 5 ans, les installations OT, y compris les systèmes d'exploitation obsolètes pour lesquels il n'existe plus de correctifs de sécurité, sont souvent utilisées pendant des dizaines d'années.
- **Transit de logiciels malveillants:** les interfaces non sécurisées permettent aux ransomwares de passer directement du réseau bureautique au niveau de commande (API/PLC) et de manipuler physiquement la production.
- **L'«Air Gap» n'offre pas une protection absolue:** il suffit que l'ordinateur portable d'un technicien soit compromis pour qu'un code malveillant pénètre directement au cœur de la production. Grâce à cet accès direct, les assaillants contournent les mécanismes de défense informatique classiques et peuvent exploiter directement les faiblesses des composants industriels.

Les systèmes OT historiques datent d'une époque antérieure à la mise en réseau. Ils sont souvent basés sur des logiciels obsolètes sans authentification moderne, tandis que des processus de certification rigides bloquent les correctifs de sécurité nécessaires. Résultat: les mécanismes de sécurité informatique standard sont souvent techniquement inapplicables

dans ces environnements ou peuvent entraîner des défaillances imprévisibles.

Quels sont les enjeux pour les entreprises?
Les risques s'étendent des arrêts de production dus au sabotage ou à la manipulation à la perte de réputation, voire à la mise en danger de vies humaines dans les infrastructures critiques telles que l'énergie, l'eau ou les soins de santé. Les conséquences juridiques et réglementaires doivent également être prises en compte, car le non-respect des consignes de sécurité peut entraîner des amendes considérables ou des risques de responsabilité.

De nombreuses entreprises sous-estiment ce risque, car elles ont été épargnées jusqu'ici. Pourtant, des attaques spectaculaires comme Stuxnet, BlackEnergy, Colonial Pipeline ou celles visant des centrales hydroélectriques en Pologne et en Norvège prouvent que les systèmes OT sont dans le collimateur des pirates et que la menace est bien réelle.

Pression réglementaire
Le législateur et les régulateurs prennent de plus en plus au sérieux les dangers qui pèsent sur les infrastructures critiques. La mise à jour de l'ordonnance sur l'approvisionnement en électricité de la Suisse, qui impose aux entreprises énergétiques de s'aligner sur le standard minimal TIC, ou encore la réglementation NIS2 de l'UE, qui s'applique également à de nombreuses entreprises suisses ayant des clients dans l'UE, témoignent de cette sensibilité accrue.

Que peuvent faire les entreprises?
La bonne nouvelle est que des approches éprouvées permettent de renforcer la sécurité OT: Identify, Protect, Detect, Respond & Recover – ces étapes bien connues du NIST Framework contribuent également à structurer la sécurité OT.

Identify: comme presque toujours, la première étape est la transparence. Les entreprises doivent avoir une vision claire des systèmes OT existants, de la manière dont ils communiquent entre eux, avec l'informatique ou Internet, et des systèmes présentant des vulnérabilités critiques. Un inventaire régulièrement mis à jour constitue la base de toute gestion des risques.

Protect: la meilleure séparation possible entre l'OT et l'IT, la segmentation granulaire du réseau OT et, si possible, la protection des

« Les cycles de vie étendus et les systèmes propriétaires ne peuvent plus servir d'excuse. À mesure que la connectivité s'accroît, il devient impératif de protéger les systèmes OT de manière aussi systématique que l'informatique classique.

Thomas Dummermuth
Head of Physical Security

endpoints et la gestion des vulnérabilités constituent des mesures préparatoires importantes pour réduire les risques. Cette approche implique également de limiter l'accès aux systèmes OT par une gestion des accès rigoureuse.

La sensibilisation des collaborateur·trice·s représente un facteur déterminant. La maîtrise des risques spécifiques et des bonnes pratiques permet de contribuer activement à la sécurité au quotidien.

