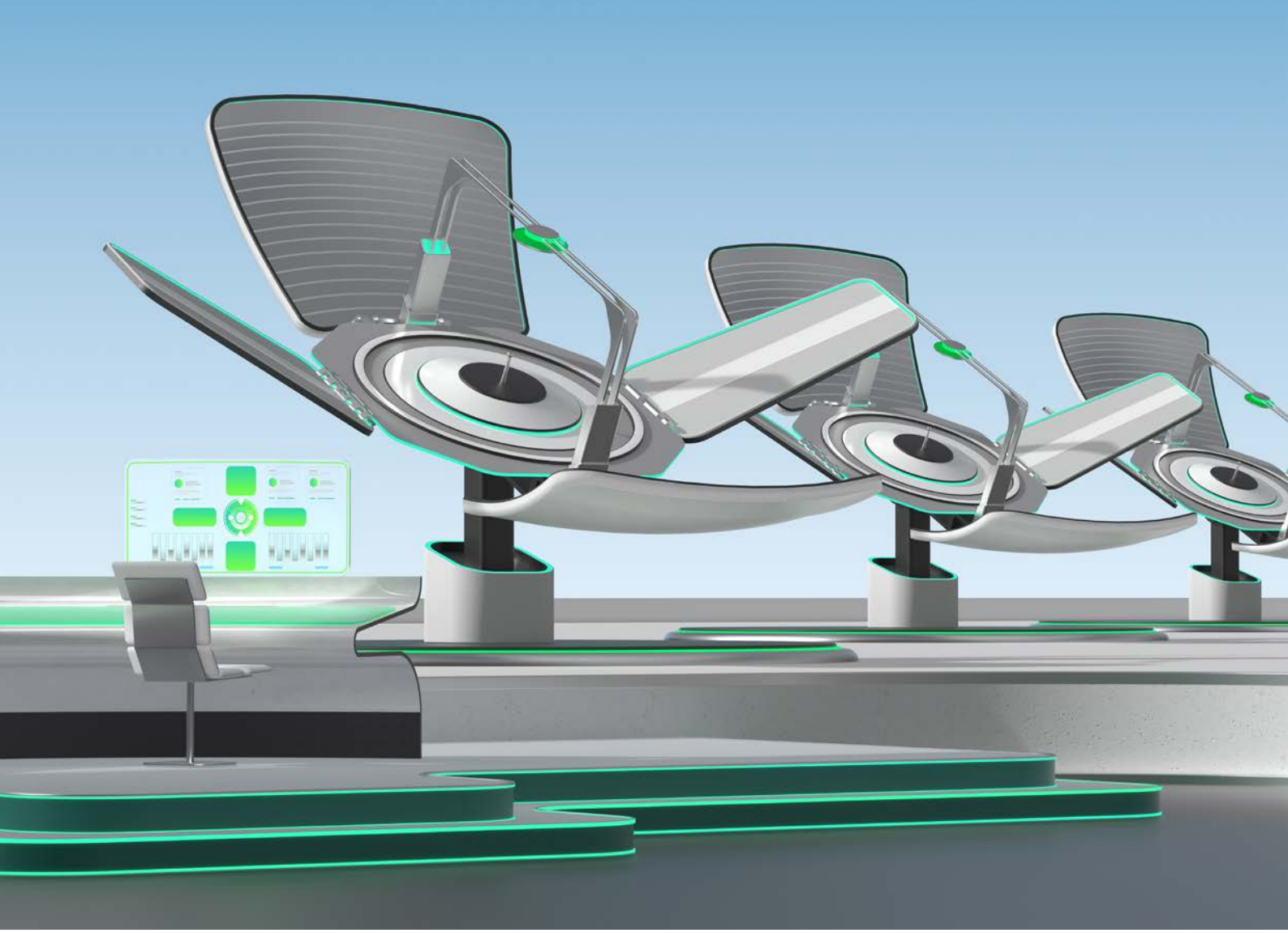


Construire un avenir plus sûr dans les télécommunications

kaspersky PRÊTS POUR L'AVENIR

https://go.kaspersky.com/Telecom.html

2021

Partage distant : les télécommunications participent à la cohésion du monde

Si vous faites partie des leaders dans le domaine des télécommunications en 2021, le monde vous en est immensément redevable. Il est impossible de quantifier la valeur prodigieuse de la contribution de votre secteur au cours de ces deux dernières années.

Le mot « télécommunications » signifie partage à distance (du grec *τῆλε*, distant, et du latin communiquer, partager). Le pouvoir de desservir des entreprises et des personnes éloignées sur le plan social est écrit dans le nom même de votre domaine d'activité et, depuis le choc provoqué par la pandémie, le secteur est largement parvenu à être à la hauteur de son nom.

La croissance a été stable, mais inégale. À mesure que nous avançons vers une véritable « société gigabit », le secteur devra se concentrer sur des moyens innovants pour développer la couverture et la monétiser. Dans cette effervescence, il est absolument essentiel que les responsables dans le domaine des télécommunications adoptent une approche prudente par rapport à l'innovation, en élaborant la cybersécurité à la racine même de leur stratégie.

Dans cet e-book, nous allons examiner les tendances principales que les leaders des télécommunications devront prendre en compte pour conserver une croissance solide en 2022 et au-delà.

Quoi que 2022 nous réserve, n'oubliez jamais à quel point le travail que vous effectuez est important. Après tout, qui était là pour que le monde continue à tourner quand la pandémie s'est déclarée ?

Vous étiez là.

Les tendances

(hyper) développement du cloud

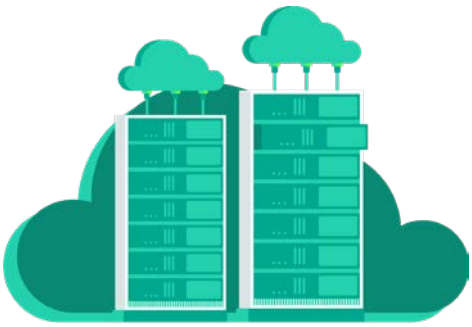
IoT et 5G

Écosystèmes

Travail à distance : travail et croissance hybrides

IA et analyse

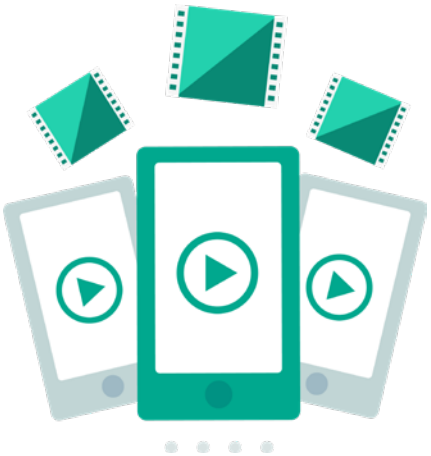
Éthique numérique



Tendance n° 1 : (hyper) développement du cloud

L'effet de l'expansion du cloud sur les télécommunications varie grandement, selon que votre société vise un modèle dépendant hyperscale, de télécommunications transitoires, natif du cloud, ou de prestation de service (ou toute autre variation de ces éléments).

En fait, en matière d'expansion du cloud et du secteur des communications, les possibilités sont aussi immenses que celles du cloud lui-même. Votre entreprise se trouve peut-être encore à la croisée des chemins, en train de discuter du bien-fondé de se concentrer sur un réseau régional ouvert, d'investir dans des plates-formes cloud ou de se concentrer sur l'établissement des partenariats requis pour se développer dans un marché d'écosystème axé sur le cloud. De plus, toutes ces pressions n'incluent même pas la question (ou l'éventualité) du contenu lui-même : ainsi, il n'est pas étonnant qu'un fournisseur de service Triple Play tel qu'AT&T se soit retiré de Warner pour se concentrer sur l'hyperscale (via Azure pour l'exploitation) et d'autres domaines.



Autrefois, c'était vraiment simple… le contenu a alors fait son apparition

Depuis l'époque d'Alexander Graham-Bell jusqu'à l'invention d'Internet par Tim Berners-Lee au CERN, les sociétés de télécommunications ont acheminé uniquement de la voix et, dans une moindre mesure, du texte. Au cours de la dernière décennie, la suprématie de la voix a été renversée d'abord par le texte, le SMS, l'email et à présent, de manière retentissante, la vidéo.

Selon CISCO, la vidéo représentera la part spectaculaire de 82 % du trafic Internet, d'ici 2022.

