Construire un avenir plus sûr pour les gouvernements

kaspersky PRÊTS POUR L'AVENIR

https://go.kaspersky.com/Gouv-FR.html

2021

Introduction

Lorsqu'il s'agit de technologie, le secteur gouvernemental porte deux casquettes distinctes, et souvent en concurrence : celle du client et celle de l'organisme de règlementation. En amorce de notre enquête concernant les opportunités et les risques auxquels les gouvernements font face pour concevoir un fonctionnement en réseau de plus en plus intelligent, il est utile d'examiner chacune de ces casquettes à tour de rôle.

Le gouvernement en tant que client

La privatisation et l'externalisation de services civiques essentiels entraînent la concurrence, ce qui peut générer des économies de coûts pour les organismes gouvernementaux locaux. Par exemple, à Londres uniquement, 14 arrondissements sur 32 externalisent la collecte des déchets à la transnationale française Veolia. Toutefois, lorsqu'il s'agit de services civiques tels que la collecte des déchets, l'externalisation est un **choix** que font les gouvernements locaux, en fonction de leurs propres besoins et budgets.

Lorsqu'il s'agit d'Internet et d'autres services informatiques, l'externalisation n'est **pas** un choix : les gouvernements n'offrent pas de tels services en interne. Alors que les gouvernements sont toujours en mesure d'émettre des appels d'offres pour ces contrats, un fait demeure : ils sont toujours tributaires des opérateurs privés externes pour la prestation de services qui sont de plus en plus essentiels, et de plus en plus complexes. Ainsi, même si les gouvernements sont toujours en mesure de lancer ces contrats dans des appels d'offres en suivant des processus d'approvisionnement rigoureux, l'externalisation des contrats pour lesquels la technologie est essentielle n'est pas facultative, elle est **obligatoire**.

Cette dynamique signifie que les gouvernements sont toujours, dans une certaine mesure, à la merci de la qualité, de la cohérence, de la sécurité et de la fiabilité des acteurs privés externes pour les services réseau, et qu'ils ne peuvent plus faire sans.

Cette dépendance chronique est à la fois protégée et compliquée par l'autre casquette du gouvernement, celle de l'organisme de réglementation.

Le gouvernement en tant qu'organisme de règlementation

Le pouvoir des gouvernements sur les fournisseurs de technologie privée (et autres) est immense. Dans le monde entier, les éditeurs doivent composer avec un immense éventail de normes imposées par le gouvernement, soit une concaténation de normes ISO, CISQ, SOP, NERC, NIST, RFC, ANSI, IEC, etc. qui, si elles ne sont pas respectées, constituent un refus de contrat et une éventuelle dissolution.

Pourtant, le rôle du gouvernement en tant qu'organisme de réglementation ne se limite pas à faire appliquer les normes essentielles aux fournisseurs de services. Comme les données sont désormais considérées comme le « nouvel or noir », les réglementations, telles que le système européen de contrôle RGPD, contrôlent la façon dont les données sont utilisées et protègent les droits des citoyens.

Composer avec ces responsabilités réglementaires s'avère être l'avènement d'un nouveau théâtre de guerre, celui du cybercrime international. D'un point de vue intrinsèque, Internet n'a aucune limite : même dans les pays qui restreignent l'accès à des services tels que Facebook ou WhatsApp, les citoyens utilisent couramment les réseaux privés virtuels (VPN) pour contourner ces interdictions. Le cybercrime international est un grand terme générique qui englobe tout : les e-mails de phishing, les attaques inspirées du terrorisme pour des services vitaux essentiels et, bien sûr, l'espionnage. Les motivations réglementaires ne sont donc pas seulement basées sur la nécessité de protéger le droit à la vie privée des citoyens, elles sont aussi basées sur la protection de l'intégrité des entreprises et sur la défense des gouvernements eux-mêmes.

La dépendance à l'égard des services qu'il réglemente lui-même fait du secteur gouvernemental un secteur unique dans le cadre des relations qu'il entretient avec les fournisseurs de services de réseau. Cela fait entrer des éléments intéressants en jeu, en particulier compte tenu des immenses progrès technologiques qui révolutionnent la façon dont les gouvernements fonctionnent dans le monde entier.

Les citoyens en tant que clients

Un « gouvernement ne peut pas hiérarchiser ses citoyens 'clients' en utilisant des indicateurs donnant leur valeur ou leur coût, des pratiques courantes dans le secteur privé dans des circonstances similaires. »
McKinsey

« HMRC a pour ambition de devenir l'une des administrations fiscales les plus avancées sur le plan numérique au niveau mondial… le compte d'impôt personnel réunit toutes les informations du client sur une seule et même plate-forme en ligne. Cela permet aux clients d'accéder au service depuis l'appareil numérique de leur choix et lorsqu'ils le souhaitent. Ils peuvent ainsi s'inscrire à de nouveaux services, mettre à jour leurs informations et voir les impôts qu'ils doivent payer. »
Her Majesty's Revenue & Customs, UK

Les gouvernements vont et viennent, mais la relation structurelle entre le gouvernement et les citoyens a toujours le monopole. Chaque pays, chaque région, ne peut avoir qu'un seul gouvernement à la fois. Les citoyens n'ont pas à choisir parmi une sélection, comme ils le font lorsqu'il s'agit d'opérateurs de marché.

Même dans les pays où le gouvernement au pouvoir change tous les quatre ans, l'organisation de la fonction publique, qui exécute la volonté de ce gouvernement, change très rarement. La longévité de carrière au sein des départements des services publics dépasse celle des entreprises privées. C'est l'un des rares secteurs dans lesquels on peut encore réellement avoir « un emploi à vie ».

En dépit de ce monopole, la relation que le citoyen entretient avec le gouvernement ressemble toujours à une relation client-fournisseur.

Les gouvernements ont des responsabilités réglementées envers leurs consommateurs pour remplir les accords de niveau de service (SLA), qu'ils soient implicites ou explicites, mais, au même titre que les entités privées, leur longévité dépend de la satisfaction de la clientèle.

Les gouvernements utilisent la technologie pour satisfaire leurs clients-citoyens de deux façons principales. Premièrement, par l'intermédiaire du bon fonctionnement des services nationaux (ou régionaux), tels que les services mis en œuvre dans les villes intelligentes, ou l'initiative Making Tax Digital du Royaume-Uni. Deuxièmement, en protégeant les clients-citoyens contre le cybercrime.

Nous savons où vous vivez

Les gouvernements en savent bien plus à propos de leurs clients que tout acteur du marché. Ils connaissent notre date de naissance, ils savent combien nous gagnons, ils connaissent notre état de santé, l'endroit où nous vivons, notre date de mort et même l'endroit où nous sommes enterrés. Les données accumulées sont riches et interminables. Les citoyens doivent pouvoir faire confiance aux gouvernements pour garder ces ensembles de données sensibles et exhaustives à l'abri des regards indiscrets et malveillants.

Toutes les industries ont une responsabilité en matière de protection des référentiels de données sensibles qu'elles accumulent. Néanmoins, lorsqu'il s'agit du gouvernement, les enjeux sont nettement plus élevés.