Detect: une surveillance continue est parallèlement judicieuse. Les réseaux OT doivent être surveillés en permanence afin de détecter les irrégularités et les indicateurs d'attaque et de pouvoir réagir rapidement en cas d'urgence. À cette fin, des systèmes de détection d'intrusion (IDS) spécialement conçus pour les environnements OT permettent de déclencher une alarme en cas de comportement anormal. La définition de ce qui est considéré comme «anormal» dépend fortement du secteur industriel et nécessite des compétences spécifiques de la part du Security Partner.

Respond & Recover: en cas d'incident, il est toutefois essentiel de pouvoir réagir rapidement, y compris en dehors des heures de bureau. Un SOC IT/OT convergent constitue une approche utile, mais implique généralement des adaptations de processus au sein de l'entreprise, telles que la clarification des responsabilités ou des chaînes d'alerte. Celles-là doivent également être coordonnées avec les principaux fournisseurs afin de garantir une remise en état rapide en cas d'incident.

La réalisation de ces étapes requiert l'association étroite des niveaux OT, IT et de la gestion dans la stratégie de sécurité. La gestion des risques liés à la sécurité OT doit figurer à l'ordre du jour de la direction ou du conseil d'administration.

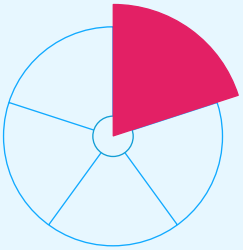
Il est temps de passer à l'action

La sécurité OT ne peut plus être négligée. Une entreprise qui exploite sa production selon des normes de sécurité obsolètes s'expose non seulement à des pertes de production et des dommages économiques, mais met aussi en péril sa réputation et, dans le pire des cas, des vies humaines. Le défi est de taille, mais il est possible de le relever. Il est essentiel que les entreprises abordent le sujet de manière proactive et appréhendent la sécurité OT comme une composante essentielle de la transformation numérique. Nous ne pouvons plus nous voiler la face. Il est grand temps d'agir et d'adopter des mesures adéquates.

« La sécurité OT consiste à exploiter les avantages de l'IT sans compromettre la stabilité de l'exploitation de la production. L'interface entre IT et OT est alors déterminante.

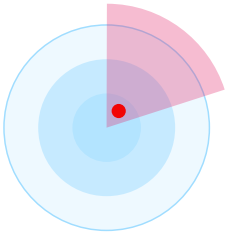
Tobias Balcon
Strategic Program Manager

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



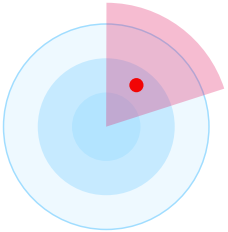
Dominant Players

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



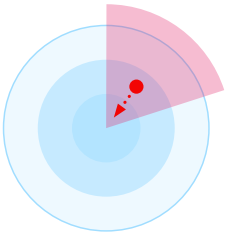
Infrastructure Integrity
Des vulnérabilités peuvent avoir été intégrées délibérément ou par négligence dans des composants essentiels des infrastructures critiques, compromettant ainsi la sécurité du système.

- Inchangé



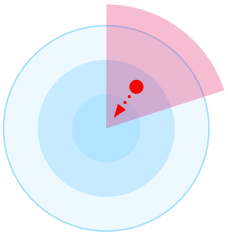
Legacy Protocols
En raison de dépendances logicielles, des protocoles totalement obsolètes et vulnérables (p. ex. NTLMv1, SMBv1, RC4) sont encore utilisés. Quelques applications peuvent ainsi compromettre la sécurité d'infrastructures complètes.

► Inchangé



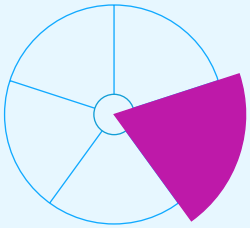
Cloud Ecosystem Dependencies
Les écosystèmes cloud centralisés génèrent des risques de masses compactes et des dépendances qui, en cas de perturbations ou de pressions politiques, peuvent porter gravement atteinte à la souveraineté et à la disponibilité numériques.

