swisscom

# Cyber Security Threat Radar
# 2020/2021

Résilience et agilité de rigueur dans les entreprises

# Table des matières



## Colophon


| | |
|---|---|
| **Éditeur** | Swisscom SA, Group Security |
| **Conception/réalisation** | Agence Nordjungs, Zurich |
| **Rédaction** | Swisscom SA, Group Security |
| **Copyright** | © Avril 2021 by Swisscom (Suisse) SA, Group Security, Alte Tiefenaustrasse 6, 3048 Worblaufen, swisscom.ch |
| **Édition** | OK DIGITALDRUCK AG, Zurich |
| **Tirage** | 125 exemplaires |




*«Les situations particulières exigent des mesures particulières lorsqu'il s'agit de sécurité, de protection et de sensibilisation aux risques.»*

**Philippe Vuilleumier**
Head of Group Security
Swisscom (Suisse) SA

# Introduction du Cyber Security Threat Radar

En cette période aussi particulière que disruptive, il est important de garder le contrôle de la situation. Beaucoup de gens se demandent si la pandémie de coronavirus a accru les cyberactivités. Sommes-nous devenus plus vulnérables à cause du télétravail, de la distanciation sociale et de l'incertitude ambiante? Notre réponse **n'est pas tranchée.**

Les situations particulières exigent des mesures particulières lorsqu'il s'agit de sécurité, de protection et de sensibilisation aux risques. Il est vrai qu'externaliser toute l'infrastructure IT chez les collaboratrices et collaborateurs a posé bien des difficultés à bon nombre d'entreprises et d'organisations.

Mais la situation actuelle induit-elle une hausse des attaques? Y a-t-il davantage de vecteurs d'attaque potentiels? Difficile d'être catégorique. Nos experts opérant dans les différents Security Operation Centers de Swisscom surveillent toute l'infrastructure réseau en Suisse et n'ont pas constaté de recrudescence du piratage ou des vagues d'attaque par hameçonnage et ransomware.

Mais alors que penser des articles signalant un nombre croissant d'attaques à l'encontre des cliniques suisses? Qu'en est-il des cyberincidents dans plusieurs entreprises suisses, qui ont été rapportés par les médias? Il y en a eu aussi en 2020 – mais étaient-ils dus au coronavirus? Clairement non. Les failles organisationnelles, opérationnelles ou techniques existaient bien avant la situation particulière actuelle. Swisscom n'a pas non plus été épargnée par les pannes de réseau en 2020. Nous avons su régler les dérangements dans des délais rapides, ils n'en laissent pas moins un goût amer. Pour de nombreuses entreprises et organisations, l'objectif est de transformer les faiblesses en forces et d'instaurer une culture de la sécurité en initiant des changements sur le plan technique, organisationnel et opérationnel, afin de pouvoir envisager un avenir sous le signe de la résilience.

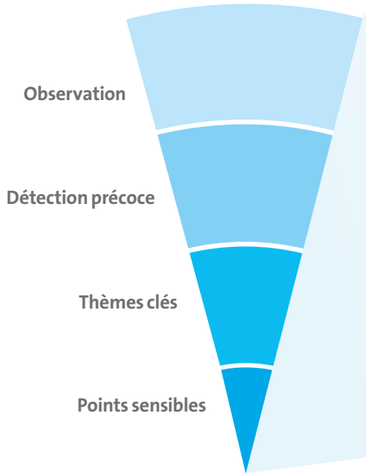
Le présent Cyber Security Threat Radar 2020/2021 vise à évaluer le niveau de menace actuel et ainsi à donner une vue d'ensemble des cyberrisques et de la menace qu'ils représentent. Il passe au crible les tendances et les défis, les évalue et définit le niveau de menace en Suisse et ses conséquences en s'appuyant sur un concentré d'expertise. Il décrit les motivations et les moyens des hackers.