Responsables de la prestation de données à distance, d'un appareil à l'autre, les sociétés de télécommunications traditionnelles étaient impliquées de façon limitée dans la nature des données. La « démocratisation d'Internet » a changé cela radicalement, en rendant possible l'entrée dans le domaine lucratif de la diffusion de contenu. L'ascension fulgurante des OTT comme Netflix, semblait présenter un scénario de type « quitte ou double » aux sociétés de télécommunications : entrer dans le match du contenu ou perdre la partie pour de bon. La vérité s'est avérée être beaucoup plus complexe, comme l'a découvert AT&T (voir ci-dessus).

Comment utiliser le cloud en toute sécurité :

Le rôle des revendeurs va changer, car certains acteurs des télécommunications font évoluer leur mission de fournisseur de connectivité vers l'ajout de services cloud de pointe utilisant la norme MEC (Multiaccess Edge Computing).
Gartner, Inc.,Top 10 Strategic Technology Trends for 2020: Empowered Edge

95 %

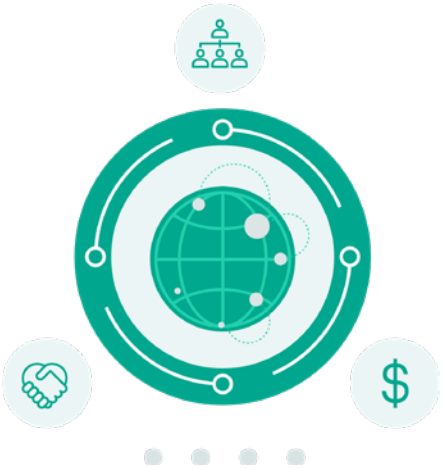
« En 2022, au moins 95 % des failles de sécurité dans le cloud seront initiées par les clients. »
Gartner, Inc.,Clouds are secure: are you using them securely?

Paradoxalement, bien que le cloud ait historiquement été considéré comme une technologie distante, délibérément **hors** site, la dernière vague va entraîner le cloud encore plus près du client. Nous parlons bien sûr de l'edge cloud, en particulier de celui des télécommunications. Si vous prévoyez de proposer des services de calcul distribué (distributed compute services), ou de travailler avec des fournisseurs intermédiaires, vous allez devoir prendre en compte ce qu'il se passe lorsque le service que vous offrez s'étend au-delà de la périphérie du réseau et du côté des clients. Lorsque vous recouvrez l'edge cloud, en travaillant avec une infrastructure virtualisée, vous allez devoir traiter la sécurité des données, leur emplacement, et les notions de propriété et de responsabilité avec le plus grand sérieux.

Lorsqu'il s'agit de cloud hybride, le modèle de sécurité en « responsabilité partagée » présente des limites. Même si un fournisseur de services cloud partage la responsabilité des données qui y sont stockées, la priorité absolue d'une société doit toujours être ses propres données sensibles (et ses propres résultats financiers). Cela confère une importance énorme à la visibilité des données : si des données sensibles (incluant les données des clients) se trouvent entre les mains d'un fournisseur tiers, les opérateurs de télécommunications doivent en être informés.

La périphérie nécessite également une attention particulière : qu'il s'agisse d'une périphérie entre des réseaux, des clouds ou des services, les configurations doivent être sans faille. Les risques les plus importants peuvent survenir à la rencontre de deux systèmes, lorsque des paramètres d'authentification ou de sécurité entrent en conflit ou ne se comprennent pas. L'échelle de telles confrontations entre systèmes signifie que la fonctionnalité de cybersécurité automatisée est plus essentielle que jamais, tout particulièrement lorsqu'il s'agit des analyses de vulnérabilité et des correctifs, notamment les vulnérabilités « zero-day ».

Étant donné que la plupart des opérateurs de télécommunication vont être tributaires de partenariats avec des fournisseurs externes pour exploiter l'expansion du cloud et les possibilités de monétarisation, il est nécessaire de traiter le problème des risques tiers et des attaques de la chaîne logistique.



Tendance n °2 : Écosystèmes : partenariats et fournisseurs tiers

Les pressions dues à la mondialisation, la diversité des appareils, mais peut-être surtout à la complexité croissante, se sont combinées pour encourager un secteur dans lequel les fournisseurs de services et d'infrastructures spécialisés (y compris les nouveaux arrivants) jouent à présent des coudes pour se faire une place parmi les géants nationaux des télécommunications, qui ont toujours historiquement profité des monopoles d'État.

C'est une bonne nouvelle. Les opérateurs de télécommunication ont adopté à juste titre l'écosystème numérique pour le bénéfice de tous, y compris des consommateurs. Les grandes entreprises bénéficient de la possibilité de profiter de services innovants extrêmement spécialisés et de solutions développées par des start-up. Cela peut tout inclure, des abonnements SaaS ou PaaS, jusqu'à des acquisitions. L'économie et l'exploitation de l'écosystème témoignent de la puissance du spécialiste, ainsi que du rôle que jouent les fournisseurs spécialisés pour alimenter les innovations des opérateurs de télécommunications, quelle que soit leur taille au niveau national.

« La gestion de l'écosystème fait référence à l'évolution de la gestion des fournisseurs et des partenaires avec une approche selon un écosystème adopté par de nombreux fournisseurs de solutions cloud : une transition vers des modèles tels que la marketplace, les produits partenaires/le regroupement et la revente de composants du produit, ainsi que la gestion de ces partenaires/revendeurs/distributeurs. »
Gartner, Inc.,Market Trends: Fundamental Changes Await the Telecom BSS Market

L'écosystème d'acquisition

« Les écosystèmes économiques ont toujours existé. »
Gartner, Inc.,How to Select the Best Platform Business Model

Les acquisitions de start-up bénéficient aux deux parties : l'une gagne sur le plan de l'innovation, l'autre accède à un financement et à un cadre mature et fiable pour la croissance et le développement.

En examinant les acquisitions sous un autre angle, certaines grosses aux entreprises de télécommunications ont même pris la décision de vendre des filiales pour de se recentrer sur leur spécialité principale. La vente de WarnerMedia par AT&T, qui avait fusionné avec Discovery un peu plus tôt cette année (2021) pour

créer un concurrent sérieux à Netflix et Disney, en est un exemple flagrant. La transaction, qui avait permis de débloquer 43 milliards de dollars américains, a été interprétée par les analystes comme un désengagement d'AT&T dans le secteur de l'activité de contenu. Cependant, cela avait du sens, et constituait encore un témoignage supplémentaire du fait que l'écosystème des télécommunications est là pour durer, et que ses fluctuations affectent les acteurs, quels que soient leur taille ou leur degré de maturité.

L'écosystème du partenariat

Les partenariats prennent de nombreuses formes : des accords de fournisseurs tiers aux co-entreprises en passant par les compléments de service et bien sûr l'économie d'écosystème qui semble se généraliser dans tous les secteurs. Dans tous les cas, les partenariats fournissent non seulement la spécialisation (en termes de technologie et de personnel), mais également des bases de clients, sans oublier, bien sûr, une connaissance profonde d'un secteur vertical.

De plus en plus, il est impossible pour les acteurs des télécommunications d'atteindre sans partenariats la pénétration de marché requise pour de nouvelles technologies. Cela semble évident, mais les technologies ne servent à rien en l'absence de cas d'utilisation : par exemple (simple), un fournisseur de services Internet ne peut pas vendre de services si le consommateur ne possède pas d'appareil. Après tout, les entreprises de télécommunications vendent de la connexion et du partage. Le partenariat naturel qui s'établit entre les opérateurs 5G et les géants de la technologie, tel que le partenariat pour la 5G entre Google et Ericsson, annoncé en juin 2021, illustre ce scénario évident. Le PDG de Google Cloud, Thomas Kurian, a parlé avec passion de l'avantage mutuel pour la chaîne de valeur des partenariats en matière de télécommunication, allant jusqu'à dire « nous ne rivalisons pas avec les entreprises de services ».

L'écosystème tiers

Les études de cas pour l'adoption de services tiers varient énormément, mais une utilisation est essentielle : l'analyse de données. Le volume considérable de données disponibles se combine avec les conséquences dramatiques de la non-adoption d'analyses optimisées (dans un marché où les concurrents y ont recours), et génère un contexte dans lequel les opérateurs de télécommunication se tournent à présent vers des fournisseurs d'analyse commerciale tiers.

