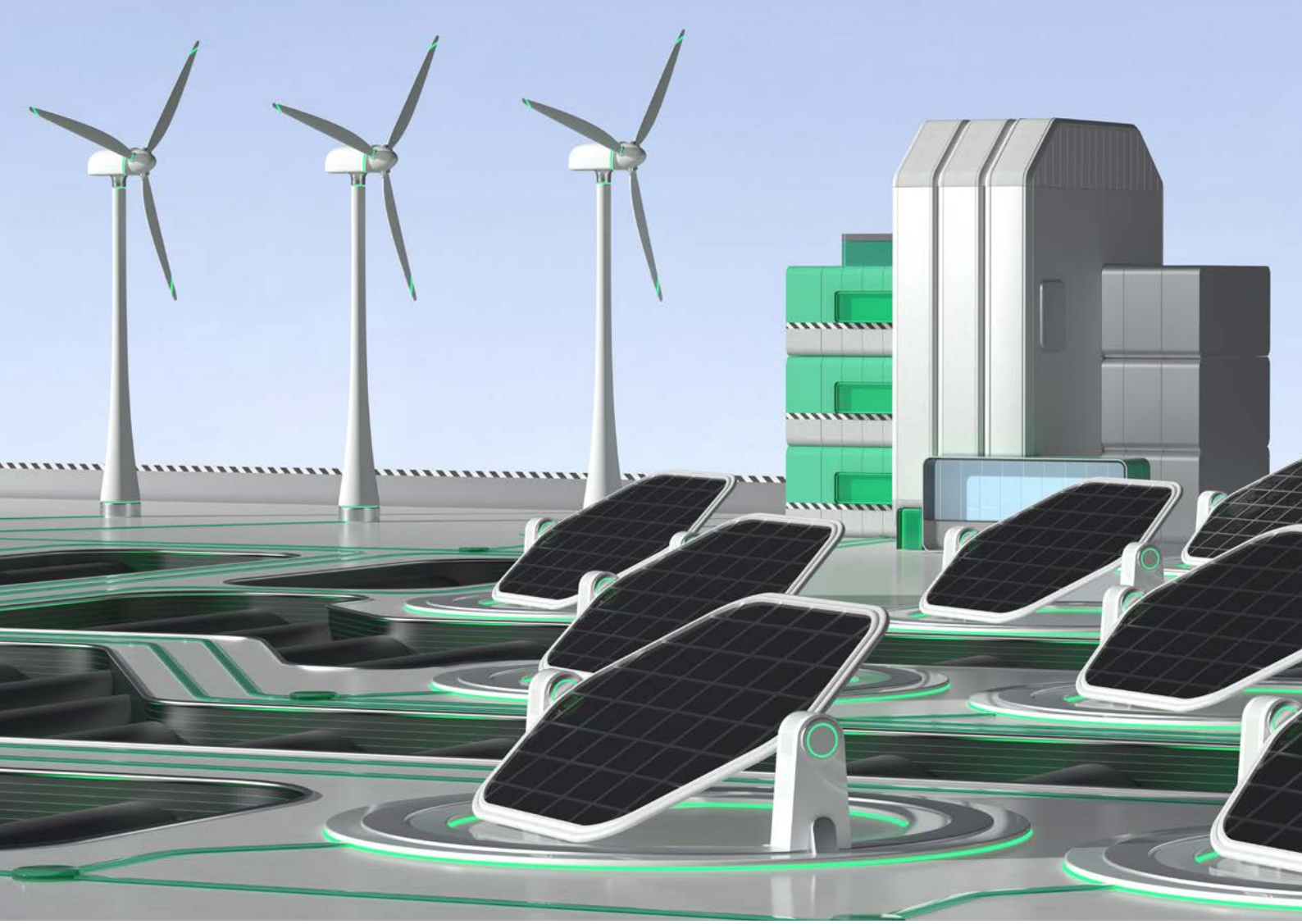

Construire un avenir plus sûr dans les services publics

Introduction

La production du secteur des services publics (services de production de chaleur, d'énergie, d'éclairage, d'eau et d'assainissement) circule dans les veines de chaque secteur d'activité de la planète comme une énergie sans laquelle rien ne fonctionnerait. Toutefois, en 2021, les incidents de cybersécurité ont démontré que le secteur des services publics est une cible de plus en plus tentante pour la cybercriminalité et les actes de cyberguerre.

Le secteur des services publics est soumis à des évolutions rapides ne montrant aucun signe de ralentissement. Venant s'ajouter à la transformation numérique déstabilisante, le secteur des services publics subit une pression particulière pour transformer les ressources qu'il produit. La décarbonisation, les énergies renouvelables, l'efficacité énergétique et la décentralisation sont à l'ordre du jour, et seule la technologie la plus intelligente et innovante peut répondre à l'appel. À cela s'ajoutent les nombreuses exigences réglementaires avec lesquelles les opérateurs de services publics doivent jongler dans un marché de plus en plus mondialisé.