Le manque de maturité technologique au sein des gouvernements

L'image du bureaucrate gratte-papier tend à disparaître. En l'absence de pressions de la concurrence sur le marché privé, l'adoption de technologies dans les gouvernements peut être ralentie par l'inertie à la fois sur le plan individuel et collectif (organisationnel). Il a été démontré que les gouvernements sont à la traîne derrière le secteur privé en matière de maturité technologique, cette disparité étant encore plus importante dans les pays en développement. Dans un environnement dans lequel de nombreuses technologies manquent également de maturité (la blockchain, par exemple), ce retard représente un défi énorme pour les gouvernements lorsqu'ils se lancent dans l'innovation.

Dans ce document, nous allons étudier les huit tendances technologiques principales et leurs conséquences sur les gouvernements du monde entier. Pour chaque tendance, nous allons également présenter les principaux risques et défis dont les gouvernements doivent être conscients pour protéger les pays ou les régions dont ils sont responsables, et obtenir la plus grande satisfaction des citoyens-clients.

« Avant la pandémie, les agences devaient principalement « faire du numérique », c'est-à-dire tirer parti des technologies numériques en vue d'améliorer leurs capacités, mais en reposant toujours en grande partie sur des modèles d'exploitation anciens. La COVID-19 a propulsé de nombreux gouvernements vers l'étape suivante de la transformation numérique. 70 % des agences gouvernementales indiquent que les initiatives de transformation numérique impulsées pendant la pandémie ont déjà des effets positifs sur leur organisation. »
Deloitte

Engagement des citoyens et identité numérique

Transformation numérique **Réalité augmentée et réalité virtuelle**

Paiements et signatures électroniques **l'IA/ML** **Blockchain**

Villes intelligentes **Aspects réglementaires**

Tendance n° 1 : Transformation numérique – innovation dans le secteur public

« Près de la moitié des organismes gouvernementaux utilisent activement les services cloud. »
Gartner

41,86 milliards de dollars

« Le marché du cloud du gouvernement des États-Unis était estimé à 14,93 milliards de dollars en 2019 et devrait atteindre 41,86 milliards d'ici 2025, avec un taux de croissance annuel composé de 18,74 % sur la période 2020-2025. »
GlobeNewsWire

« La pandémie de COVID-19 a accéléré l'avènement d'un gouvernement réellement numérique, avec des agences leaders qui établissent des éléments essentiels de l'infrastructure numérique, les besoins en effectif et la connectivité des citoyens. »
Deloitte

La transformation numérique est un vaste sujet qui pourrait couvrir chacune des tendances et chacun des défis que nous allons étudier dans ce document. Après tout, la transformation numérique, c'est ce qui arrive à la société, que les citoyens le veuillent ou non, lorsque les gouvernements mettent en œuvre des solutions technologiques pour résoudre des problèmes d'ordre civique. Toutefois, dans le cadre de notre étude, nous allons parler de la transformation numérique interne ; c'est-à-dire l'utilisation d'innovations technologiques pour transformer les activités des organismes gouvernementaux.

Étant donné que l'adoption du cloud est la condition **sine qua non** de la transformation numérique, il est utile d'examiner l'attitude des organismes gouvernementaux face à la transformation numérique à travers le prisme de l'adoption du cloud. Gartner prévoit une augmentation de 23,1 % des dépenses des utilisateurs finaux dans le monde entier pour des services de cloud public en 2021, pour un total d'investissement de 332,3 milliards de dollars. Pour 2022, la prévision est de 480 milliards de dollars.

Toutefois, ces statistiques optimistes diffèrent légèrement lorsque nous comparons la proportion entre le cloud privé et le cloud public entre les gouvernements.

Il va sans dire que la vie privée est une préoccupation majeure pour le gouvernement, notamment en raison du modèle citoyen-client qui propulse l'engagement numérique, et des services publics (y compris les services de paiement d'impôt local) proposés en ligne. Les énormes quantités de données citoyen-client très sensibles que les gouvernements détiennent et traitent expliquent pourquoi l'adoption du Cloud est plus importante dans le secteur privé que dans le secteur public.

La souveraineté des données est également une des raisons pour lesquelles les gouvernements sont moins susceptibles d'adopter les services de Cloud public (et donc d'en bénéficier). En vertu de ce principe, les données doivent être traitées ou conservées uniquement dans le pays ou la région dans lequel/laquelle elles ont été collectées. La préoccupation à laquelle les gouvernements font souvent face est la suivante : comment peuvent-ils garantir que des données conservées dans un Cloud public ne seront pas conservées à l'étranger, voire dans un pays avec laquel ils ne partagent pas de cadre réglementaire fiable ? Quelles seraient les implications en matière de conformité ?

Une partie du problème concerne l'immaturité technologique de certains organismes gouvernementaux. Encore confrontés à des systèmes hérités ainsi qu'à une évolution tardive due à la prudence (parfois justifiée),

« Cette accélération (de l'innovation numérique) offre aux leaders gouvernementaux de nouvelles opportunités pour tirer parti des données et des technologies qui établissent la confiance, l'agilité et la résilience dans les institutions publiques. »
Gartner

les fonctionnaires manquent souvent de formation en matière de cybersécurité, nécessaire pour pouvoir faire avancer les stratégies de transformation numérique essentielles sans craindre les cyberattaques. En fait, Gartner cite le « manque de personnel qualifié » comme l'un des défis auxquels font face les gouvernements lorsqu'il s'agit de moderniser des systèmes hérités, et prévient que « l'adoption de technologies émergentes et le passage au gouvernement numérique sont entravés par la culture et le manque de compétences. »

Cette attitude prudente envers l'adoption du Cloud public, bien qu'en partie compréhensible, signifie que les gouvernements qui poursuivent leur transformation numérique peuvent perdre une partie de l'agilité et de l'efficacité associées à l'utilisation du Cloud public.

Transformation numérique – Pleins feux sur la menace – Prudence invalidante

99 %

L'Estonie a bâti un écosystème efficace, sécurisé et transparent, dans lequel 99 % des services gouvernementaux sont en ligne.

Globalement, les gouvernements ont accéléré le déploiement des systèmes de gestion de crise des services numériques en réponse à la pandémie de COVID-19 actuelle. Le numérique est devenu la nouvelle norme maintenant que les gouvernements du monde entier se dépêchent pour transformer les services et bénéficier de gains de productivité et financiers.

Cependant, contrairement aux industries commerciales qui n'ont d'autre choix que de faire confiance au cloud public (ou qui risquent d'être évincées par des concurrents plus efficaces), les gouvernements sont, dans une certaine mesure, capables de se rabattre sur la dynamique du monopole abordée plus tôt.

Le risque est que, si les gouvernements ne parviennent pas à mettre en œuvre des formes d'adoption du Cloud similaires à celles exploitées par les banques et les industries, un décalage critique se produise. Les gouvernements peuvent avoir du mal à fournir les services numériques qu'attendent de plus en plus les clients-citoyens.