▲ Croissant



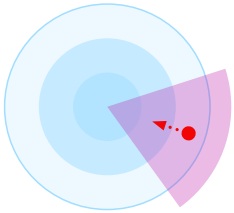
Manipulated Generative AI
Des manipulations ciblées permettent de modifier les résultats d'un système d'IA. L'objectif est alors d'introduire des données malveillantes, fausses ou corrompues dès la phase d'entraînement, de voler des modèles LLM, ou de générer des prompts qui peuvent avoir des effets 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).

▲ Croissant



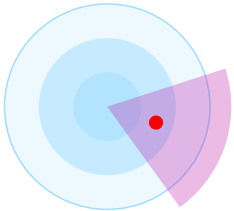
Technology Dynamics

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.



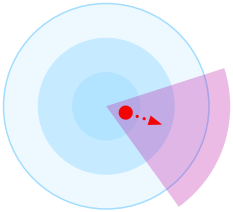
Quantum Computing
Les ordinateurs quantiques peuvent rendre inutiles les procédés cryptographiques actuels, car ils sont en mesure de les contourner en très peu de temps.

▲ Croissant



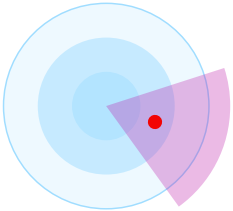
Unsecure AI
Les systèmes d'IA non sécurisés mettent en danger les chaînes d'approvisionnement et la protection des données, car les modèles génératifs peuvent divulguer des données confidentielles de manière incontrôlée. Cela peut non seulement porter atteinte à la continuité des activités, mais aussi 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



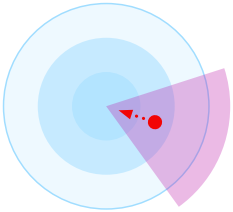
Ransomware
Les données critiques sont cryptées en masse puis (éventuellement) décryptées moyennant le versement d'une rançon.

▼ Décroissant



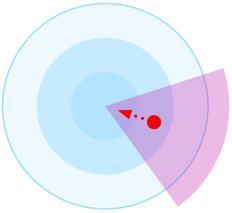
Increased Complexity
La complexité des systèmes, en particulier au-delà des limites des technologies et des entreprises, ne cesse de croître. Les paysages IT se complexifient d'autant plus dans un environnement hybride/multicloud intégrant de nombreux fournisseurs de cloud. L'exposition aux risques augmente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

► Inchangé



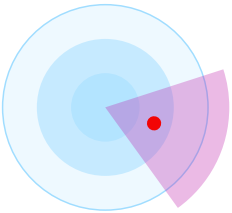
AI-Based Attacks
Les attaques basées sur l'IA sont plus ciblées et donc plus difficiles à détecter. L'IA les rend plus efficaces par le biais de vecteurs d'attaque classiques tels que le ransomware, le phishing, le spear-phishing, ainsi qu'avec de nouveaux modes opératoires moins répandus comme les deepfakes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

▲ Croissant



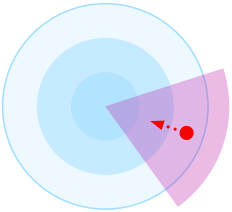
Agentic AI
L'IA agentique est proactive et capable de prendre des décisions et d'adapter des stratégies de manière autonome. Cela augmente la surface d'attaque, car les systèmes d'autoapprentissage et adaptatifs peuvent développer des comportements imprévisibles et interagir de manière indépendante avec 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 une assistance IA apparemment inoffensive peut causer des dommages considérables en raison d'instructions erronées ou de manipulations de la part d'assaillants.