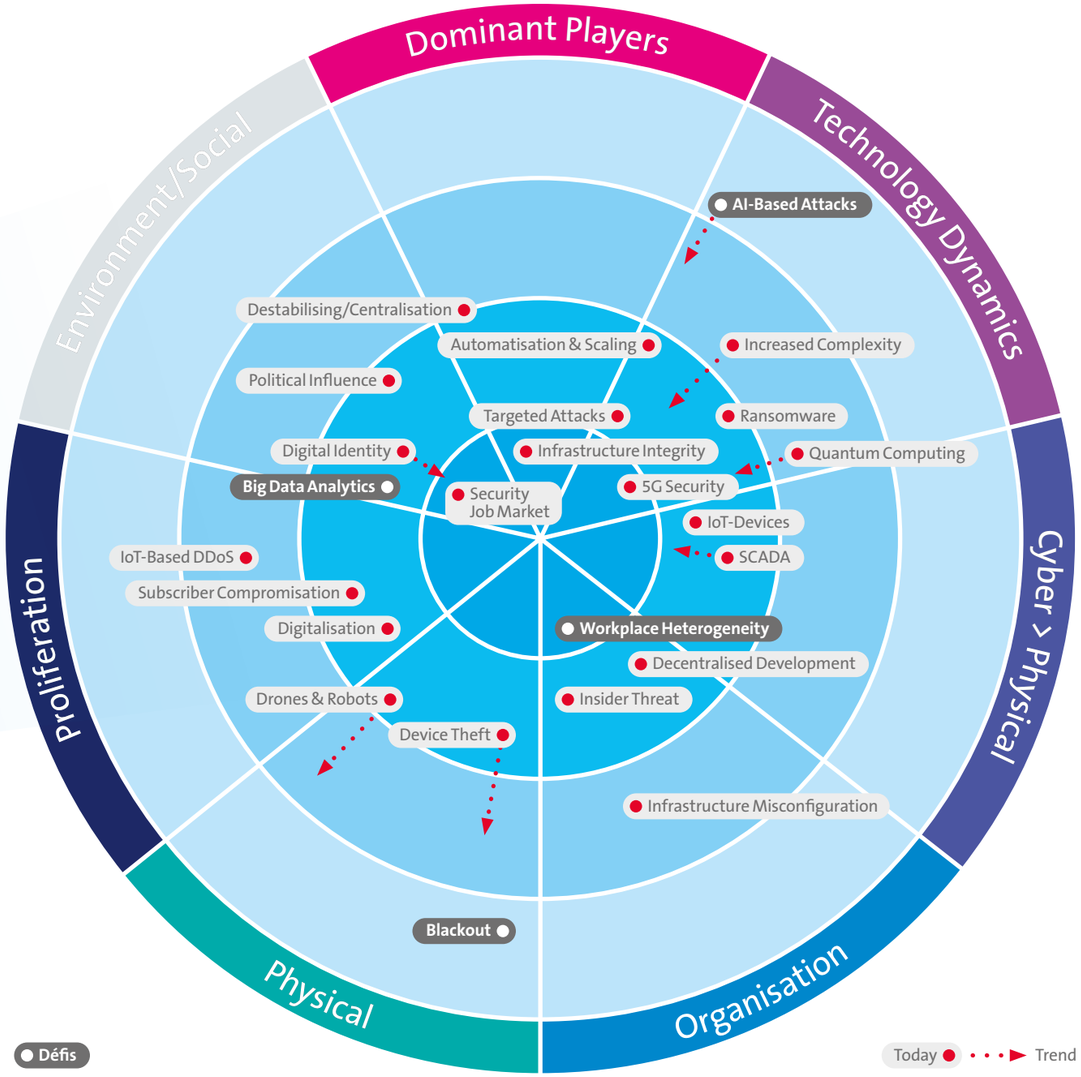
À partir des données collectées et analysées par Swisscom, il précise également les méthodes et les outils les plus souvent utilisés par les hackers. En outre, il présente des mesures préventives particulièrement efficaces pour pouvoir détecter au mieux une attaque. Le Cyber Security Threat Radar 2020/2021 sert de guide et de boussole pour évoluer en toute sécurité dans le cybermonde.