Ensuite, les environnements numériques des gouvernements peuvent diverger considérablement par rapport à ceux des entreprises relevant de leur juridiction, provoquant ce que l'on appelle plus couramment « des problèmes de communication. »

Ces problèmes de communication peuvent se traduire par une incapacité à comprendre « la vie sur le terrain » ou par des difficultés d'externalisation en raison de systèmes incompatibles. Ajouté à cela, un manque de maîtrise des systèmes numériques potentiellement idiosyncrasiques du gouvernement peut entraîner un manque de compétences, en vertu de quoi les personnes hautement qualifiées peuvent ne pas être disposées à (ou se voir dans l'impossibilité de) transmettre les compétences inestimables qu'ils auraient acquises dans le secteur privé.

Les implications de cette prudence sont conséquentes, et placent la cybersécurité et la vie privée en première position dans la liste des risques. S'appuyer sur des solutions propriétaires « décalées » plutôt que de se tourner vers les solutions de Cloud novatrices utilisées sur le marché libre pourrait exposer les données du gouvernement à de nombreuses vulnérabilités non corrigées pouvant attirer les attaques malveillantes.

Si l'adoption du Cloud est excessivement limitée au Cloud privé, tout le patrimoine numérique pourrait être exposé à des attaques, bien que le cloisonnement via une architecture de Cloud hybride correctement orchestrée pourrait permettre de conserver les données stratégiques en toute sécurité.

Même si les gouvernements fournissent des efforts considérables en matière de cybersécurité pour leurs organisations de renseignement et de défense nationale, ils auront toujours besoin de leaders en matière de solutions de cybersécurité dans le secteur privé pour défendre leurs opérations internes et protéger leurs stratégies de transformation numérique. Ils doivent donc prendre des décisions éclairées et réfléchies, en recherchant des stratégies de transformation numérique qui permettront de les préparer à garantir une cyberdéfense robuste pour leurs opérations.

Tendance n° 2 : Engagement des citoyens et identité numérique

« Notre objectif ultime est de permettre aux résidents de mener toutes leurs affaires avec le gouvernement, sans jamais entrer dans un bureau du gouvernement. »
Ervan Rodgers Ohio (ancien) CIO

Pendant la pandémie de COVID-19, les gouvernements du monde entier ont connu une demande croissante de la part des citoyens pour disposer de meilleurs services gouvernementaux en ligne. Ainsi, la vitesse à laquelle les services numériques gouvernementaux se sont développés est une conséquence inattendue de la pandémie. De tout nouveaux services numériques ont été développés et déployés pour faire face à un monde en confinement, dans lequel les citoyens avaient besoin de collaborer de manière transparente avec le gouvernement à l'aide de plusieurs canaux.

En 2021, les habitants des pays développés se sont habitués à un engagement exigeant aligné sur leurs besoins immédiats comme étant un droit. Ils attendent désormais de pouvoir interagir avec les organisations gouvernementales au moment où ils le souhaitent, en utilisant l'appareil de leur choix, exactement comme ils interagissent avec les entreprises du secteur privé les plus avancées technologiquement. Pour faire simple, ils veulent des possibilités fluides sur plusieurs canaux et souhaitent que celles-ci soient comparables à ce que ce qui se fait de mieux dans ce que le secteur public peut leur offrir.

Les gouvernements ont répondu en accélérant le concept d'engagement citoyen, en déployant une large offre de services et d'engagements en ligne couvrant pratiquement tous les aspects de la vie d'un citoyen. Ils mettent également en place des mesures en ligne pour impliquer davantage les citoyens dans la mise en forme des processus gouvernementaux. Gartner s'attend à ce que 30 % des gouvernements utilisent des mesures d'engagement pour suivre la quantité et la qualité de la participation citoyenne dans les décisions relatives à la politique et aux budgets d'ici 2024.

L'identité numérique du gouvernement se trouve au cœur de l'engagement citoyen sur plusieurs canaux. La pandémie de COVID-19 et les confinements qui se sont ensuivis ont démontré à quel point il était essentiel d'être en mesure de valider à distance des informations d'identité.

82 %

« 82 % des directeurs informatiques gouvernementaux constatent une augmentation de l'utilisation des canaux numériques pour joindre les citoyens en 2020 et s'attendent à ce que cette augmentation se maintienne en 2021. »

73 %

« 73 % des directeurs informatiques gouvernementaux indiquent que le rôle des canaux en libre-service pour l'assistance des citoyens a augmenté en 2020. »
Enquête Gartner réalisée auprès de directeurs informatiques en 2021

« Gartner prévoit qu'une véritable norme d'identité mondiale, portable et décentralisée va émerger sur le marché d'ici 2024, afin de traiter les cas d'utilisation professionnelle, personnelle, sociale et sociétale et d'absence de visibilité de l'identité. »
GartnerTop 10 government technology trends

Aucune interaction en personne n'était possible, mais les utilisateurs avaient quand même besoin d'accéder à toute la gamme des services gouvernementaux. Toutefois, les citoyens technophiles ne s'attendent pas à rencontrer des complications pour accéder directement aux services. Bien que les services gouvernementaux s'en soient admirablement bien sortis, l'authentification et la preuve d'identité sont devenues fastidieuses, avec une navigation difficile. Une seule identité numérique permettant d'accéder à tous les services gouvernementaux en ligne est donc devenue la priorité absolue dans les pays développés.

Une unité numérique unique, qui comprend et réunit tous les services gouvernementaux utilisés par un citoyen, offre des avantages évidents : fluidification de la livraison du service, accumulation de données pour rendre les services plus intuitifs et proactifs, invitation des clients à effectuer les actions suivantes, élimination de la réinitialisation des mots de passe pour des services gouvernementaux individuels, et amélioration de l'expérience client globale : tout cela mené sans compromettre les données ou exposer les systèmes à de nouvelles menaces. Le concept d'identité numérique des citoyens est également en train de s'élargir et de s'adapter pour satisfaire l'augmentation des demandes.

Engagement citoyen et identité numérique – Pleins feux sur la menace

La transformation de la culture dans les agences gouvernementales, afin d'atteindre les mêmes normes que le secteur privé, est un défi considérable. Pour une identification numérique et un engagement des citoyens efficaces, les gouvernements doivent acquérir les compétences pour exploiter les données et les renseignements afin de générer les solutions qui feront partie de l'expérience fluide sur plusieurs canaux.

Toutefois, l'augmentation des services gouvernementaux et la manipulation potentielle des données génèrent des inquiétudes parmi les citoyens. Les cyniques qualifient l'identité numérique et l'engagement des gouvernements en faveur de plusieurs canaux de porte ouverte à la surveillance de masse, à une mauvaise utilisation des données et à un profilage des citoyens. Les gouvernements doivent instaurer la confiance en garantissant la responsabilité et la transparence. Toute faille de cybersécurité ruinera la confiance des citoyens : assurer la sécurité est un impératif au cœur de la stratégie d'engagement des gouvernements. Le fait de reposer sur une solution de sécurité qui ne serait pas optimale augmente le risque d'exposition des données gouvernementales critiques. Plus que jamais, les solutions de cybersécurité des meilleurs acteurs du secteur privé sont nécessaires pour protéger les gouvernements lorsqu'ils transfèrent la grande majorité de leurs opérations en ligne.