Ceux-ci permettent aux entreprises de télécommunications d'optimiser la planification du réseau, de comprendre le comportement des clients afin d'augmenter la captation et la rétention, et de réaliser des économies de coûts en se déchargeant de données (par exemple).

« Les cybermenaces ne font pas de distinction entre les marchés finaux. Au lieu de cela, les cyberattaquants ne voient que des systèmes vulnérables et des ports d'adresses IP ouverts, le résultat d'une récompense, une probabilité de succès et un potentiel de compromission. »
ABI Research, Smart IoT Gateways: Security, Analytics, and Ecosystem Assessment

Commencer par le problème d'un client, et non avec l'envie d'un écosystème

Toute entreprise peut participer dans une économie de plate-forme en montrant ses compétences via des API et en adoptant les plates-formes de partenaires pour accélérer et faire évoluer son activité. Toutefois, pour construire une plate-forme commerciale qui génère de l'argent, vous devez attirer les clients un par un, commercialiser vos API pour les clients et les fournisseurs, et réaliser une construction par étapes, comme une entreprise spécialisée dans les logiciels.
Forrester, Earn Your Place In The Platform Economy

Les experts mondiaux de Kaspersky expliquent les attaques contre la chaîne d'approvisionnement

Les attaques contre la chaîne d'approvisionnement représentent en quelque sorte un changement radical parmi les pirates. Elles ne sont pas nouvelles, mais elles deviennent rapidement beaucoup plus courantes, tout en évoluant pour échapper à la détection.

Ces attaques impliquent une implantation de la partie de virus qui exécute une attaque (la charge utile) dans des composants comme des logiciels, des micrologiciels et des matériels. Cette charge utile fait alors partie intégrante du produit fini. Les entreprises qui vendent ces produits se transforment alors en distributeurs involontaires. Ces charges utiles se cachent de manière silencieuse sur les ordinateurs ou les réseaux des clients, jusqu'à ce que quelque chose déclenche leurs processus malveillants.

Comment tirer parti de l'écosystème en toute sécurité :

Un secteur connecté dans un monde connecté a conduit au tissage d'un Web de plus en plus sujet à l'enchevêtrement. Il est facile pour une personne de défendre son propre château, beaucoup moins de défendre l'intégrité d'un vaste royaume. Les défenses de chaque partenaire ne sont sûres que si celles des deux combinés le sont : si une partie est faible, toutes les parties sont vulnérables. Tous les opérateurs de télécommunications doivent travailler de manière proactive afin d'éliminer les risques d'attaque de la chaîne d'approvisionnement.

Les transformations numériques font de chaque organisation une entreprise de logiciels qui dépend d'une multitude de fournisseurs externes, qui viennent s'ajouter à des menaces de tiers difficiles à gérer. Cela peut sembler catégorique, mais lorsqu'il s'agit de cybersécurité, c'est une réalité. Les leaders dans le domaine des télécommunications qui se concentrent sur la sécurisation de leurs écosystèmes seront les gagnants sur le long terme.

Les partenariats d'écosystèmes fonctionnent souvent au-delà des frontières, traversant des contextes géopolitiques très différents, et sont confrontés à des appareils et des terminaux disposant de niveaux de protection très inégaux. Toutes les parties ont besoin d'accéder aux solutions de cybersécurité tournées vers l'avenir et qui tiennent compte de cette réalité du terrain, car une réelle innovation ne peut pas produire de résultats dans un contexte de crainte et de risque.

ÉCOSYSTÈMES, CLOUD, IA : Pleins feux sur les ATTAQUES CONTRE LA CHAÎNE D'APPROVISIONNEMENT

Un secteur connecté dans un monde connecté a conduit au tissage d'un Web de plus en plus sujet à l'enchevêtrement. Il est facile pour une personne de défendre son propre château, beaucoup moins de défendre l'intégrité d'un vaste royaume. Les défenses de chaque partenaire ne sont sûres que si celles des deux combinés le sont : si une partie est faible, toutes les parties sont vulnérables. Entrez dans l'ère des attaques contre la chaîne d'approvisionnement.

En 2018, nos ingénieurs ont découvert « Shadow Pad », une dangereuse attaque contre la chaîne d'approvisionnement qui a touché NetSarang, un développeur d'outils de gestion pour les serveurs et les clients. Le logiciel de NetSarang étant utilisé dans des centaines de réseaux critiques dans le monde entier, le potentiel de dommages et de pertes sur une grande échelle était immense. NetSarang a été obligé de retirer la version et de faire ses excuses auprès de sa base de clients lucrative. Bien que les ingénieurs de Kaspersky aient été en mesure de porter un coup d'arrêt à l'attaque Shadow Pad contre la chaîne d'approvisionnement, cet événement a prouvé que toutes les parties au sein d'une chaîne d'approvisionnement devaient demander à leurs fournisseurs de disposer d'un niveau de sécurité optimal.

La complexité de la chaîne d'approvisionnement n'est pas ici le seul défi (bien qu'il soit de taille). Les partenariats fonctionnent souvent au-delà des frontières, traversant des contextes géopolitiques très différents, rencontrant des appareils et des terminaux avec des niveaux de protection très inégaux. Toutes les parties doivent avoir accès à des solutions de cybersécurité axées sur le futur qui tiennent compte de cette réalité du terrain.

Les fournisseurs de services de télécommunications et leurs partenaires doivent être en mesure de croire que les cyberdéfenses de l'autre partie sont suffisamment robustes pour protéger tout le monde, y compris les clients.

Voici les quatre moyens essentiels en matière de sécurité que chaque opérateur de télécommunications doit exiger de ses partenaires :

1. Sécurité du trafic ;
2. Tests de pénétration/évaluation de la sécurité des applications ;
3. Sécurité du Web et des e-mails ;
4. Formation de sensibilisation à la cybersécurité.

La cybersécurité doit être la pierre angulaire de toutes les initiatives conjointes, afin que toutes les parties puissent progresser sans crainte et continuer à former les partenariats produisant les technologies et services dont le marché est de plus en plus friand.

La 5G rend possibles la connexion et l'interaction de milliards d'appareils de toutes sortes et la collecte de données depuis ces appareils. En effet, la connectivité 5G promet d'amener les consommateurs, les industries et les gouvernements vers de nouveaux horizons en matière de productivité et d'innovation. Deloitte

Tendance n° 3 : IoT : La 5G a-t-elle tenu toutes ses promesses ?

La connectivité optimisée de la 5G est absolument déterminante pour la réussite (ou l'échec) de tout fournisseur de services technologiques ou fabricant d'appareils déterminé à rester leader au cours de la décennie à venir.

Essentiellement, ce sont les possibilités ouvertes pour l'IoT, les infrastructures de bureaux virtuels et la réalité augmentée qui ont fait que la 5G change véritablement la donne et ne se limite pas à une simple mise à niveau de la 4G. Tout en étant plus rapide que son prédécesseur, la 5G s'accompagne d'une gamme complète de protocoles d'appareil normalisés, qui permettent à un nombre sans précédent d'appareils et de réseaux d'interagir les uns avec les autres. Cet aspect de la 5G est une nécessité absolue pour l'évolution permanente de l'IoT, depuis les slogans accrocheurs jusqu'à la réalité quotidienne.

Un certain nombre d'applications existantes concernent la sécurité elle-même. Les répercussions que le paradoxe du double usage pourrait avoir sur ces dernières (voir ci-dessus) sont faciles à imaginer.

Le paradoxe du double usage : le bon, la brute et le (vrai) truand

Les recherches sur le double usage portent traditionnellement sur des technologies pouvant s'appliquer à un usage tant civil que militaire. Toutefois, le terme s'étend désormais au paradoxe selon lequel toute technologie bonne pour les consommateurs ou les entreprises peut également être utilisée par des criminels. Le paradoxe du double usage est la raison pour laquelle l'accueil

réservé à toutes les nouvelles technologies en réseau comme la 5G, l'ITO ou la réalité augmentée doit toujours être tempéré par la conscience du fait que les cybercriminels auront également hâte d'utiliser ces innovations.