▲ Croissant



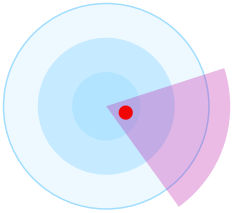
Targeted Attacks
Attaques ciblées et complexes poursuivant un objectif concret. Des personnes clés sont identifiées et attaquées de manière ciblée, directement ou indirectement (Lateral Movement, méthodes d'ingénierie sociale) afin d'obtenir des informations pertinentes ou de causer un maximum de dommages. 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



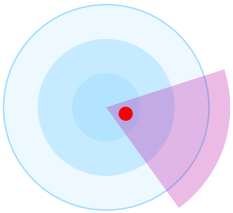
Subscriber Compromise
Des logiciels malveillants se créent un accès aux données privées des utilisateur·trice·s mobiles ou sont utilisés pour cibler les infrastructures IT ou de télécommunication. Les attaques de phishing, smishing, vishing et MFA Bypass ciblent les Subscriber Credentials. Des identités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

▲ Croissant



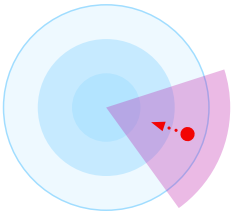
DDoS Attacks
Une attaque par Distributed Denial of Service (DDoS) est une tentative malveillante visant à perturber le trafic de données normal d'un serveur, d'un service ou d'un réseau cible en inondant la cible ou son infrastructure d'un flot de trafic Internet. L'efficacité des attaques DDoS repose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



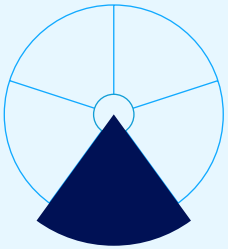
Supply Chain Attacks
Les attaques contre la chaîne d'approvisionnement visent à exploiter les relations de confiance et d'affaires entre une entreprise et des parties externes. Il peut s'agir de partenariats, de relations avec les fournisseurs ou de l'utilisation de logiciels de tiers. Les attaques contre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

► Inchangé



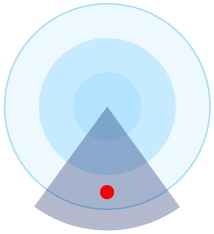
Residential Proxies
Les Residential Proxies sont des connexions établies via des adresses IP réelles et utilisées pour masquer l'origine du trafic de données. Les contrôles de sécurité basés sur la réputation des IP ou la géolocalisation perdent ainsi en efficacité, et les risques tels que le vol d'identifiants et d'informations ou le contournement du géoblocage se trouvent accrus. De ce fait, la protection contre les attaques DDoS devient également plus complexe.

▲ Croissant



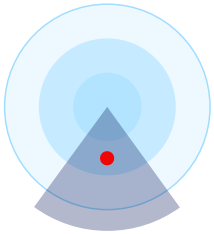
Organisation

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



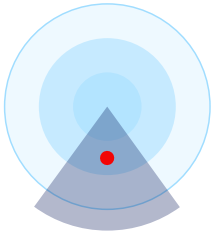
Workplace Heterogeneity
Malgré les nombreuses opportunités qu'offrent les nouveaux modèles de travail comme le «Bring Your Own Device» (BYOD) ou le télétravail, la mise en place incontrôlée de ce type de modèles expose davantage aux risques.

► Inchangé



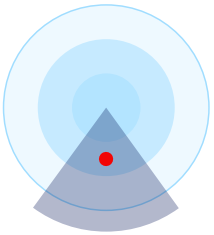
Decentralised Development & Operations
Les départements de développement classiques périclitent tandis que le développement des applications est davantage confié aux Business Units, avec des cycles de release de plus en plus courts. Le contrôle et la gestion de la sécurité deviennent ainsi compliqués.

► Inchangé



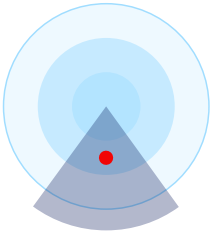
Insider Threat
Des partenaires ou des collaborateur·trice·s manipulent, détournent ou vendent des informations par négligence ou de façon intentionnelle.