Pour conclure, les gouvernements viennent de comprendre comment il est devenu essentiel de fournir une identité numérique et des services en ligne sur plusieurs canaux qui correspondent aux attentes croissantes de leurs citoyens. Les gouvernements qui sont lents à effectuer cette transformation risquent de se mettre à dos les citoyens, en particulier la jeune génération. Cependant, l'identité numérique et l'engagement des citoyens s'accompagnent de l'énorme responsabilité supplémentaire de protéger tous les services présentés contre les failles ou les risques de cybersécurité.

Tendance n° 3 : paiements et signatures électroniques – le cœur de la gouvernance électronique

Généralement, les citoyens s'habituent aux nouvelles technologies bien avant que leurs gouvernements les mettent en œuvre dans les services qu'ils proposent. Nous utilisons peut-être Alexa à la maison, et nous payons peut-être via Apple Pay, mais nous avons encore besoin de recourir à des processus fastidieux et frustrants pour déclarer ou payer nos impôts.

Les innovations que sont le paiement électronique et la signature numérique ont progressivement été appliquées par les gouvernements dans le monde entier. Nous avons déjà mentionné le Royaume-Uni et son initiative Making Tax Digital, mais le Royaume-Uni est loin d'être le seul pays à mettre en œuvre des initiatives en matière de paiement électronique et de fiscalité numérique. En juin 2018, Singapour a annoncé que le pays était déterminé à proposer les options de paiement électronique et de signature numérique pour tous les services gouvernementaux d'ici 2023. Cet engagement a été lancé par le bureau national Smart Nation and Digital Government Office.

Une décennie numérique en une seule année

La pandémie de COVID-19 a été de loin la plus grande impulsion vers un gouvernement électronique. Tout le monde étant « bloqué à domicile, dans l'impossibilité de se rendre visite ou de travailler dans les bureaux, le besoin de services gouvernementaux sans contact, facilité par les signatures numériques, est devenu impératif. « Une décennie numérique en une seule année » est ce que la conférence sur la gouvernance électronique de mai 2021 à Tallinn, en Estonie, a décrit comme l'évolution spectaculaire vers les services en ligne.

Le vote : la signature numérique la plus puissante qu'un citoyen puisse apposer

Le gouvernement du Canada cite l'utilisation généralisée des technologies d'Internet sur le plan professionnel et sur le plan récréatif par ses citoyens comme l'un des moteurs essentiels dans le cadre de l'instauration du vote électronique, dans l'exposé et la défense plutôt longs de ses plans destinés à élaborer cette technologie. La recherche sur l'attitude contrastée des citoyens au sujet du vote électronique menée par le gouvernement canadien a permis de démontrer ce qui suit :

« La valeur du marché mondial de la signature numérique s'élevait à 1 858,3 millions de dollars en 2020, et devrait présenter un taux de croissance annuel composé de 29,2 % pendant la période de prévision (2021–2030). »
PSmarketresearch

« Un peu moins de la moitié des électeurs (49,1 %) sont d'accord, 31,5 % sont plutôt d'accord et 17,6 % sont tout à fait d'accord sur le fait que les « Canadiens et les Canadiennes devraient avoir la possibilité de voter par Internet lors d'élections fédérales. » Ces pourcentages tranchent avec les 39,4 % d'électeurs qui ne sont pas d'accord. » Et pourtant, dans les régions où la technologie a été mise à l'épreuve, l'accueil a été tout sauf contrasté, et la plupart des Canadiens (en réalité 99 %) ont affirmé être susceptibles d'utiliser le vote en ligne s'ils en avaient la possibilité.

Les paiements électroniques et les signatures numériques - Pleins feux sur la menace - Est-ce vraiment vous ?

Selon un livre blanc Forrester, les flux de travail relatifs à la signature électronique font progresser l'activité, tout en stimulant la croissance des revenus à long terme grâce à une amélioration de l'expérience des clients et des employés. Les gens ne veulent simplement plus perdre de temps dans une file d'attente pour signer en personne, alors qu'ils savent très bien qu'il existe une technologie qui permet de faire ces choses-là en un clin d'œil en ligne.

Toutefois, les signatures numériques présentent clairement un risque de cybersécurité et, si des mesures concrètes ne sont pas prises par les gouvernements qui adoptent la technologie, l'usurpation d'identité à grande échelle pourrait progresser, étant donné que les criminels pourraient utiliser des signatures numériques volées et abattre ainsi les barrières existantes imposées par la vérification d'identité en personne.

Les règlementations gouvernementales relatives aux signatures numériques varient d'une région à l'autre. Le règlement eIDAS (Identification électronique et services de confiance) mis en place par l'UE insiste sur les « signatures qualifiées » et sur les certificats délivrés par les fournisseurs de services de confiance, alors qu'aux États-Unis, il n'existe pas de telle exigence.

La fraude en matière de signature numérique est entrée en scène presque en même temps que le lancement de la technologie. En 2011, un homme d'affaires de Rome a découvert que toutes les actions de sa société avaient été transférées à un fraudeur qui utilisait la fraude à la signature numérique pour se faire passer comme l'unique directeur de l'entreprise.

Tendance n° 4 : La réalité numérique (RA/RV) dans le gouvernement

Construire un avenir plus sûr pour les gouvernements

« Je suis convaincu qu'une partie importante de la population qui vit dans les pays développés, et peut-être dans tous les pays, vivra quotidiennement des expériences de RA (réalité augmentée), et que cela deviendra presque une habitude, comme manger trois repas par jour. Cela fera partie de vous. »
PDG d'Apple, Tim Cook

« La [RA] offre aux travailleurs des outils pour interagir avec les données numériques dans le monde réel. »
Deloitte

Parmi les deux principales catégories de réalité numérique, les gouvernements sont plus susceptibles d'adopter la réalité augmentée, plutôt que la réalité virtuelle. Alors que la seconde implique la création intégrale de « mondes » virtuels, la réalité augmentée (RA) implique la superposition graphique d'éléments de réalité numérique sur des images en temps réel du monde tel qu'il est.

Une des applications essentielles de la RA pour le gouvernement consiste à permettre aux travailleurs sur le terrain de voir en temps réel comment réparer ou construire exactement une ressource publique ou un bien public, simplement en suivant les signaux visuels, audio et haptiques de la RA, grâce notamment aux dispositifs d'affichage visiocasques mains libres (HMDS). Cela augmente considérablement la portée géographique des travailleurs techniques, et permet d'atteindre le double objectif qui comprend l'amélioration de la précision et la réduction des coûts.

La RA peut être appliquée à d'innombrables applications incluant l'engagement de citoyens, l'armée, la sécurité, les services d'urgence, l'offre culturelle, l'éducation, la santé, la maintenance et les transports. La navigation est également une application essentielle pour les trains, les avions et les automobiles. Les superpositions graphiques guident les conducteurs et les pilotes pour un atterrissage ou une arrivée en toute sécurité, comme nous l'espérons à chaque fois.

Tirer parti de la richesse des données obtenues grâce à l'IoT et aux villes connectées (dont nous reparlerons plus loin), multiplie les applications potentielles de la RA, en particulier lorsqu'il s'agit de la planification stratégique. Par exemple, à l'aide de données relatives à la circulation automobile et pédestre, les gouvernements peuvent voir l'effet qu'une série de décisions pourrait avoir sur le flux du trafic, sur la sécurité et sur la pollution.