« D'ici quelques années, les réseaux 5G prendront en charge une latence extrêmement faible et des communications stratégiques qui permettront aux applications et aux processus d'accompagner la transformation numérique des industries, qui va s'accélérer pour certaines en raison de la COVID-19. Sur le court terme, malheureusement, les déploiements de la 5G font face à des perturbations sans précédent parmi les constructeurs, les acheteurs, les organisations de normalisation et les entités gouvernementales responsables des fonctions de support essentielles, telles que l'octroi de licences de sites et la vente aux enchères du spectre de fréquences. »
451 Research, COVID-19 and 5G: Short-term pain for long-term gain

Pour comprendre les effets éventuels du paradoxe du double usage, prenons l'exemple de l'attaque par le ransomware WannaCry, qui a mis à genoux le service national de santé britannique, en utilisant la fuite d'un logiciel espion de l'Agence nationale de sécurité américaine ou d'un outil de piratage appelé EternalBlue.

L'incidence de la pandémie sur le déploiement de la technologie IoT a été quelque peu partagée. D'un côté, l'apparition soudaine et pratiquement universelle du travail à la maison et de l'école à domicile a accéléré le besoin d'adopter la technologie des capteurs IoT à des fins de surveillance de contrôle à distance. D'un autre côté, le choc de la pandémie sur les économies mondiales a entraîné la mise en attente de certains projets IoT prévus pour 2020 (et 2021). Les pressions économiques n'ont pas bien sûr été seul problème : le déploiement à grande échelle de l'IoT dépend de la fabrication de capteurs physiques, qui a été considérablement bouleversée par les restrictions liées à la pandémie. Une pénurie de condensateurs céramiques multicouches en août 2021 a frappé durement les constructeurs de matériel. La cause était simple : l'usine d'un fournisseur essentiel a dû fermer pendant une semaine en raison du variant delta de la COVID-19.

Comment utiliser la 5G et l'IoT en toute sécurité :

« Les préoccupations en matière de sécurité risquent de planer au-dessus de la 5G au cours des années à venir en raison de points d'entrée plus importants pour les attaquants, selon l'établissement des fournisseurs et le fonctionnement des réseaux 5G et, par extension, les opérations de sécurité, qui peuvent conduire à des problèmes vitaux pour l'intégrité et la fiabilité du réseau. »
ABI Research,Smart IoT Gateways: Security, Analytics, and Ecosystem Assessment

La 5G est un domaine dans lequel les entreprises de télécommunications doivent tenir compte très attentivement des implications du paradoxe du double usage. Selon le légendaire informaticien Stuart Madnick, du MIT, les consommateurs ne sont pas les seuls à pouvoir espérer bénéficier de la vitesse du turbo de la 5G.

Madnick est particulièrement préoccupé par le coup de pouce que la 5G pourrait offrir à d'éventuelles attaques DDoS, dans lesquelles les cybercriminels infectent des machines non protégées à l'aide de programmes malveillants, qui bombardent ensuite un serveur cible dans le but de le saturer et de provoquer son arrêt. C'est ce qui s'est passé pour des centaines de sites Web dans le monde en 2016 avec l'attaque par déni de service distribué de Dyn, dans laquelle un botnet Mirai analysait les appareils IoT et utilisait des mots de passe par défaut pour transformer en armes les appareils en vue de l'attaque.

Il n'est pas étonnant que des analystes de la sécurité aient suspecté une attaque par déni de service distribué, visant l'IoT/la 5G, comme étant responsable de la panne de Facebook en octobre 2021 (bien que la société, qui a changé de nom pour s'appeler Meta, ait mis cela sur le compte d'un problème technique interne). Madnick déclare : « Le fait que la 5G augmente la vitesse signifie qu'il faut encore moins d'attaques par déni de service distribué pour submerger une organisation donnée, puisqu'il est désormais possible d'obtenir un taux exponentiel du trafic en direction de quelqu'un. Le pire reste à venir. »

La devise du Mois de la sensibilisation à la cybersécurité en 2020 du NIST est un bon conseil (simple, également) : « Si vous connectez l'informatique, protégez l'informatique ». Prendre au sérieux la sécurité de l'IoT (en prenant en compte l'éventualité d'une violation de la vie privée sur des marchés moins bien régulés) semble être du bon sens commercial. Après tout, la réputation et la confiance des clients sont intimement liés, tout comme les résultats financiers.

Une éducation à l'échelle de l'entreprise est essentielle pour supprimer tout risque d'erreur lors de l'utilisation des appareils IoT, en étant attentif aux bases de la cyberhygiène, telles que les mots de passe complexes, afin de protéger les utilisateurs et défendre les réseaux contre les attaques par déni de service distribué visant la 5G.

Dans de nombreux cas, les attaques contre (ou via) les appareils IoT proviennent d'appareils, de systèmes ou de protocoles anciens, avec une sécurité faible. Les problèmes historiques avec le protocole AKA (Authentication and Key Agreements), lorsqu'ils ont été transférés directement de la 3G vers la 5G sans toute l'attention requise, ou les architectures sur un réseau régional ouvert basé sur le cloud, ont provoqué des vulnérabilités.

Tendance n 4 : Travail à distance : consolidation et croissance

« Comme les environnements distants et hybrides deviennent la nouvelle norme, les leaders dans le domaine des infrastructures et de l'exploitation ont la tâche de pérenniser ce modèle à long terme, en continuant à adopter des technologies qui augmenteront davantage la qualité des services informatiques, augmenteront la souplesse organisationnelle et réduiront le risque. »
Gartner, Inc.,Hype Cycle for Digital Workplace Infrastructure and Operations, 2021

« Même si le monde se prépare à revenir travailler (au bureau), il y aura davantage de jours flexibles et plus de travail à distance que jamais auparavant, de sorte que la tendance au déplacement vers une sécurité fournie dans le cloud va se poursuivre. »
Forrester, The Top Security Technology Trends to Watch, 2021

Avant 2020, nous avions l'habitude de consacrer quelques paragraphes à plaider en faveur des avantages du travail à distance (13 % plus efficace, selon l'l'université Stanford). Une telle introduction n'est plus nécessaire. La question à présent, pour l'avenir, est de savoir comment nous pouvons (nous tous) consolider les progrès immenses que nous avons effectués dans le travail à distance, et de nous inspirer de ceux-ci au moment où nous adoptons la réalité durable du travail hybride.

Quel que soit l'état du travail à distance, c'est l'industrie des télécommunications qui le rend possible. Même si la pandémie a retardé divers projets de télécommunications, s'il y a une chose que les entreprises ont apprise partout, c'est que le futur réside dans les télécommunications.

D'après Harvard Business Review, les employés attendent désormais une flexibilité du travail hybride et, de manière plus large, l'autonomie que cela représente. En juin 2021, lorsqu'Apple a forcé ses employés à revenir au bureau 3 jours par semaine, il y a eu des manifestations et des débrayages. Pour le secteur des télécommunications, le défi consiste à fournir les solutions et les services dont les entreprises auront besoin afin d'offrir un modèle de travail hybride réellement fluide, souligné par des niveaux élevés de service et de sécurité identiques, que les employés soient devant leur table de cuisine ou au bureau.

Sans surprise, la sécurité n'est pas le seul défi auquel nous devons faire face lorsqu'il s'agit d'estomper les frontières entre le domicile et le travail. Il est indispensable que les employeurs tiennent compte des effets sur la santé mentale des employés qui doivent à présent porter deux casquettes, sans possibilité d'évasion au travail ou au domicile. Les régulateurs ont commencé à se jeter dans la mêlée, le Portugal étant considéré comme le premier pays ayant rendu illégal pour les entreprises le fait de contacter leurs employés à distance après les heures de travail dans une nouvelle loi (novembre 2021).

Globalement, le cadre juridique concernant le travail à distance est variable, l'initiative portugaise constituant un cas atypique. En Espagne, les tentatives de réguler le travail à distance (qui incluent les contrats bilatéraux employé/employeur) ont rencontré les objections de la part des employeurs, qui prétendaient que les conditions étaient trop draconiennes, un expert universitaire prétendant même que la loi trahissait un manque d'imagination (novembre 2021).

Ces deux exemples pris dans la péninsule ibérique ont tous deux ont été rendus publics le même jour, le 8 novembre 2021, et sont révélateurs d'une absence notable d'uniformité dans les réponses globales à l'accélération du travail à distance (ou hybride) lié à la pandémie.

Ce rapport indique également qu'il existe une nette prise de conscience parmi les législateurs que les directives temporaires ou d'urgence concernant le travail à distance, qui ont étaient suffisantes pour les entreprises pendant le premier choc de la pandémie, ne conviendront pas pour une culture du travail à distance et hybride, qui va certainement s'installer dans la durée. L'impression globale est la suivante : « D'accord, le travail à distance va se généraliser. Maintenant que nous pouvons souffler un peu, qu'allons-nous faire à ce sujet ? ».