Dans ce document, nous examinons les principales tendances qui transforment à l'heure actuelle le secteur des services publics et découvrons les défis et les risques qu'elles impliquent. Notre vision est celle d'un monde où les opérateurs de services publics sont libres d'optimiser l'adoption d'une technologie intelligente qui améliore l'efficacité, sans crainte des ravages que peuvent causer des cyberacteurs malveillants.

Intelligence artificielle

Analyse des données

Décarbonisation

Ressources énergétiques distribuées

Aspects réglementaires

Tendance n° 1 : Intelligence artificielle (IA)

L'intelligence artificielle bouleverse les conditions d'approvisionnement constant (et efficace) du secteur dont dépendent la réputation et les contrats des fournisseurs. Ces technologies ont été rendues possibles par la mise à disposition d'une puissance de calcul massive dans le Cloud, la prolifération du big data et la sophistication croissante de l'expertise algorithmique.

Côté production, les opérateurs de services publics exploitent l'IA pour prévoir les charges, optimiser les rendements, analyser la consommation, prévoir la demande, prévenir le vol ou les interférences malveillantes et effectuer des tâches de maintenance et de réparation prophylactiques. Les opérateurs de services publics cherchent également à mettre en œuvre ces technologies perturbatrices dans d'autres fonctions de leur activité, notamment les ventes, l'exploitation, les services clientèle, la gestion des installations, l'approvisionnement et l'informatique.

Applications d'IA pour les services publics :

- Remodelage de l'expérience client ;
- Simplification des tâches de maintenance ;
- Anticipation des charges énergétiques ;
- Intégration des ressources énergétiques distribuées ;
- Optimisation de la génération de la transmission et de la distribution.

Les applications courantes de l'IA incluent l'analyse des phénomènes météorologiques historiques afin de calculer les conséquences à prévoir sur le réseau et le comportement des clients, et de mettre en place des équipements et les effectifs pour minimiser à l'avenir les indisponibilités liées à la météorologie. Les services publics expérimentent des drones sans pilote couplés à l'IA pour collecter des données et des images des équipements de terrain et identifier les risques de défaillance de manière beaucoup plus précise que par des inspections manuelles. Les opérateurs de services publics commencent également tout juste à réaliser le rôle potentiel de l'IA pour la coordination des ressources d'énergie distribuée telles que l'éolien, les batteries et le solaire. Mais ce n'est que le début. Les services publics peuvent s'appuyer sur d'énormes quantités de précieuses données clients et disposent de la capacité d'utiliser l'IA pour améliorer tous les aspects de leur engagement à l'égard des clients et transformer leur modèle d'activité.

« Une centrale électrique dont le fonctionnement reposera sur l'« intelligence artificielle » est sur le point de démarrer en Afrique occidentale. La coentreprise entre Xcell Security House and Finance basée en Suisse et Beyond Limits basé aux États-Unis intégrera les renseignements et la connaissance dans l'exploitation, ce qui va créer de meilleurs rendements, une productivité importante et un accroissement des protections environnementales ».
Forbes

L'IA facilite également l'automatisation robotisée des processus. L'automatisation robotisée des processus est flexible, évolutive et peut être adaptée aux exigences spécifiques de chaque service public. Elle réduit les coûts et rend possibles les mises à niveau des services. Elle contribue également à résoudre les pénuries de personnel, à la gestion des tâches simples pour les clients, telles que les relevés de compteurs automatiques, et à répondre à certains aspects de contrôle et de conformité réglementaires. Les services publics transfèrent rapidement les processus routiniers basés sur des règles systématiques vers l'automatisation robotisée des processus.

Dans l'immense majorité des cas, les opérateurs de services publics se tournent vers des tiers pour fournir les technologies innovantes dont ils ont besoin. Ces tiers comprennent des grandes sociétés expérimentées (comme General Electric), ainsi que des nouveaux arrivants (comme Open Energi). Examinons ces deux exemples :

Digital Wind Farm de General Electric utilise des données collectées en permanence sur la météo, les messages de composants, les rapports de service et les performances de modèles similaires pour élaborer un modèle prédictif qui permet aux clients d'améliorer les performances, de réduire les risques et de diminuer les coûts. Selon les propres termes de General Electric, « Digital Wind Farm est un système d'énergie éolienne de bout en bout qui exploite les données, les analyses et les applications logicielles en lien avec nos solutions matérielles et de services pour améliorer l'efficacité, la cybersécurité, la fiabilité et la portabilité de vos ressources tout au long de leur durée de vie. »

Open Energi « gère l'énergie distribuée afin de réduire radicalement les coûts d'électricité et de fournir une capacité flexible pour permettre un système d'énergie 100 % renouvelable ». La plate-forme Dynamic Demand d'Open Energi exploite l'IA pour maximiser l'utilisation des ressources, réduire les coûts et optimiser les performances. En juillet 2021, British Petroleum a acquis Open Energi et prévoit de développer son modèle d'activité sur le plan mondial.