# État des lieux – introduction au radar des menaces

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

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



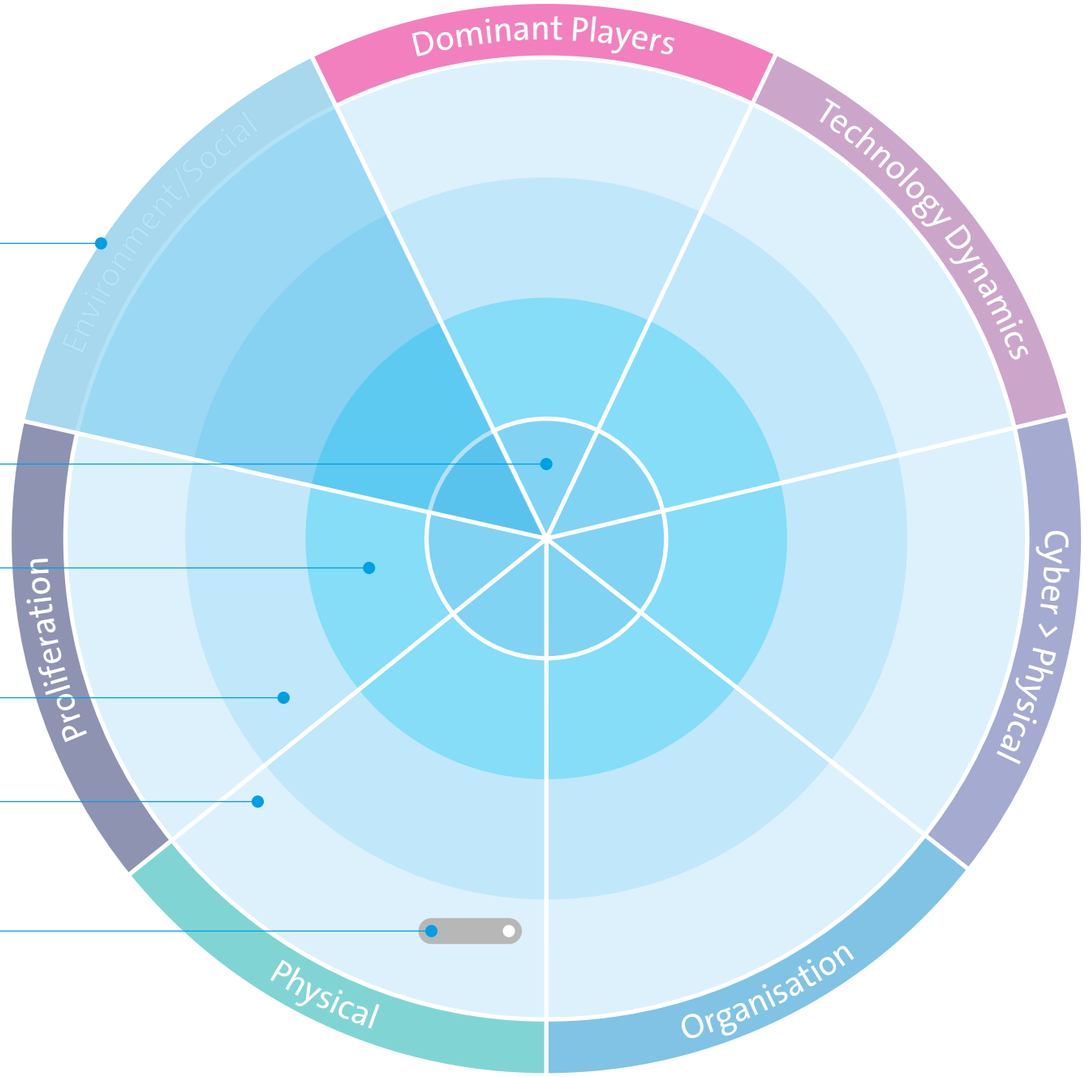
# Méthodologie

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

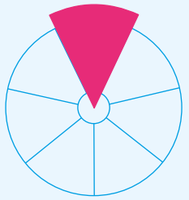
**Ces cercles mettent en évidence:**

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

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

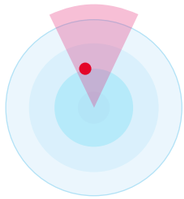


# Zoom sur les tendances et évolution sur un an



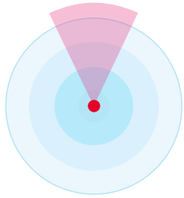
## Dominant Players

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



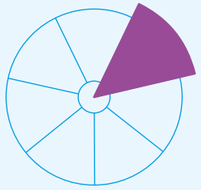
**Destabilising/Centralisation**
La forte centralisation au sein de la structure de l'Internet induit des risques cumulés. La défaillance d'un service, par exemple une panne d'Amazon Web Services (AWS), peut avoir des répercussions dans le monde entier.