Pour les télécommunications, cette acceptation réglementaire du travail à distance comme modèle durable est une bonne nouvelle. Après tout, les télécommunications sont le secteur vers lequel les entreprises du monde entier doivent se tourner pour faire du travail hybride une réalité. Le passage soudain au travail à distance en mars 2021 n'était pas juste une fluctuation soudaine (comme certains ont pu le penser).

Les réponses réglementaires différentes au travail à distance vont nécessiter une attention spéciale de la part des entreprises de télécommunications, car il n'existe que très peu d'entreprises qui ne s'étendent pas au-delà les frontières nationales, sous une forme ou une autre. Le cas des centres d'appels externalisés, avec des fuseaux horaires très différents de ceux de la société cliente, peut constituer un exemple approximatif de cela, mais ce type de communications transnationales pose une question évidente pour le respect des lois dans des régions (comme le Portugal) qui réglementent les heures de travail.

Encore une fois, bien que la question de nouvelles réponses légales au travail à distance ne constitue peut-être pas un problème explicite en matière de cybersécurité, nous devons toujours avoir en tête que tout ce qui a une incidence sur l'équilibre travail/vie, ou qui estompe la frontière entre le travail et loisirs, entraîne des conséquences en termes de sécurité. Cela doit inclure les lois draconiennes qui forcent les employés (de leur plein gré ou non) à recourir à d'autres appareils ou réseaux pour que le travail soit fait, lorsque la loi leur interdit directement de travailler (par exemple) après 18 h 00, ou le week-end.

Le risque ne provient pas seulement d'un manque de clarté en ce qui concerne l'utilisation d'un appareil et du réseau. Pour un bon nombre d'employés, la liberté de travailler le week-end (ou le soir) est le principal attrait du travail à distance, en permettant aux parents de partager les responsabilités de garde d'enfants en formant une « équipe de relais », par exemple. L'anéantissement de cette flexibilité radicale peut être dévastateur pour certains employés qui ont découvert une nouvelle liberté, pratique et extrêmement productive, due à la force de la pandémie. L'équilibrage de l'éventail d'intérêts et de forces qui entrent en concurrence va demander aux leaders des télécommunications dans le monde de partager leur expertise avec les législateurs, pas seulement en ce qui concerne la technologie de travail à distance qu'ils proposent, mais également en tant qu'employeurs (tout particulièrement dans la mesure où les télécommunications se situent juste à côté des organismes gouvernementaux et des sociétés de service public en termes de nombre d'employés).

Comment utiliser le travail à distance en toute sécurité :

« Même si une part importante de personnes n'a guère d'autre choix que de se rendre physiquement au travail, 40 % de toutes les heures de travail des Américains sont quand même effectuées à domicile. »
The Economist

Les entreprises de télécommunications doivent développer une plus grande agilité lorsqu'il s'agit d'appliquer des différences aux lieux qu'ils desservent. Vente au détail ? Ou entreprise ? Selon TechRadar, la ligne de démarcation n'est pas très nette. En fait, cette zone diffuse est le reflet direct du changement culturel plus vaste en direction du modèle consistant à « être soi-même au travail » (et, par conséquent, malheureusement, peut-être, ramener votre travail à domicile).

Que se passe-t-il lorsqu'un réseau d'entreprise est attaqué en utilisant l'un de vos services comme vecteur, pendant que l'employé travaille chez lui ? La réponse au défi de sécurité que pose le travail à distance va forcer les entreprises de télécommunications à trouver de nouvelles approches vers les limites floues du modèle hybride.

Il existe une connexion évidente entre le travail à distance (ou hybride) et la révolution de l'écosystème, dans la mesure où les acteurs des télécommunications se tournent vers des partenariats tiers pour fournir les services demandés par le marché. Là encore, il s'agit d'un scénario clair appelant à l'évaluation des risques des fournisseurs qui prend très au sérieux la sécurité des fournisseurs tiers, notamment les protocoles d'authentification et les appareils.

En mars 2020, nous n'avons pas eu le temps de nous préparer. Le monde a été forcé de travailler à domicile sans presque aucun avertissement. Mais à présent que nous attendons 2022 avec impatience, il s'agit d'une opportunité fantastique pour les entreprises en général (et les télécommunications en particulier) de regarder de manière plus holistique comment rendre le travail à distance sécurisé et réussi (dans la mesure où l'un ne va pas sans l'autre).

Lorsque nous employons le terme holistique, nous voulons signifier que la technologie (par exemple, les VPN) doit être accompagnée par des changements culturels. Comme nous l'avons vu avec les exemples ibériques, les législateurs sont confrontés au défi à long terme du travail à distance, et les entreprises feraient bien de donner la priorité à la formation, aussi bien pour les employés que les clients, afin de garantir que les produits et les services sont utilisés en toute sécurité.

Tendance n° 5 : IA et analyse

Le cas d'utilisation principal pour l'IA dans les télécommunications est l'optimisation grâce à l'analyse, avec l'acquisition de Sedona Systems par CISCO, Netfusion, un exemple emblématique de fournisseur de services. Netfusion prétend « réduire la complexité, le coût, le temps et les ressources dont vous avez besoin pour planifier, prévoir et exploiter l'infrastructure réseau optimale en vue d'offrir des services, des performances et une fiabilité inégalés ».

Dans le même temps, des services d'automatisation de processus, tels que Kryon, assurent que « Développé par une technologie d'IA propriétaire brevetée, cet outil leader sur le marché fonctionne dans la plus grande discrétion en arrière-plan pour générer automatiquement une image complète des processus métier manuels et de leurs variantes, les évaluer et recommander ceux qu'il faut automatiser. Il génère ensuite instantanément les flux de travail. »

L'optimisation qu'offre la prochaine génération d'analyses utilisant l'IA va permettre aux entreprises de télécommunications de proposer des services réactifs, flexibles et fiables, sans avoir à faire appel au temps et à l'expertise précieux de leur personnel pour l'analyse de données et la prévision de résultats.

Dans tous les cas d'utilisation, l'IA est appelée à être considérablement utilisée en 2022, en partie en raison de la disponibilité d'ensembles de données encore plus volumineux qu'auparavant, ainsi que de l'apparition de nouveaux services d'analyse algorithmique, qui testent en permanence des algorithmes générés de manière aléatoire par rapport aux données, afin d'apprendre, d'affiner, de prédire et de préconiser.

« Bien que l'on puisse prétendre que les humains sont toujours à l'origine de systèmes autonomes, il est possible à des systèmes artificiels de développer des comportements qui ne sont pas forcément prévus par leurs développeurs (en dehors des erreurs de programmation, évidemment). »
Gartner, Inc., Improve Decision Making Using Decision Intelligence Models

---

« Les entreprises avancées fondées sur la connaissance sont 1,9 fois plus susceptibles de mettre en œuvre des outils de génération de rapports et d'analyse pour la veille économique en libre-service, et 1,8 fois plus enclines à développer des programmes de lecture des données à l'échelle de l'entreprise… les entreprises avancées fondées sur la connaissance ont environ une probabilité deux fois supérieure à celle des nouveaux arrivants de signaler une augmentation de la valeur vie client et une plus grande capacité à développer de nouveaux flux de recettes comme avantage de l'utilisation des données et des analyses. »
Forrester, Chart Your Course To Insights-Driven Business Maturity

Comment utiliser l'IA en toute sécurité :

« Les modèles d'IA qui sont déployés en production doivent être soumis aux mécanismes régulateurs adéquats pour garantir une génération de valeur régulière. Un ensemble de contrôles du risque et de la sécurité, ainsi que des validateurs approuvés, doivent être déployés et utilisés en permanence pour régir et gérer le cycle de vie de l'IA… Les organisations vont prendre des décisions opérationnelles qui ne seront pas optimales en cas de mauvaises performances de l'IA. Dans le pire des cas, une interférence malveillante avec les résultats de l'IA entraînera des défaillances de sécurité, une perte financière et de réputation, ainsi que des dommages sociaux liés à des résultats d'IA incorrects, manipulés, contraires à l'éthique ou biaisés. Gartner, Inc., Hype Cycle for Artificial Intelligence

« Le fait de devenir une société basée sur les connaissances est une mutation opérationnelle fondamentale vers laquelle les entreprises doivent basculer maintenant si elles ne veulent pas risquer d'être désavantagées par rapport aux concurrents et aux nouveaux acteurs. » Forrester, The Four Essential Steps To Transform Into An Insights-Driven Business

Très peu (le cas échéant) d'entreprises de télécommunications vont être en mesure de développer en interne des systèmes d'analyse IA propriétaires, ce qui est une bonne nouvelle pour les fournisseurs tiers tels que Netfusion et Kryon (mentionnés ci-dessus). Nous vous recommandons vivement de lire notre section relative aux écosystèmes afin de comprendre les implications plus larges d'un recours de plus en plus répandu à des fournisseurs externes. Cela est même encore plus important, étant donné la sensibilité des données que vous aurez nécessairement à rendre disponible à des systèmes tiers.