L'éducation financée par l'État est un autre secteur en train d'adopter la RA aussi vite que possible afin d'affronter la révolution de l'apprentissage à distance déclenchée par la pandémie de COVID-19. L'apprentissage à distance optimisé va continuer à se développer globalement dans les systèmes d'éducation.

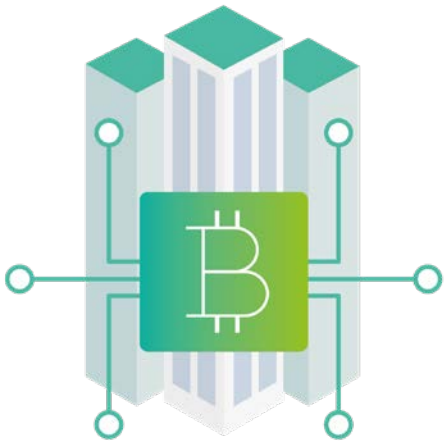
Réalité numérique - Pleins feux sur la menace - Au-delà de la distraction

L'aviation a toujours été une cible terroriste clé, depuis les pirates de l'air de 1970 aux attentats suicides du 11 septembre. Comme les pilotes s'appuient de plus en plus sur la RA pour l'aide à la navigation, éviter les risques (tels que les vols d'oies sauvages), améliorer l'efficacité énergétique et permettre des atterrissages sécurisés, des terroristes de l'air pourraient lancer des attaques en toute sécurité depuis leur propre poste de travail.

Pour ce qui est du secteur gouvernemental, l'aviation militaire a été particulièrement rapide pour saisir les opportunités qu'offre la RA. BAE, une multinationale britannique qui travaille dans les secteurs de la défense, de la sécurité et de l'aérospatial, a développé un dispositif d'affichage couleur à RA adaptable sur casque qui projette les écrans et les commandes d'un cockpit interactif en réalité virtuelle et en réalité augmentée directement devant les yeux du pilote, remplaçant les agencements actuels des cockpits. D'après le chef-pilote d'essai de l'entreprise, Steve Formoso, la technologie « fournit un précieux avantage sur celui contre qui vous vous battez ».

Le problème, c'est que la RA pourrait permettre à des terroristes de pirater les vulnérabilités et de déplacer efficacement le théâtre d'une cyberguerre du bureau (dans le cas du cyberterrorisme conventionnel) au cockpit militaire. Dans le cas de l'aviation militaire, l'utilisation de la RA en est encore à ses balbutiements, mais l'enquête canonique sur les risques liés aux domaines technologiques émergents, réalisée par l'université Carnegie Mellon, a déjà averti que « la criticité de tels systèmes ne fait aucun compromis sur le fait qu'un événement à risque potentiellement élevé fasse des victimes. »

Les risques s'étendent au-delà l'interférence fatale directe avec les champs visuels des pilotes, et comprennent l'espionnage en temps réel et les éventuelles fuites critiques.



Tendance n° 5 : Blockchain dans le secteur public

L'utilisation de blockchains a été lente, jusqu'à ce jour, dans le secteur gouvernemental. L'immaturité de la technologie, combinée à la barrière que représentent la complexité et la mysticité des blockchains, ainsi que leur association avec les cryptomonnaies, en sont probablement la cause.

Selon l'enquête Gartner réalisée auprès des directeurs informatiques au sein du gouvernement, alors que 66 % s'intéressent à la blockchain, seulement 20 % ont planifié une action. Parmi les applications probables figurent l'identification des citoyens, le droit de vote, la réalisation de transactions, ainsi que les finances.

En revanche, certaines régions sont en avance sur les autres en ce qui concerne la mise en œuvre de blockchains, la Chine étant peut-être dans le peloton de tête. Alibaba et Ant Financial ont conduit un partenariat public-privé pour développer des applications de blockchain pour le gouvernement. Shanghai, Shanxi, Henan, Guangzhou, Guiyang et Hangzhou ont tous élaboré des politiques visant à encourager le développement des blockchains.

Sous la forme d'un ordre direct du président Xi Jinping, le soutien du gouvernement central met en évidence l'utilisation de technologies blockchain pour créer une Smart City, dans le cadre du plan directeur pour la zone économique du nouveau district de Xiongan.

Ce leadership technologique audacieux est susceptible d'inspirer des applications similaires dans le monde entier, car les organismes gouvernementaux tendent à adopter des applications de blockchains urbaines « testées et éprouvées », et qu'ils sont soucieux de ne pas se laisser distancer.

83,3 milliards de dollars

« Un marché de 4,47 millions de dollars dans le monde en 2020, qui devrait croître rapidement jusqu'à 83,3 milliards de dollars en 2027, à mesure que les banques centrales comprennent comment utiliser la blockchain dans leurs initiatives de devises numériques. » prnewswire

La technologie blockchain, qui est décentralisée et basée sur la technologie des registres distribués, réduit considérablement la nécessité d'une autorité centrale telle qu'un gouvernement (paradoxalement). Toutefois, ce n'est pas aussi effrayant que ça en a l'air. En fait, il est peu probable que la technologie blockchain détruise les gouvernements centraux, mais si elle est utilisée de manière appropriée, elle permettra d'éliminer les points centraux de défaillance, de garantir des données essentielles et des transactions plus sécurisées que jamais afin de protéger les citoyens.

Blockchain – Pleins feux sur la menace – Les risques encourus et la non-réglementation

La plupart des organismes gouvernementaux sont susceptibles d'utiliser des blockchains « privées » plutôt que des blockchains « publiques » (à la Bitcoin). Le bureau de l'innovation dans le secteur public (OPSI) de l'OCDE compare cette distinction à celle de l'utilisation de l'intranet au lieu de l'Internet.

En raison de l'utilisation de registres privés, les gouvernements doivent mettre en œuvre des modèles de consensus rigoureux qui restreignent les autorisations d'utilisation, sans restreindre l'efficacité de la technologie.

Plusieurs aspects de la technologie blockchain présentent des risques et des défis importants pour les gouvernements qui souhaitent la mettre en œuvre. Il peut exister un conflit concernant la réglementation sur la protection des données, en raison de l'immutabilité inhérente à la blockchain (les données peuvent être ajoutées, mais pas supprimées).

Le stockage de données peut également relever du défi : une blockchain est conçue pour une utilisation très restreinte, elle n'est pas conçue pour fonctionner dans les énormes data center privés auxquels les gouvernements sont habitués. La complexité reste un défi, et (comme nous l'avons vu en Chine) la plupart des gouvernements auront besoin de confier une très grande partie de la conception et du codage à des prestataires externes s'ils entendent mettre en œuvre des blockchains à grande échelle. L'audit et le suivi d'un si large éventail de fournisseurs vont être un enjeu majeur.