► Inchangé



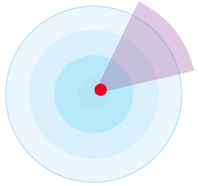
**Infrastructure Integrity**
Des vulnérabilités peuvent avoir été intégrées délibérément ou par négligence dans des composants essentiels des infrastructures critiques, compromettant ainsi la sécurité du système.

► Inchangé



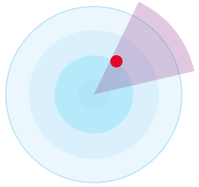
# Technology Dynamics

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



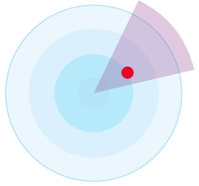
**5G Security**
La 5G est une technologie encore récente. Son déploiement crée de nombreuses opportunités, mais s'accompagne aussi de menaces encore inconnues.

▲ Niveau de menace croissant



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

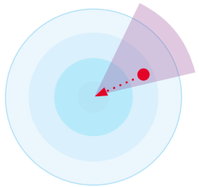
▲ Niveau de menace croissant



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

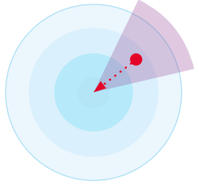
▼ Niveau de menace décroissant





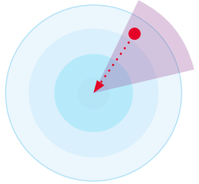
**Quantum Computing**
Les ordinateurs quantiques peuvent rendre inutiles les procédés cryptographiques actuels, compte tenu de leur capacité à les craquer en un rien de temps.

► Inchangé



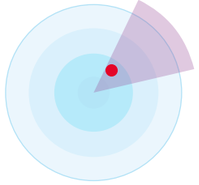
**Increased Complexity**
La complexité des systèmes ne cesse de croître, notamment hors du cadre technologique de l'entreprise. Cela augmente l'exposition aux risques et complique la recherche d'erreurs.

► Inchangé



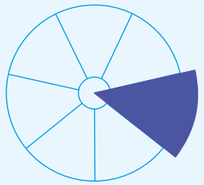
**AI-Based Attacks**
Les attaques au moyen de l'intelligence artificielle (AI) sont plus ciblées et ainsi plus difficiles à détecter. Grâce à l'AI, elles peuvent se révéler plus efficaces sur des vecteurs d'attaque classiques tels que le ransomware, l'hameçonnage et le spear phishing, ainsi que sur de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

▲ Niveau de menace croissant



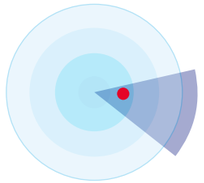
**Targeted Attacks (APTs)**
Des attaques ciblées et complexes poursuivant un objectif concret. Les personnes clés sont identifiées et ciblées directement ou indirectement (lateral movement) afin d'obtenir des informations sensibles ou de causer un préjudice maximal. La persistance est un aspect essentiel,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

► Inchangé



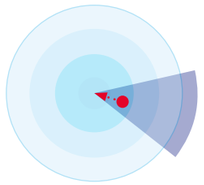
# Cyber > Physical

**Ce terme regroupe les attaques utilisant l'infrastructure du cyberespace et causant davantage de dégâts dans le monde physique.**



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

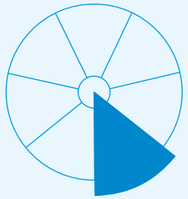
► Inchangé



**SCADA**
Il existe encore de nombreux systèmes de contrôle mal ou non protégés pour les éléments d'infrastructure critique.