La chose étonnante, en ce qui concerne les analyses ayant recours à l'IA, est que même si les utilisateurs finaux peuvent bénéficier de leur utilisation, les entreprises doivent contrebalancer cet avantage avec le risque d'embarras des consommateurs pour le partage de leurs données privées. Les avertissements en jargon juridique concernant le partage des données clients avec des « fournisseurs tiers sélectionnés » risquent de ne pas apaiser les préoccupations des utilisateurs finaux lorsque leurs données sont exposées à des systèmes d'IA externes.

Nous allons traiter la position éthique et réglementaire plus en détail dans la section suivante, mais il est très probable que des marques (de commerce entre entreprises ou d'entreprise aux particuliers) perçues comme étant de farouches défenseurs de la vie privée des clients seront celles qui vont réellement bâtir et gagner la confiance des clients et des parts de marché. Cela implique de défendre les données du client avec toute l'énergie dont elles disposent, et rechercher une puissance supérieure si elles ne n'ont pas déjà sous la main l'arsenal de défenses approprié.

La technologie des affaires fondée sur les connaissances utilisant l'IA évolue rapidement et, bien qu'il semble à présent improbable que les machines soient moralement en absence non autorisée, la plupart des sociétés qui adoptent l'analyse IA précisent que la supervision humaine aura toujours un rôle à jouer.

Tendance n° 6 : Éthique numérique – Au-delà de la réglementation

La réglementation représente un énorme défi pour les télécommunications. Les pressions réglementaires sont plus violentes que jamais dans un marché mondial dans lequel des fournisseurs experts établissent des partenariats au-delà des frontières géographiques pour délivrer des services évolués à l'échelon international.

« Les récents scandales d'entreprises mettent en évidence le fait que certaines des entreprises les plus importantes dans le monde n'ont pas de dirigeants soucieux de l'éthique. Malheureusement, un trop faible nombre d'entreprises a réalisé en avance que l'époque où il était possible de profiter d'une utilisation non éthique des données des clients était révolue. » **Forrester, Make your digital transformation an ethical one**

Cependant, force est de constater que la réglementation représente également un défi prodigieux pour les régulateurs eux-mêmes. L'innovation évolue à une vitesse tellement fulgurante, et cette vitesse se combine avec l'augmentation de la complexité des services, des plates-formes et des partenariats, pour créer un scénario dans lequel les régulateurs ont des difficultés à maintenir la cadence.

C'est la raison pour laquelle nous recommandons vivement que les entreprises de télécommunications se penchent sur la question de l'éthique en même temps que celle de la régulation lorsqu'elles examinent la conformité, et la confidentialité des données en particulier.

En plaçant l'éthique sur le devant de la scène, les entreprises peuvent être mieux placées pour éviter certaines des répercussions négatives qui se sont abattues même sur des acteurs majeurs tels que Facebook, lorsqu'elles ont été perçues par les consommateurs comme ayant eu un mauvais comportement. Alors même que l'économie des données (et de la surveillance) évolue rapidement, les problèmes éthiques qui entourent l'utilisation des données ne vont pas disparaître. Pour donner un peu de contexte, c'est une utilisation non éthique des données (via Cambridge Analytica, entre autres), qui a conduit Mark Zuckerberg à être obligé de témoigner devant le Congrès américain.

Les arguments en faveur de la gestion des données éthiques ne vont pas disparaître : **50 psychologues** ont écrit une lettre ouverte qui a eu un grand retentissement à l'American Psychological Association pour dénoncer la conception manipulatrice de l'expérience client et l'utilisation des données des médias sociaux. Pendant ce temps, la liste des « rock stars » lanceurs d'alerte de la Silicone Valley qui se sont également élevés contre l'utilisation non éthique des données ou la conception manipulatrice de l'expérience client continue de s'allonger, incluant notamment **Tristan Harris**, de Google, **Sean Parker** et, désormais, **Frances Haugen** (tous deux de Facebook). Mark Benioff de Salesforce est allé jusqu'à dire devant toute une assemblée à Davos que Facebook **devrait être réglementé au même titre que les fabricants de tabac**.

Plus d'éthique, davantage de profits, mais en le faisant correctement : un coup d'œil sur Nike et Gilette

Les consommateurs ne sont pas bêtes : ils peuvent flairer le manque d'authenticité de la posture soi-disant éthique d'une entreprise.

La preuve ?

Lorsque Nike a lancé Dream Crazy, une campagne assumant la controverse et mettant en scène une vedette sportive militant contre le racisme, Colin Kaepernick, ses bénéfices ont augmenté de 31 %, par rapport aux 17 % de la période d'achat pendant le Labor Day de l'année précédente. Cela a eu lieu en dépit d'une vaste campagne sur les réseaux sociaux : #BoycottNike – kaepernick, de la part de consommateurs (et de Trump) qui éprouvaient du ressentiment à l'égard de Nike « faisant l'apologie de la vertu du woke », ou Kaepernick's taking the knee – boyer, contre le racisme. Selon Nike, « le but de l'entreprise est de faire avancer le monde grâce au pouvoir du sport : faire tomber les barrières et bâtir une communauté afin de changer les règles pour tous ».

La campagne Nike, bien que risquée, s'est avérée être un succès incroyable, et la publicité Kaepernick a même gagné une récompense Emmy.

Les choses ne se sont pas passées aussi bien pour la publicité sur le Web de Gillette, inspirée de #MeToo, Be the Best a Man Can Be. La publicité d'une longueur de deux minutes a représenté un tournant par rapport à une affirmation basée sur le produit, « The Best a Man Can Get », et a plutôt exhorté les hommes à tourner le dos à leur « masculinité toxique ». Ce trimestre, même si la société mère Procter & Gamble a publié des ventes importantes, Gillette encaissé une lourde perte de 8 milliards de dollars américains. Cela été suivi d'un boycott énorme, facile dans un marché en effervescence avec des startup dans le domaine du rasage, telles que « Dollar Shave Club », qui n'ont eu qu'à tweeter quatre simples mots : « Welcome to the club » pour attirer d'importants groupes d'anciens clients mécontents de Gillette.

Dans un article dans Forbes, Avi Dan a expliqué le problème avec la campagne de Gillette :

Ce qui rend cette publicité si déplaisante est le fait que Gillette ne se contente pas de condamner un mauvais comportement, ce que la plupart des hommes font également. Elle laisse entendre que le comportement vulgaire représente la norme parmi les hommes et, en faisant cela, elle calomnie un genre complet.

Les critiques et les analyses continuent à comparer et à opposer les deux campagnes, et beaucoup suggèrent que Gillette a mal compris son marché principal (les personnes qui souhaitaient simplement acheter un rasoir) et a dépassé les bornes en leur faisant la morale d'une manière qui leur est restée en travers de la gorge. Selon cette analyse, la campagne de Nike a été réussie, non seulement parce que les valeurs exaltées par la campagne de Kaepernick semblaient authentiques, mais aussi parce qu'elles trouvaient un écho avec la base des clients de Nike. Avi Dan (voir ci-dessus) faisait partie de ceux qui ont fustigé le manque d'authenticité de la publicité de Gillette, en la qualifiant de « peu convaincante ».

Le contraste entre Nike et Gillette prouve que l'éthique a son importance : les consommateurs y sont attentifs, et les entreprises doivent l'être également. Mais le « woke-washing » ne suffit pas non plus.

Les entreprises de télécommunications, qui sont par essence en contact avec d'énormes quantités de clients (et d'entreprises) extrêmement sensibles, doivent apporter une attention toute particulière aux leçons tirées des expériences de Nike et de Gillette. Être leader pour une pratique éthique des données (et promouvoir cela) est essentiel, mais tout message doit absolument être soutenu par une action et un engagement sérieux dans les coulisses. Si vous ne joignez pas le geste à la parole, vous ne devez jamais, au grand jamais, faire de beaux discours.