L'interopérabilité est l'un des principaux problèmes qui pourraient être résolus grâce à la mise en œuvre de normes. Le manque d'interopérabilité actuel est une arme à double tranchant, comme l'explique Deloitte : « Le manque de normes garantit la liberté des développeurs et des codeurs de blockchains et peut donner des maux de tête aux départements informatiques lorsqu'ils découvrent que les plates-formes ne peuvent pas communiquer sans l'aide de la traduction. »

Étant donné que chaque réseau blockchain utilise ses propres plates-formes, mécanismes de codage et autres particularités très spécifiques, il peut être difficile d'intégrer en toute sécurité une solution blockchain dans un environnement de données en réseau existant. Si les normes ne sont pas suffisamment rigoureuses, l'interopérabilité en soi pourrait engendrer des problèmes pouvant nuire à la sécurité bien connue des blockchains, comme l'explique un analyste de CapGemini :

« Compte tenu de l'interopérabilité entre les réseaux, les problèmes de sécurité d'un réseau peuvent facilement être déportés vers un autre réseau par le biais d'intégrations ou d'appels de contrats intelligents. Cela peut compromettre la sécurité de l'ensemble du réseau. »

Tendance n° 6 : Gouvernance de villes intelligentes et IoT

Les villes intelligentes n'ont pas besoin d'être aussi ambitieuses et globales que la zone économique Xiongan, en Chine, censée incarner une nouvelle ère (voir ci-dessus). Des initiatives, qui tirent parti de la technologie de l'IoT pour la création de villes intelligentes, sont mises en œuvre dans toutes les régions du monde, pièce après pièce, car les gouvernements sont de plus en plus friands de tous ces moyens testés et éprouvés qui permettent d'augmenter l'efficacité et de réduire les coûts.

« Les innovations en matière d'infrastructure intelligente pourraient faire économiser des millions aux villes. »
Ernst & Young

Dans les villes intelligentes, des capteurs installés au sein des infrastructures (publiques et privées) sont sauvegardés par le biais d'une puissance de traitement basée dans le cloud, dans un système de données intégré qui ressemble à une boucle de rétroaction constante, permettant de titrer les décisions et stratégies en temps réel. Parmi les applications courantes, on retrouve les compteurs d'eau intelligents, le contrôle de la circulation, les transports publics, l'efficacité énergétique dans les bâtiments et les initiatives relatives à la sécurité publique.

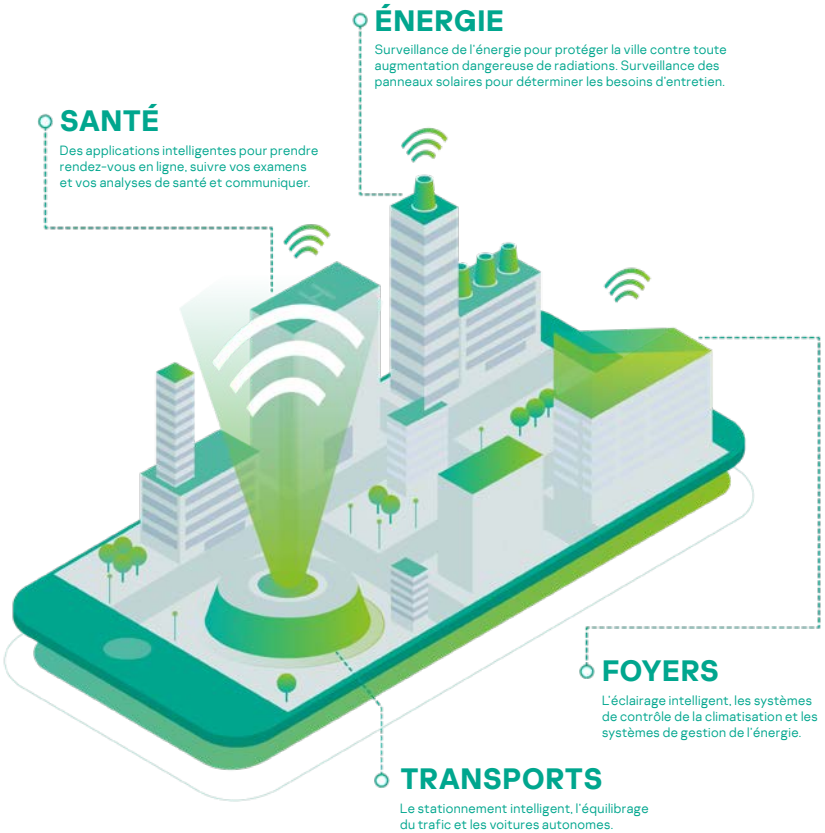
Dans la plupart des cas, si ce n'est dans tous les cas, les gouvernements se tournent encore une fois vers les fournisseurs de téléphonie mobile privés pour mettre en œuvre la technologie de l'IoT, qui est essentielle pour mener à bien la révolution des villes intelligentes. Voici un excellent exemple : la collaboration entre Nordkapp, une startup finlandaise spécialisée dans les technologies de la santé, et Urbanscale, entreprise spécialisée dans la pratique de conception des réseaux urbains basée à New York, qui a permis la création d'Urbanflow, un projet visant à faire de Helsinki une ville plus accessible et agréable à la fois pour les habitants et pour les visiteurs, grâce à l'installation d'un service interactif.

327 milliards de dollars

« La dépense des villes intelligentes consacrée à la technologie au cours des six prochaines années devrait croître selon un taux de croissance annuel composé de 22,7 %, pour atteindre 327 milliards de dollars d'ici 2050, en partant de 96 milliards de dollars en 2019. »
Frost & Sullivan

Urbanflow comprend l'installation d'écrans interactifs dans toute la ville, qui proposent des cartes à facettes multiples enrichies par les données de la ville intelligente, et offrent des conseils en matière de navigation et de transport, ainsi que des données sur la pollution ambiante, la densité du trafic et d'autres informations utiles. Selon les fondateurs, grâce à Urbanflow, « toute la ville devient plus transparente et plus réactive aux besoins de ses citoyens », et « les fonctionnaires et les gouvernements municipaux peuvent disposer d'une toute nouvelle façon de communiquer avec les citoyens et les visiteurs, car une ville qui communique davantage avec ses habitants travaille mieux et se sent mieux. »

Étant donné que l'ONU prévoit que 68 % de la population mondiale vivra dans des villes d'ici 2050, le boom des villes intelligentes ne pourra que s'accélérer, car les gouvernements tentent de relever le défi qui consiste à organiser et à protéger ces immenses populations (en pleine croissance).



Villes intelligentes – Pleins feux sur la menace – L'éternel paradoxe des nouvelles technologies

Chaque fois qu'une nouvelle technologie prometteuse entre en scène, les utilisateurs bienveillants ne sont pas les seuls à s'en emparer. Cette tension est une extension du paradoxe du double usage. 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. L'accueil de toutes les nouvelles technologies en réseau de l'IoT et des villes intelligentes doit toujours être modéré, en gardant à l'esprit que les cybercriminels se feront également un plaisir de faire usage de ces innovations.

Le talon d'Achille de l'IoT est la multiplication des interfaces d'attaque qui accompagne naturellement tout système en réseau hyper connecté. Pour répondre à ces préoccupations, le National Cyber Security Centre au Royaume-Uni a publié en mai 2021 un ensemble de principes sur la façon de concevoir et de gérer les villes intelligentes pour les rendre résistantes aux cyberattaques.