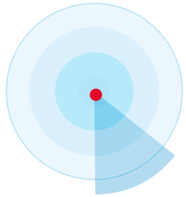
► Inchangé





# Organisation

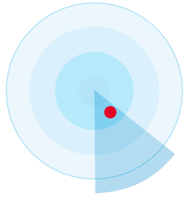
**Cette tendance désigne les menaces résultant des changements dans les organisations ou consistant à exploiter les failles de ces dernières.**



**Workplace Heterogeneity**

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

▲ Niveau de menace croissant



**Decentralised Development**

Les départements de développement classiques périclitent; le développement d'applications est confié davantage aux Business Units, avec des cycles de release toujours plus courts.

► Inchangé

**Insider Threat**

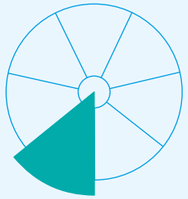
Des partenaires ou des collaborateurs manipulent, détournent ou vendent des informations par négligence ou de façon intentionnelle.

▲ Niveau de menace croissant

**Infrastructure Misconfiguration**

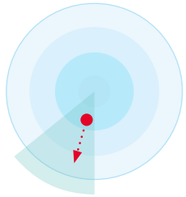
Exploitation d'éléments de l'infrastructure mal configurés et/ou de vulnérabilités identifiés et corrigés tardivement.

▼ Niveau de menace décroissant



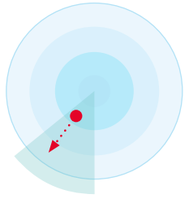
# Physical

**Menaces liées à l'environnement physique et davantage axées sur des cibles physiques en règle générale.**



**Device Theft**
Le vol, notamment de composants de l'infrastructure critique ou de plus en plus d'appareils IoT dans le futur, peut entraîner la perte de données ou compromettre la disponibilité des services.

► Inchangé



**Drones & Robots**
La reconnaissance ou les attaques à grande portée deviennent plus faciles et moins coûteuses. La miniaturisation rend les hackers plus difficiles à détecter.

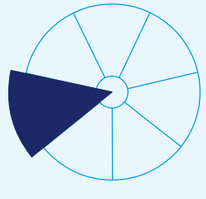
► Inchangé



**Blackout**
Attaques ciblant des infrastructures critiques telles que celles des opérateurs de réseau électrique. La sûreté de fonctionnement est un élément important et le thème de la Business Continuity revient fréquemment dans les débats sur la cyberrésilience.

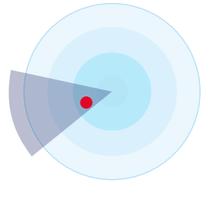
▲ Niveau de menace croissant





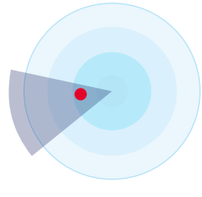
# Proliferation

**Ce segment inclut les menaces résultant de la disponibilité accrue et à moindre coût des connaissances et des supports IT. En effet, leur diffusion offre de nouveaux points d'attaque et accroît la disponibilité des outils de piratage.**



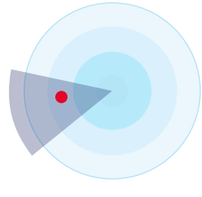
**Digitalisation**
L'interconnexion croissante du monde réel et virtuel dans la vie privée et professionnelle élargit l'éventail des vecteurs d'attaque.

► Inchangé



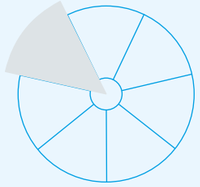
**Subscriber Compromisation**
Des programmes malveillants s'attaquent aux données privées des utilisateurs mobiles ou servent à cibler les infrastructures IT et de télécommunication.

► Inchangé



**IoT-Based DDoS**
Une forte croissance combinée à une faible protection des appareils IoT accroît les prises de contrôle potentielles par le biais des réseaux de bots.

► Inchangé



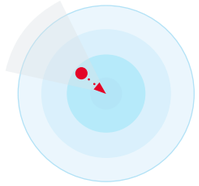
# Environment/Social

**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 les attaques plus profitables.**



**Security Job Market**
La demande en professionnels de la sécurité est difficile à satisfaire, ce qui induit une moindre expertise sur le terrain pour gérer les attaques d’un niveau croissant de complexité et d’ingéniosité.