Dans la plupart des cas, et dans un monde idéal, la réglementation représente une riposte essentielle à l'encontre du développement technologique incontrôlé et non maîtrisé, comme un casque sur la tête d'un pilote de Formule 1.

Les exigences réglementaires peuvent habituellement être classées selon l'une de deux préoccupations possibles :

1. Protéger les données précieuses (incluant la protection des données personnelles)
2. Empêcher un accès à des ressources interdites

Le Règlement général sur la protection des données de l'UE est un exemple bien connu de la première catégorie. Cette réglementation est conçue pour sécuriser les grandes quantités de données personnelles qui vont être générées dans un monde de plus en plus connecté. L'un des effets d'une telle réglementation, qui provient de plus d'une région aussi vaste et influente que l'UE, est que les fournisseurs du monde entier sont contraints de promulguer ou d'envisager de promulguer une réglementation similaire, ne serait-ce que pour s'assurer de pouvoir poursuivre leurs activités sur des marchés hautement réglementés. Le résultat de cette influence est que les « objets » IoT provenant de l'étranger ne seraient pas nécessairement susceptibles d'introduire des vulnérabilités, ce qui aurait pu être craint à une époque sans réglementation.

Le transfert en toute sécurité des données personnelles ou précieuses est principalement garanti par l'utilisation du chiffrement classique du trafic basé sur SSL. De nombreuses entreprises sont confrontées à la tâche herculéenne de protéger des volumes potentiellement gargantuesques de données personnelles, ce qui crée un besoin urgent pour une sécurité de stockage dans un centre de données dédié. Les entreprises de télécommunications qui exécutent de telles charges de travail pour la protection des données dans leur cloud propriétaire doivent également être extrêmement attentives aux capacités de sécurité de leur cloud hybride, en gardant à l'esprit qu'une fuite à un endroit donné peut également se transformer en une fuite partout. À nouveau, nous encourageons la prudence et la réflexion par rapport au risque de l'écosystème et aux attaques de la chaîne d'approvisionnement.

En ce qui concerne la deuxième préoccupation réglementaire, les entreprises de télécommunications doivent être attentives aux listes de ressources interdites publiées et mise à jour régulièrement par les institutions réglementaires dans le monde. Il existe plusieurs niveaux de débat pour savoir où se situe la responsabilité pour la protection des propres charges de travail des locataires des services cloud. Toutefois, en tenant en compte des dommages qu'une violation des réglementations peut faire peser sur le fournisseur de cloud computing, les entreprises de télécommunications doivent être proactives, en investissant dans une sécurité du trafic Web orientée au niveau mondial, et rechercher des options qui permettent d'effectuer un blocage personnalisé des catégories concernées.

Cependant, quel que soit le degré de frustration que peuvent ressentir ceux qui sont forcés d'appliquer ces réglementations, il est intéressant de prendre du recul et d'apprécier que tous les règlements concernant les données soient motivés par une position éthique que n'importe quel être humain est en mesure d'apprécier. Les données sont précieuses, les données personnelles le sont encore plus. Si je vous communique quelque chose de personnel qui me concerne, j'attends de vous un traitement précautionneux de ces informations, peu importe que vous soyez mon médecin personnel ou mon fournisseur de télé communications.

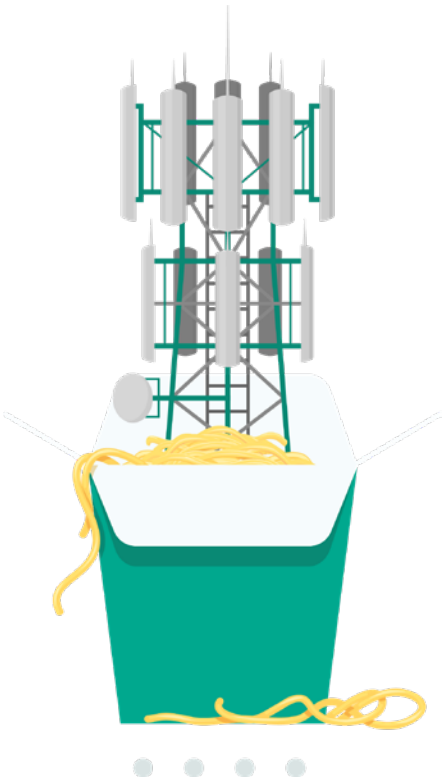
30 %

Selon Gartner, Inc, « d'ici 2023, les sociétés qui gagnent et maintiennent la confiance numérique avec leurs clients vont constater 30 % de profits supplémentaires dans le commerce numérique par rapport à leurs concurrents. »

C'est une bonne nouvelle. Cela signifie que les entreprises de télécommunications peuvent faire preuve d'un réel leadership dans un environnement réglementaire en ayant une approche de leurs feuilles de route à travers une approche éthique. En outre, les leaders visionnaires des télécommunications pourraient activement adopter une culture éthique des données afin d'anticiper les modifications réglementaires susceptibles d'apparaître après la réalité de la mise en œuvre.

La réglementation englobe bien plus que le simple fait d'éviter des amendes, cela concerne la confiance des clients, ce qui prouve que notre affirmation d'adopter une posture ethnique envers à la confidentialité des données sera en fin de compte bénéfique pour les entreprises de télécommunications.

Il va sans dire que les acteurs des télécommunications ont besoin d'une cybersécurité dédiée au niveau de l'entreprise pour soutenir leurs efforts de conformité réglementaire en vue d'une confidentialité des données basée sur l'éthique. L'ampleur des données potentiellement à risque, et de leurs emplacements de plus en plus distribués, signifie que les solutions de cybersécurité traditionnelles (incluant des offres propriétaires accompagnées de services de partenariat tiers) ne vont pas conduire à une situation de confiance extrêmement élevée. La seule manière d'atteindre le leadership en matière de confidentialité des données, avec un niveau d'éthique élevé, ainsi qu'une conformité sans heurts avec la réglementation, consiste à choisir une cybersécurité qui « comble les lacunes », en fournissant une défense complète prenant tout en compte : partenariats, cloud, clients et surtout, l'avenir.



Le carrefour technique en échangeur embrouillé (« Tech Spaghetti Junction ») des possibilités des télécommunications

Même l'oracle de Delphes ne pourrait probablement pas prédire exactement à quoi va ressembler le secteur des télécommunications dans une décennie. Nous avons mentionné à plusieurs reprises dans cet article la volte-face de WarnerMedia d'AT&T, non parce qu'il s'agit d'un événement extraordinaire, mais parce que cela prouve que l'industrie des télécommunications arrive réellement à un carrefour, et que même les prédictions et stratégies les plus audacieuses peuvent être susceptibles de changer.

En fait, nous devrions appeler « Tech Spaghetti Junction » ce carrefour des télécommunications qui s'annonce pour 2021-22. Mais c'est un « Tech Spaghetti Junction » des possibilités, quelle que soit la complexité de l'environnement de l'écosystème, quelle que soit la multitude de gammes de services et de modèles de modélisation susceptibles d'être offerts. La sensation écrasante dans ce secteur à l'heure actuelle représente l'une des opportunités. Lorsqu'il s'agit d'opportunités, il existe (dans le sens le plus large) deux risques à prendre en compte.

En premier lieu, on trouve la **peur de manquer quelque chose**, sensation que vous pouvez éprouver lorsqu'un concurrent bondit en avant pour s'approprier le départ sur un marché ou dans une région que vous n'avez pas encore été en mesure de cibler. Dans de nombreux cas, c'est peut-être la peur qui a retenu votre société de télécommunications, et tout particulièrement la crainte d'un risque de cybersécurité (ou d'une réglementation).

Le second risque est qu'**on ne vit qu'une fois** : se précipiter, car le marché semble « s'enflammer » et se sentir submergé par la sensation que le temps d'agir (établir un partenariat, se transformer, évoluer) est venu. Maintenant, ou jamais. Néanmoins, peu importe la mesure dans laquelle 2022 peut ressembler à un épisode de la ruée vers l'or en 1849, il est probable que les entreprises de télécommunications qui choisissent des stratégies d'innovation prudente (en plaçant la cybersécurité au centre) vont être celles qui seront finalement récompensées. La précipitation sans toute l'attention nécessaire est beaucoup trop risquée.