Kitchin et Dodge ont identifié cinq vulnérabilités clés dont les cybercriminels cherchent à tirer profit en lançant des attaques contre les villes intelligentes. Ce sont ces points précis auxquels les gouvernements doivent prêter une attention particulière s'ils veulent éviter le désastre :

1. La sécurité des logiciels et le chiffrement des données trop faibles.
2. L'utilisation de systèmes hérités non sécurisés et la maintenance continue médiocre.
3. Les nombreuses interdépendances et les surfaces d'attaque vastes et complexes.
4. Le potentiel des effets en cascade.
5. L'erreur humaine et les actes répréhensibles délibérés des (anciens) salariés mécontents.

Tendance n° 7 : L'automatisation et l'analyse avec l'IA/le ML – avantages pour le gouvernement

Le Machine Learning permet aux ordinateurs d'automatiser le raisonnement inductif en ce qui concerne les données, en se fondant sur des inférences de résultats et d'événements tirés d'occurrences passées. Il ne s'agit pas d'une technologie autonome, mais d'un composant qui peut être inséré dans un système existant, afin de stimuler la puissance et l'efficacité de traitement.

Chez Kaspersky, nous utilisons le Machine Learning depuis de nombreuses années, et nous mettons en œuvre des ensembles d'arborescences décisionnelles, le hachage sensible à la localisation, et la mise en cluster de flux entrants afin de garantir la protection des terminaux et d'autres ressources de données. Découvrez-en plus ici.

« L'automatisation peut permettre aux gouvernements de fournir un niveau exceptionnel d'expérience client, stimulé par les innovations qui sont aussi sensibles aux personnes qu'à la technologie. »

« Nous avons identifié trois types d'avantages. Le plus évident de ceux-ci est peut-être la fiabilité et la simplicité… Une deuxième manière dont l'automatisation peut renforcer l'expérience client dans les services gouvernementaux consiste à donner aux fonctionnaires la possibilité de proposer des prestations de services plus complexes et attentionnées… Une troisième amélioration de l'expérience client pouvant être offerte par l'automatisation des services gouvernementaux est la prestation de services personnalisée, incluant un service basé sur l'IA.
McKinsey

Forbes est arrivé à la conclusion que « 2021 est l'année où l'IA sera intégrée aux appareils existants et fera de certaines fonctionnalités plus rapides et plus précises une norme ». Il est clair qu'aujourd'hui nous y sommes presque, car l'IA et le ML sont déjà largement utilisés dans le cadre de nombreux projets de bureaux, d'usines et d'infrastructures.

Gartner a estimé que 60 % des investissements gouvernementaux en matière d'IA et d'analyse des données affecteront directement les processus de prise de décision et les résultats. L'automatisation va réduire les temps de traitement et augmenter la productivité en automatisant le travail manuel. IBM a constaté que « plus de 95 % de tous les incidents ayant fait l'objet d'une enquête avaient fait apparaître « l'erreur humaine comme un facteur contributif ». Il est clair que l'un des principaux avantages de l'IA et du ML réside dans la capacité à exclure complètement l'erreur humaine de l'équation des risques cybernétiques. Un algorithme codé de façon appropriée ne laissera pas entrer n'importe qui.

En tant que composants de la technologie, les applications de l'IA et du ML pouvant être mises en œuvre par le gouvernement sont multiples et variées, et comprennent les interactions citoyen-client (chatbots), les départements RH, la fiscalité, l'audit, la prévention de la fraude et la sécurité. L'analyse automatisée peut sensiblement réduire les risques, si ces risques sont d'ordre financier, médical, sécuritaire, ou autre. Quelle que soit la mise en œuvre, l'objectif final est d'accroître la précision, de réduire les coûts et de réduire les heures de main-d'œuvre humaine.

En 2021, les gouvernements vont globalement commencer à profiter des avantages de l'IA et du ML, en introduisant des services innovants et améliorés, en augmentant la productivité, en économisant sur les coûts et en améliorant le processus de décision axé sur les données. Les applications principales des gouvernements se situent dans l'éducation, la sécurité nationale, les transports, la santé et le bien-être social.

Par exemple, le gouvernement australien a déjà lancé une initiative expérimentale en matière d'IA qui emploie des caméras haute définition et la technologie d'IA pour identifier les conducteurs qui sont distraits, particulièrement par l'utilisation illégale de leur téléphone portable lorsqu'ils sont au volant.

IA/ML – Pleins feux sur la menace – Que se passe-t-il lorsque les humains ont le dos tourné ?

Tous les amateurs de cinéma connaîtront la crainte que les machines prennent le dessus. Lorsque les êtres humains sont retirés de l'équation, comment pouvons-nous garantir que les systèmes restent humains ?

L'UE cherche à se tourner vers l'élaboration d'un ensemble de politiques modérées et réfléchies relatives aux technologies cognitives, tout en garantissant d'une part que les investissements soient réalisés, et d'autre part que l'intérêt public soit toujours en première ligne de toute technologie. En fait, l'UE cite le besoin de faire confiance au ML/à l'IA comme l'une des raisons qui se cachent derrière l'adoption du RGPD.

En théorie, les technologies cognitives pourraient être vulnérables à une forme particulière de cyberattaque qui pourrait s'appeler le « faux apprentissage » : les pirates alimentent de fausses données dans un système pour lui faire apprendre des « faits » erronés qui fausseront les résultats de sa mission. À ce jour, on comptabilise très peu d'attaques semblables, d'une part car l'industrie de la cybersécurité s'est elle-même montrée très encline à l'utilisation de l'IA, et d'autre part, car la technologie est encore récente, ce qui laisse aux pirates moins de temps pour s'adapter.

Cependant, il est clair que des mises en œuvre à grande échelle de l'AI et du Machine Learning offrent aux cybercriminels de nouvelles possibilités d'attaques contre le « Big Data ». L'IA est utilisée dans les attaques par des ransomwares, des programmes malveillants et par phishing. Les algorithmes de l'IA sont utilisés pour créer des vidéos, de l'audio et des images deepfake créant de possibles désordres dans les sociétés, de sorte que la frontière entre la réalité et la fraude devient encore plus floue.

Un autre problème réside dans l'introduction par les gouvernements d'une technologie IA sans protections suffisantes. En juin 2021, le rapport de l'U.S. Government Accountability Office a mis en relief le fait que les agences fédérales utilisant la reconnaissance faciale faisant appel l'IA n'avaient pratiquement aucune responsabilité par rapport aux données collectées.

Tendance n° 8 : Défis réglementaires

Au vu de toutes les technologies que nous avons étudiées dans le présent document et du très grand nombre de clients-citoyens impliqués, la pression n'a jamais été aussi forte pour les gouvernements quant à la mise en œuvre d'une règlementation appropriée. Les gouvernements doivent trouver l'équilibre entre encourager les entreprises à innover (afin que leur pays ne soit pas en retard) et mettre en œuvre des règlements pour assurer la sécurité et la satisfaction de leurs citoyens.