► Inchangé



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

► Inchangé



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

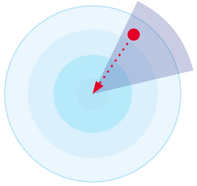
▲ Niveau de menace croissant



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

► Inchangé

# Défis et tendances



**AI-Based Attacks**

## De quoi s'agit-il?

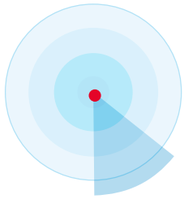
Ces dernières années ont été marquées par des violations de sécurité et de la protection des données. Mais la question des deepfakes et de la désinformation générale était également en ligne de mire.

## Quelle évolution?

L'intelligence artificielle se renforce, acquiert de nouvelles aptitudes et apprend en permanence. Et les avantages et inconvénients de cette technologie – partie pour rester – ont toujours été sous les feux de la rampe.

## Comment réagir au défi ou à la tendance?

- Priorité absolue à la formation et à la sensibilisation du personnel
- Précaution technique avec le SOC pour analyser et identifier ce type d'attaque



**Workplace Heterogeneity**

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

C'est la plus forte évolution dans le radar depuis 2020, avec une requalification en point sensible – une quasi-rupture imputable de toute évidence à la situation de pandémie mondiale. Même après la pandémie, il est certain que le modèle «New Work» reposant sur le télétravail va s'enraciner dans les entreprises et devenir un modèle de travail accepté.

- Adaptation des politiques et directives existantes; sortie du «poste de télétravail» au profit du Mobile Working
- Intégration des standards de sécurité tels que le Privileged Access Management
- Accélération de la gestion des risques agile en l'étendant aux postes de travail mobiles
- Consolidation de l'authentification multifacteur et intégration dans le paysage système
- Instauration d'une culture de la sécurité rigoureuse impliquant le personnel (human centered approach)

**Blackout**

## De quoi s’agit-il?

Attaques ciblant des infrastructures critiques telles que celles des opérateurs de réseau électrique. Les médias montrent que les infrastructures critiques sont nettement plus vulnérables aux cyber-attaques. La sûreté de fonctionnement est un élément important et la Business Continuity revient fréquemment dans les débats sur la résilience.

## Quelle évolution?

Il est certain que les attaques contre les infrastructures critiques vont continuer d’augmenter et s’intensifier. Nous percevons également un risque élevé lié au départ de personnes clés en raison de leur âge pour assurer l’exploitation de systèmes SCADA et une complexité croissante des appareils IoT sur les plateformes des exploitants.

## Comment réagir au défi ou à la tendance?

- Nécessité de mieux tenir compte du Business Continuity Management dans la planification des stratégies de cybersécurité
- Action collaborative et interdisciplinaire dans les entreprises et les organisations
- DevSecOps – mise en place de frameworks dans des configurations agiles et soutien actif
- Renfort de la responsabilité de la première ligne de défense





**Big Data Analytics**

Le volume accru de données et les modèles d’analyse améliorés peuvent être utilisés abusivement pour influencer le comportement des gens par rapport aux données et aux systèmes IT. De plus en plus, la prise de décisions est confiée à des systèmes autonomes. Les données des «big data lakes» sont utilisées de manière abusive à des fins de désinformation, de fake news et d’analyses sociétales et psychosociales. Cela induit une violation de la sphère privée pouvant avoir des conséquences sociétales.

Les données sont le nouvel or noir. C’est du moins ce que titrent souvent les articles scientifiques et la presse spécialisée. Tout l’intérêt réside dans l’appréciation de systèmes sociaux complexes et la disponibilité de données à des fins d’analyse, par exemple dans le secteur de la santé. Dans ce domaine, il existe un fort potentiel de nouveautés, mais aussi un fort risque de surveillance excessive ou de fuite massive de données (d’entreprise) sensibles. La corrélation entre données disponibles et consultables, par exemple via l’OSINT, ouvre également la porte aux cybercriminels et aux experts du social engineering.