La « Tech Spaghetti Junction » des possibilités des télécommunications est la raison pour laquelle nous sommes, chez Kaspersky, si enthousiastes à propos du secteur des télécommunications. C'est pour cela que nous adorons contribuer à la transformation des télécommunications au niveau mondial, à développer et à découvrir de nouvelles façons de monétiser et d'optimiser, sans mettre en danger leur activité principale. Nous pensons qu'il faut aller de l'avant audacieusement, avec conviction et confiance. Mais nous savons également qu'une montée d'adrénaline est un risque trop important.

Cybersécurité par étape pour l'innovation dans le domaine des télécommunications

Nos solutions de cybersécurité dédiées au niveau de l'entreprise offrent la certitude et la confiance dont ont besoin des entreprises de télécommunications pour continuer à aller de l'avant au cours de la prochaine décennie de transformations. Tout comme avec la contribution du secteur pour nous aider à tous surmonter l'état d'urgence, nous sommes profondément convaincus que le monde dépend des services exceptionnels et passionnants que les leaders des télécommunications, tels que vous, allez nous apporter, au travail ou à domicile.

L'aide à la transformation des télécommunications mondiales consiste à offrir des solutions adaptées. Nous rencontrons nos clients des télécommunications là où ils se trouvent, en accordant en permanence la priorité à la continuité de l'activité et à l'innovation sécurisée.

Tout ce que nous faisons s'appuie sur la Threat Intelligence de Kaspersky reconnue mondialement, en renforçant notre recherche durable pour protéger les données, les clients et la continuité de l'activité 24h/24, 7j/7 contre les menaces avancées et les attaques ciblées.

Approche de la cybersécurité par étapes de Kaspersky

1

Kaspersky Security Foundations – protection de base essentielle automatisée et basée sur le cloud pour tous les appareils, infrastructures VDI et serveurs hybrides, avant que les organisations progressent en douceur vers...

2

Kaspersky Optimum Security - pour les organisations nécessitant une sécurité plus spécialisée contre les menaces nouvelles et évasives, avant de mettre en œuvre de manière fluide...

3

Kaspersky Expert Security – pour les organisations disposant d'équipes de sécurité informatique établies et matures luttant contre les attaques ciblées les plus complexes.

Cybersécurité niveau de maturité	Solution
Informatique Petites entreprises ne disposant d'aucune équipe spécialisée dans la sécurité informatique	**Quoi** Kaspersky Security Foundations **Comment** Mise en œuvre des éléments fondamentaux de la sécurité pour les organisations de toutes tailles et complexité, en délivrant une prévention automatique gérée dans le cloud contre les cybermenaces liées aux produits courants sur tous les appareils, les infrastructures VDI et de serveur hybride. ▸ **Terminaux :** Protégez chaque terminal de votre organisation avec Kaspersky Endpoint Security for Business ; Kaspersky Embedded Systems Security ▸ **Cloud :** Bénéficiez d'une sécurité sans limite avec Kaspersky Hybrid Cloud Security ▸ **Réseau :** Sécurisez votre périmètre avec Kaspersky Security for Mail Server ; Kaspersky Security for Internet Gateway ▸ **Données :** Protégez les données précieuses et sensibles avec Kaspersky Security for Storage ▸ **Gestion de la sécurité :** Accédez à l'expertise avec Kaspersky Premium Support ; Services professionnels Kaspersky
Cybersécurité Entreprises à la recherche d'une défense avancée, mais disposant de peu de ressources spécialisées en sécurité informatique	**Quoi** Kaspersky Optimum Security **Comment** Lutte contre les menaces évasives, grâce à une détection et une intervention efficaces sur les terminaux, ainsi qu'à un suivi continu de la sécurité, le tout sans les coûts prohibitifs et la complexité associés ▸ **Détection avancée :** Optimisez l'analyse comportementale fondée sur l'apprentissage machine, le sandboxing, la Threat Intelligence et la recherche de menaces automatisée* avec Kaspersky Sandbox, Kaspersky Threat Intelligence Portal et Kaspersky Managed Detection and Response Optimum ▸ **Analyse et investigation :** améliorez la visibilité des menaces et le processus d'enquête simplifié avec Kaspersky Endpoint Detection and Response Optimum ▸ **Réponse rapide :** déployez des options de réponse automatisées dans le produit, ainsi que des scénarios de réponse guidée et gérée* avec Kaspersky Endpoint Detection and Response Optimumet Kaspersky Managed Detection and Response Optimum ▸ **Sensibilisation à la sécurité :** équipez les employés avec des outils automatisés à tous les niveaux et développez des compétences de cybersécurité essentielles avec la formation de sensibilisation à la sécurité de Kaspersky *Soutenu par les experts Kaspersky

Équipe de sécurité informatique expérimentée et parfaitement qualifiée et/ou SOC dédié

- Disposent d'un environnement informatique complexe et distribué
- Constituent une cible privilégiée pour les attaques complexes et de type APT
- Ont une aversion pour le risque en raison des coûts élevés des incidents de sécurité et des violations de données
- Sont concernées par la conformité aux réglementations

Quoi
Kaspersky Expert Security

Comment
Maîtrise totale des cyberattaques les plus complexes et les plus ciblées

- **Équipé :** Donnez à vos experts internes les moyens de faire face à des incidents complexes dans le domaine de la cybersécurité. Profitez d'une solution de cybersécurité unifiée. **La plate-forme Kaspersky Anti Targeted Attack Platform,** qui repose sur **Kaspersky EDR**, offre à votre équipe des capacités XDR.
- **Informé :** approfondissez vos connaissances avec la Threat Intelligence et développez les compétences de vos experts pour gérer les incidents complexes :
  - Intégrez des informations sur les menaces immédiatement exploitables dans votre programme de sécurité. **Kaspersky Threat Intelligence** vous donne un accès instantané à une solution de Threat Intelligence technique, tactique, opérationnelle et stratégique.
  - Grâce à la **Kaspersky Cybersecurity Training**, développez les compétences pratiques de votre équipe interne, notamment en ce qui concerne l'utilisation de preuves numériques, l'analyse et la détection de logiciels malveillants, ainsi que l'adoption de pratiques exemplaires dans le cadre de la réponse aux incidents.
- **Renforcé :** faites appel à des experts externes pour assurer une évaluation de la sécurité, une assistance immédiate et un soutien :
  - Profitez de l'assistance immédiate de l'équipe **Kaspersky Incident Response**, composée d'analystes et d'enquêteurs très expérimentés, pour résoudre votre cyberincident de manière rapide et efficace.
  - Avec Kaspersky **Managed Detection and Response**, vous bénéficiez d'un deuxième avis et de l'expertise d'un partenaire de confiance en matière de Threat Hunting. Vos experts internes en sécurité informatique disposent ainsi de plus de temps pour réagir aux problèmes critiques qui requièrent leur attention.
  - Déterminez le niveau d'efficacité de vos défenses contre les cybermenaces potentielles et si vous représentez déjà la cible involontaire d'une attaque furtive à long terme, grâce à **Kaspersky Security Assessment**.

Solutions ciblées

Quoi	Comment
Kaspersky Fraud Prevention	Advanced Authentication (l'authentification avancée) permet une authentification sans friction et continue, réduisant les coûts de traitement du deuxième facteur de l'authentification pour les utilisateurs légitimes, tout en conservant des taux de détection de fraude élevés en temps réel. Automated Fraud Analytics analyse minutieusement les événements qui se produisent au cours de l'intégralité de la session en les transformant en données précieuses. Protège le périmètre extérieur de n'importe quelle entreprise, assurant la sécurité et la protection des clients.
Kaspersky DDoS Protection	Couvre une bande passante allant jusqu'à 2 Gbits/s, avec couverture de service étendue, comprenant les rapports d'analyse d'attaque et les évaluations de capacité anti-DDoS. Atténuation des risques DDoS permanente et automatique facultative, enrichie par les ingénieurs de Kaspersky qui effectuent des vérifications parallèles pour optimiser la défense en fonction de la nature de chaque attaque DDoS.

Actualités sur les cybermenaces : www.securelist.com

Actualités dédiées à la sécurité informatique : www.kaspersky.com/blog

Portail de Threat Intelligence : opentip.kaspersky.com

Aperçu des technologies : www.kaspersky.com/TechnoWiki

Prix et distinctions : https://www.kaspersky.fr/about/awards

Portefeuille produits interactif : kaspersky.com/int_portfolio

kaspersky PRÊTS POUR L'AVENIR