► Inchangé



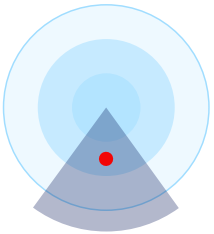
Digital Transformation Risks
L'interconnexion croissante entre le monde réel et le monde virtuel dans la vie privée et professionnelle multiplie l'éventail des vecteurs d'attaque. Le nouveau modèle «New Work» et la transposition opérée dans des environnements de télétravail renforcent également les cyberrisques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

► Inchangé



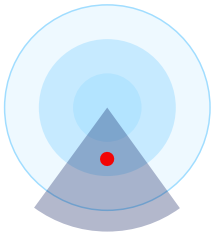
Security Skills
La complexité des cyberattaques et la progression de la numérisation rendent les Security Skills et le recours à des cyberprofessionnels indispensables dans l'organisation. Une menace de «Downskilling», à savoir le désapprentissage des connaissances lié à l'automatisation dans l'informatique 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



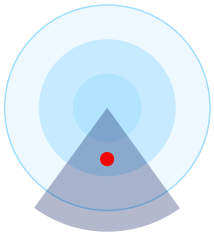
Fragile Workforce
Une organisation de travail fragile décrit la vulnérabilité des équipes de cybersécurité et de cyberdéfense face à la charge psychique et à l'absence de prévention du stress et du burnout. Lorsqu'une personne est psychologiquement instable et ne peut pas agir correctement sous pression, 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.

► Inchangé



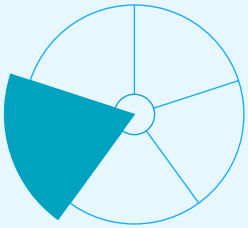
Infrastructure Misconfiguration
Exploitation de composants de l'infrastructure mal configurés et/ou de vulnérabilités identifiées et corrigées tardivement. L'automatisation renforcée des processus d'exploitation techniques aura des conséquences plus importantes en cas d'attaques efficaces ou de configurations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

► Inchangé



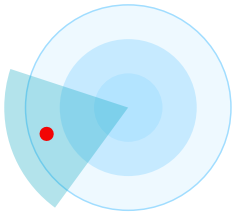
Fraud
La fraude désigne des actes frauduleux basés sur la tromperie et l'enrichissement illicite. Elle se manifeste par des transactions falsifiées, des vols d'identité ou la manipulation de documents. Pour les entreprises et les particuliers, la fraude représente un danger considérable, car elle peut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

► Inchangé



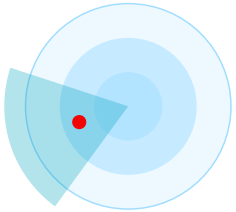
Physical

Ce terme désigne les attaques sur l'infrastructure du cyberspace 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.



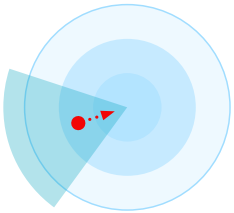
Energy Instability
Attaques sur des infrastructures critiques telles que celles des exploitants du réseau électrique. La sûreté de fonctionnement est essentielle et la Business Continuity alimente de plus en plus le débat sur la cyberrésilience. La pénurie d'électricité, le black-out (panne générale 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



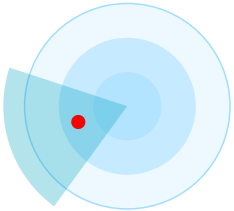
Targeted Sabotage
Attaques ciblées contre des infrastructures, des installations d'approvisionnement et des connexions, qui peuvent restreindre de manière considérable le fonctionnement d'Internet. Le sabotage ciblé des câbles à fibre optique sensibles se développe actuellement et constitue un danger 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



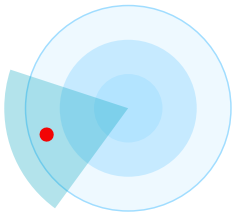
Unsecure IoT/OT
Qu'il soit déployé dans des technologies opérationnelles (OT) pour la surveillance et la gestion de processus, des appareils et infrastructures physiques ou dans des appareils IoT, l'Internet des objets est omniprésent. Des tâches très variées – des plus simples au plus complexes – y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