- Directives et principes éthiques particulièrement importants ici – vaut aussi pour l’utilisation des données confiées à un tiers
- Nécessité d’une restriction technique et organisationnelle de l’accès aux données
- Davantage sensibiliser: quels Cloud Services utiliser? Quelles données stocker, et où?

# Conclusion

L'année 2020 a été disruptive et difficile pour les organisations et entreprises, le personnel et les départements de sécurité suisses. Mais ce fut aussi une année qui a permis de jeter les bases pour de nouvelles évolutions et perspectives malgré tous les obstacles et restrictions.

Sans surprise, le thème Workplace Heterogeneity s'est hissé au rang de point sensible dans l'édition 2021 du Cyber Security Threat Radar et compte sans aucun doute parmi les plus fortes évolutions observées sur un vecteur de menace ces dernières années. La mise en place du télétravail pour tout le personnel du jour au lendemain a été l'un des défis les plus ardus pour les services IT et de sécurité. Un défi plus ou moins bien relevé selon les cas. Mais dans l'ensemble, les choses se sont bien déroulées. Et cela souligne l'absolue nécessité pour les entreprises et les organisations d'être agiles dans le monde d'aujourd'hui, afin de rester dans la course vis-à-vis de la concurrence, du marché et des exigences sociétales.

Bon nombre d'entreprises et d'organisations ont fait un grand pas en avant en matière de transformation numérique. Mais les grandes innovations manquent, aucune réelle nouveauté n'est apparue. Les outils existants se sont ainsi davantage répandus grâce au «New Way of Working». Les efforts consentis pour améliorer la sécurité de Zoom (passant du zoombombing à la communication cryptée de bout en bout) et l'évolution de Microsoft Office 365 en outil collaboratif sont tangibles et visibles. Le tournant numérique se poursuit à une vitesse fulgurante, souvent au détriment de la sécurité ainsi que de la protection de la sphère privée et des données, comme le prouve à merveille Clubhouse, application de visioconférence tendance.



« Le tournant numérique se poursuit à une vitesse fulgurante, souvent au détriment de la sécurité ainsi que de la protection de la sphère privée et des données, comme le prouve à merveille Clubhouse, application de visioconférence tendance. »

Le Big Data joue un rôle toujours aussi important pour les réseaux sociaux, les nouveaux services collaboratifs et la machine marketing. L'intelligence artificielle prend quant à elle une nouvelle importance avec les actes de piratage de type désinformation (deepfakes, fake news). Les modes d'attaque des cybercriminels deviennent de plus en plus élaborés et prennent une nouvelle dimension. Un phénomène qu'il est impératif d'anticiper.

À cet égard, tout se jouera sur la capacité à observer une culture de la sécurité rigoureuse. La RSA Conference 2020 avait mis l'accent sur l'élément humain, tel un présage de la situation particulière que nous vivons actuellement. L'approche centrée sur le facteur humain, la réponse ciblée à ses besoins, ses exigences et ses problèmes, sa protection et son soutien dans la mise en place des processus de sécurité sont définitivement redevenus une priorité en 2020, une tendance qui se poursuivra en 2021, et bien au-delà. L'adaptation dynamique de l'organisation, de la culture et des processus devient plus cruciale que jamais, au regard des nouveaux vecteurs d'attaque.

Notons que les dangers du monde numérique n'ont pas faibli. Toutefois, nos experts du Security Operation Center de Swisscom n'ont pas constaté de hausse significative. Simplement, ceux-ci ont pris une forme différente en fonction de la situation et souvent ciblé l'humain comme vecteur d'accès. Le collaborateur, dans son rôle de première ligne de défense, reste le maillon principal de la chaîne de sécurité et doit être considéré comme tel.

# Pour un monde interconnecté plus sûr

Swisscom place les besoins des collaborateurs, clients et partenaires au cœur de toutes les problématiques de sécurité.

Nous développons des **solutions, produits et services sûrs** pour nos clients et partenaires. Pour les protéger, nous avons recours à des **technologies de pointe** et à notre **infrastructure complète,** et observons une **culture de la sécurité** rigoureuse.

# #talkingaboutsecurity

**swisscom.ch/security**