Une autre difficulté résulte du fait immuable qu'est la mondialisation et de l'ampleur de la révolution numérique. Que se passe-t-il lorsque les citoyens d'une juridiction interagissent avec les services fournis par une autre juridiction, peut-être moins réglementée ? Comment les gouvernements peuvent-ils contrôler cela ?

Les règlementations à l'échelle mondiale sont beaucoup trop nombreuses pour pouvoir les résumer ici. L'Union internationale des télécommunications des Nations unies s'efforce de promouvoir des réglementations adaptées pour ses 193 états membres et d'établir des normes internationales pour une société mondialisée plus sûre. La base de données réglementaire de l'ITU (22e édition, janvier 2019) est la référence canonique pour les milliers de normes appliquées de différentes façons par les pays du monde entier.

7,8 milliards

« Le nombre d'appareils connectés à Internet devrait passer de 31 milliards en 2020 à 35 milliards en 2021, et à 75 milliards en 2025. »
Securitytoday.com

Les défis de la règlementation - Pleins feux sur la menace - Le « problème de rythme »

Les analystes de Deloitte affirment que les organismes de réglementation peuvent avoir du mal à suivre le rythme de l'innovation technologique, ce qu'ils appellent le « problème de rythme » :

Bakul Patel, directeur associé du centre américain pour la santé numérique de la Food and Drug Administration (FDA), affirme « qu'il existe un décalage entre la vitesse, le développement itératif et la nature connectée omniprésente des technologies relatives à la santé numérique et les structures et processus réglementaires existants. L'approche réglementaire actuelle n'est pas correctement adaptée pour soutenir le rythme rapide de développement ».

Les risques pour les gouvernements sont doubles. Ne pas réussir à suivre le rythme des nouvelles technologies pourrait entraîner des risques de sécurité plus importants et un décalage critique entre la sophistication technique des services numériques du gouvernement et l'ingéniosité des pirates et cybercriminels. Dans le même temps, recourir à des réglementations laxistes pour accélérer le développement et l'adoption de nouvelles technologies pourrait s'avérer fatal.

Résumé

Les organisations gouvernementales portent globalement une lourde responsabilité pour répondre aux exigences essentielles en matière de sécurité nationale, mais aussi pour sécuriser leurs opérations (et leurs citoyens). Bien évidemment, toutes les industries ont une responsabilité en matière de protection des référentiels de données sensibles qu'elles accumulent, mais pour les gouvernements, les enjeux sont beaucoup plus importants. Chaque avance technologique adoptée par les organisations gouvernementales est susceptible d'augmenter les cybermenaces inattendues et nouvelles. La compréhension de ce à quoi pourraient ressembler ces menaces est essentielle. Compte tenu des grandes quantités de données personnelles à caractère très sensible des citoyens et de la masse de capital intellectuel politique tout aussi importante, faire le bon choix en matière de cybersécurité est crucial. Sans cybersécurité, les gouvernements peuvent ne pas se sentir libres d'exploiter les nouvelles technologies prometteuses dont ils ont besoin pour construire les villes intelligentes et explorer les nombreuses autres innovations sociétales connectées qui deviendront peu à peu la norme dans les pays du monde entier.

Le fait d'avoir un partenaire de sécurité intervenant réellement sur le plan mondial et disposant d'une expérience appropriée dans toutes les technologies émergentes pertinentes est une aide essentielle, accompagnant les organisations dans l'exploration de l'avenir. Malgré un environnement actuel extrêmement exigeant et versatile, Kaspersky est la solution idéale pour protéger vos données et celles des citoyens. Il vous suffit de choisir dans le tableau ci-dessous la solution la plus adaptée.

Choisissez ce qui correspond le mieux pour protéger votre organisation

Kaspersky aide les organismes gouvernementaux à adopter globalement des stratégies éprouvées dans l'environnement actuel extrêmement exigeant et volatile. Nos solutions et services sur-mesure parfaitement conçus, reposant sur une veille stratégique leader du marché, protègent les données et la continuité de l'activité 24h/24, 7j/7 contre les menaces avancées et les attaques ciblées, ce qui permet d'atténuer les risques, de détecter précocement les attaques, de traiter de manière efficace les attaques en direct et de renforcer la protection dans le futur.

Approche de la cybersécurité par étapes pour une protection à l'épreuve du temps

Notre approche par étapes en matière de cybersécurité est conçue pour clarifier le niveau de sécurité et les solutions spécifiques les mieux adaptés à votre organisation. Les structures fournissent un ensemble complet de mesures de protection contre les menaces faciles à gérer, se coordonnant en toute transparence entre elles, afin de répondre aux besoins de chaque organisation individuelle et d'offrir une feuille de route de la cybersécurité assurant en douceur la transition d'un niveau de maturité de sécurité informatique vers un autre le moment venu.

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 vagues, avant de mettre en œuvre de manière fluide notre troisième version...

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 organisation, assurant la sécurité et la protection des citoyens et 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 Lab qui effectuent des vérifications parallèles pour optimiser la défense en fonction de la nature de chaque attaque DDoS.
 **Kaspersky Threat Attribution Engine**	Un outil d'analyse des programmes malveillants déployé sur votre réseau, « sur site », dans votre cloud privé ou public, qui intègre 22 années de la base de données de Kaspersky d'échantillons de programmes malveillants APT. Délivre une analyse automatisée de la « génétique » et des « génotypes » des logiciels malveillants pour les similarités dans le code avec les échantillons ATP étudiés précédemment pour faire rapidement le lien entre les nouvelles attaques et les logiciels, acteurs, campagnes ATP connus et les attaques ciblées précédentes.
 **Kaspersky Research Sandbox**	Émule des systèmes spécifiques à l'entreprise dans un environnement isolé, en effectuant une analyse automatisée comportementale des logiciels malveillants, et permettant une détonation et une détection en toute sécurité des menaces avancées et encore inédites.

...Ou faites-le vous-même !

Construisez votre propre solution de sécurité nationale.

Prenez le contrôle total de votre cyberdéfense en concevant des produits de sécurité basés sur les technologies personnalisées de Kaspersky, grâce au programme Kaspersky Technology Alliances. Nous offrons plusieurs kits de développement logiciel (SDK) et flux de données sur les menaces, pour vous permettre de développer votre propre solution sur mesure, 100 % adaptée à vos caractéristiques uniques.

Votre solution personnalisée offre de multiples avantages uniques, notamment :

- Effectuez le déploiement où et quand vous en avez le plus besoin, pour répondre parfaitement à vos exigences uniques.
- Choisissez de mettre en œuvre des solutions personnalisées en tant que suites de sécurité logicielles « classiques », ou sur une plate-forme matérielle (passerelle Web sécurisée ou appareil UTM).
- Mettez en œuvre une protection multi-niveaux, par exemple, en déployant des portails Web sécurisés Kaspersky aux points d'entrée du réseau.
- Éliminez la complexité avec le texte brut ultra-net de Threat Data Feeds.
- Maintenez un contrôle et une souveraineté totale sur vos données grâce à une solution personnalisée développée par des experts et dotée de toutes les autorisations de sécurité nécessaires dans votre propre pays.
- Configurez des solutions de protection dans le cloud pour contourner les risques inhérents au déploiement de solutions tierces.

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