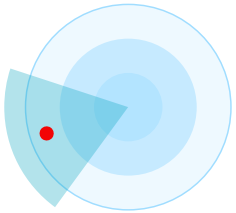
Environmental Influence
Les effets du changement climatique et de l'urbanisation entraînent une multiplication des phénomènes et influences météorologiques imprévisibles tels que la chaleur, les fortes pluies, les tornades, la grêle ou les éclairs intenses. Ces phénomènes affectent la résilience des infrastructures et peuvent ainsi causer d'importants dommages sur l'environnement externe et interne d'un système d'information ou d'un réseau.

► Inchangé



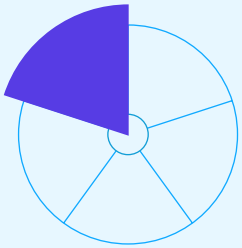
UAS Threats
Les UAS Threats (Unmanned Aerial System Threats) désignent les risques liés à l'utilisation d'aéronefs sans pilote, autrement dit les drones. Ces risques s'étendent de l'espionnage, la surveillance, le vol de données, la contrebande et le sabotage en passant par les attaques physiques contre les infrastructures ou le personnel. Dans le contexte de l'entreprise, les scénarios les plus pertinents concernent l'espionnage industriel, la surveillance aérienne des sites d'usine et la perturbation d'installations sensibles. La diffusion et l'autonomie croissantes des technologies de drones renforcent considérablement la menace qui pèse sur la sécurité.

► Inchangé



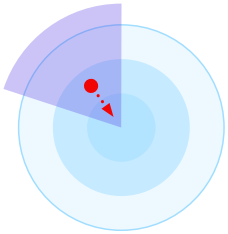
Hybrid Warfare
L'association de moyens militaires classiques avec des tactiques non militaires telles que les cyberattaques, la désinformation, la pression économique ou l'influence politique est qualifiée de guerre hybride. Les attaques étant souvent dissimulées et menées en dessous du «seuil de guerre», elles sont difficiles à identifier et à contrer. Elles visent à déstabiliser les États, saper la confiance et encourager la division sociale. Leur efficacité est amplifiée par la numérisation, les réseaux sociaux et à l'interconnexion mondiale.

► Inchangé



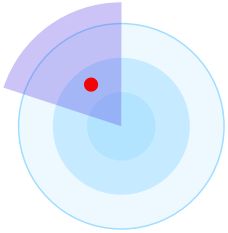
Environment/Social

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.



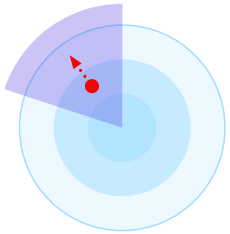
Identity Theft & Impersonation
Les identités numériques personnelles certifiées peuvent être volées ou détournées pour usurper l'identité d'une personne ou d'une organisation. Les attaquants peuvent ainsi accéder sans autorisation à des systèmes et à des informations, ou effectuer des actions au nom de tiers telles que la conclusion de contrats, des paiements ou des communications.

▲ Croissant



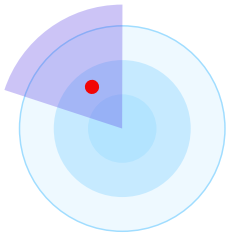
Geopolitical Situation / State Level Attacks
En périodes de guerres, de terreur et d'instabilité politique au sein des pays et des sociétés, les conséquences négatives dans le cyberespace tendent à s'accentuer. Il s'agit de piratages commandités par différents pays et groupes de hacktivistes à motivation 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.

► Inchangé



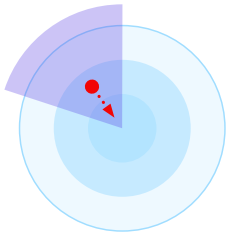
Security Job Market
Les besoins énormes en professionnels de la sécurité sont très difficiles à satisfaire. Il en résulte une perte de savoir-faire dans la lutte contre des attaques de plus en plus complexes et intelligentes.

▼ Décroissant



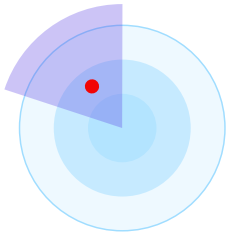
Disinformation & Destabilisation
La diffusion intentionnelle d'informations erronées peut entraîner une déstabilisation économique et sociale. Son utilisation ciblée dans les scénarios de crise, y compris via le cyberespace, se développe de plus en plus.

► 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.

▲ Croissant



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

Conclusion

La transformation numérique entraîne une dépendance de plus en plus forte vis-à-vis d'écosystèmes externes.

Les plateformes cloud, les chaînes d'approvisionnement logicielles, les modèles d'IA et les systèmes de contrôle industriels sont hautement interconnectés et échappent souvent au contrôle direct des entreprises. Les limites de sécurité classiques sont redéfinies en conséquence. La confiance seule ne suffit plus – la sécurité doit être traçable, vérifiable et maîtrisable. L'origine, l'intégrité et les dépendances des logiciels, des données et des systèmes doivent être transparentes et gérées de manière proactive.

Cette nécessité se manifeste particulièrement lors d'attaques de la chaîne d'approvisionnement et de la souveraineté numérique. La méconnaissance du processus de développement des logiciels, du lieu de traitement des données ou des conditions-cadres juridiques auxquelles les fournisseurs sont soumis entraîne un risque de perte de contrôle et des conséquences potentiellement majeures pour l'ensemble de l'entreprise. Les évolutions réglementaires telles que la NIS2 et le CRA ou les lois sur la protection des données accentuent cette pression et font de la sécurité traçable la norme.

L'intelligence artificielle agit comme un accélérateur. Elle peut accroître la productivité, l'innovation et la résilience, mais en l'absence de gouvernance, elle renforce les risques existants tout au long de la chaîne de création de valeur. Les modèles opaques, le risque de «Shadow AI», la perte de compétences et nouvelles surfaces d'attaque le montrent clairement: l'enjeu n'est pas l'utilisation de l'IA en tant que telle, mais la manière dont elle est déployée, contrôlée et gérée.

La sécurité OT et IoT est un domaine souvent sous-estimé et pourtant critique. La convergence croissante de l'IT et de l'OT fait des installations de production et des infrastructures critiques des cibles de choix. La sécurité OT ne peut plus être traitée comme une discipline technique secondaire, mais doit figurer à l'ordre du jour de la direction.

L'état des menaces 2026 révèle que les risques émergent de plus en plus à l'interface entre technologie, organisation et géopolitique. La résilience devient une compétence clé – sur les plans technique, organisationnel et culturel.

Les plus grands dangers apparaissent là où la complexité se heurte à un manque de transparence, l'automatisation à un manque de responsabilité, et la rapidité à un manque de compétence. La réponse ne réside pas dans un outil unique, mais dans une approche globale. Celle-là nécessite des stratégies claires, une sécurité traçable, un choix conscient des partenaires, une formation continue régulière et une culture de la sécurité incarnée de manière active et crédible par les cadres.

Les évolutions mises en lumière dans l'actuel Cybersecurity Threat Radar montrent clairement que la cybersécurité n'est plus seulement une discipline technique, mais un facteur de succès stratégique. La cybersécurité n'est pas un état, mais un processus stratégique continu. Sa gestion active permet de renforcer la résilience, la confiance et la souveraineté numérique.

#EngageYourSecuritySkills

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

Édition
OK DIGITALDRUCK AG, Zurich

Tirage
140 exemplaires

La cybersécurité conditionne aujourd'hui la confiance et la capacité d'action, car la transformation numérique, l'IA et les dépendances géo-politiques abolissent les frontières de sécurité, faisant de la sécurité transparente et traçable ainsi que de la résilience globale une obligation stratégique.

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? Alors dépose ta candidature ici: swisscom.com/securityjobs

#EngageYourSecuritySkills