Pleins feux sur la menace : l'IA est comme l'énergie nucléaire, « toutes deux prometteuses et dangereuses » (Bill Gates)

Les risques liés à l'IA, quelle que soit l'application : si le système de calcul derrière ces technologies est compromis, les systèmes qui en dépendent seront paralysés. Le problème pour le secteur des services publics est que les enjeux sont très importants. Sans électricité, eau, traitement des eaux usées, énergie et lumière, nos sociétés s'écrouleront. Cette précarité est renforcée par l'immaturité de ces technologies perturbatrices.

Le fait que la survie de populations entières (sans parler des entreprises) dépend de l'approvisionnement fiable en eau, en électricité et en gaz, fait des entreprises de services publics des cibles sensibles, non seulement pour le cybercrime, mais aussi pour la cyberguerre. Les acteurs étatiques savent que paralyser l'infrastructure des services publics

d'un pays depuis le confort d'un ordinateur malveillant pourrait faire plus de dégâts que n'importe quelle bombe. Une récente étude réalisée par Forrester a déterminé que 88 % des professionnels de la sécurité informatique s'attendent à ce que les attaques basées sur l'IA deviennent monnaie courante.

Le 6 mai 2021, un coup de semonce a été tiré lorsque Colonial Pipeline, le plus gros oléoduc pour le transport des hydrocarbures aux États-Unis a été arrêté à la suite d'une attaque de ransomware, attribuée à DarkSide, un groupe de pirates parlant le russe.

Tendance n° 2 : Analyse des données

Les données sont le carburant indispensable pour propulser l'avance numérique et technologique dans le secteur des services publics. Le secteur des services publics assiste à une révolution dans la collecte et l'analyse des données en temps réel et à un rythme de plus en plus rapide pour activer la planification proactive et la prise de décision. Les analyses avancées combinées à l'expérience humaine permettent aux services publics d'améliorer non seulement l'intérêt des clients, mais également de mieux gérer la chaîne logistique et le réseau, et de mettre à niveau les tâches de maintenance préventive et de planification des ressources. Afin de faciliter la collecte des données, les services publics installent et mettent à niveau des plates-formes d'analyse conçues pour faciliter l'utilisation et la traçabilité.

Les compteurs intelligents sont un domaine essentiel pour les réformes du secteur énergétique. La technologie transforme la manière de fonctionner des secteurs publics de l'électricité, du gaz et de l'eau pour atteindre de nouveaux objectifs ambitieux. L'installation mondiale de compteurs intelligents est en train de prendre de l'ampleur. Entre 2021 et 2025, plus de 572 millions de compteurs électriques intelligents vont être déployés en Chine, en Inde, au Japon et en Corée du Sud. Non seulement les compteurs intelligents séduisent les clients qui peuvent les utiliser pour réduire leurs factures énergétiques, mais la grande quantité de données qu'ils collectent permet également aux fournisseurs de gagner en efficacité côté demande, dans le cadre du réseau intelligent.

Le réseau intelligent est le pendant indispensable de la révolution des compteurs intelligents. On s'attend à ce que le marché du réseau mondial intelligent atteigne plus de 92 milliards de dollars d'ici 2026. La technologie de l'Internet des objets industriel est mise en œuvre dans toute la chaîne de valeur des services publics, de la production à la distribution et à la consommation. Selon un rapport de Global Market Insights, le marché de l'IoT est censé enregistrer des gains de plus de 20 % jusqu'en 2024. Les capteurs sur les équipements dans les centrales électriques, les installations hydroélectriques, les éoliennes et les panneaux solaires permettent des prises de décisions informées et parfois automatisées, ce qui donne aux opérateurs les moyens d'économiser sur les coûts, d'optimiser l'alimentation et de satisfaire la demande. La collecte de données fournit des informations précieuses pour l'amélioration de la sécurité et la résistance.

Le rapport d'Orbis Research sur le Big Data mondial sur le marché du secteur énergétique montre comment le Big Data a aidé les entreprises de services publics à suivre le modèle de consommation et les prévisions, pour modifier en conséquence l'approvisionnement en termes d'espace et de temps, ce qui se traduit par une utilisation efficace des ressources.

Pleins feux sur la menace : plus il y a d'appareils, plus il y a de problèmes (« ne vous y trompez pas, c'est une guerre »)

L'ajout d'appareils à un réseau revient à ajouter des fenêtres à un bâtiment. Plus il y a de fenêtres, plus le risque d'effractions (ou de failles de cybersécurité) augmente. Nous pouvons également ajouter, « plus il y a de données, plus il y a de problèmes » ; après tout, les données sont aux cybercriminels ce que les espèces sont aux cambrioleurs. Chaque outil de collecte des données qui s'ajoute au réseau offre une surface d'attaque importante à exploiter.

La décarbonisation augmente également de manière exponentielle le nombre de points d'intrusion. Par exemple, un plus grand nombre d'appareils, comme les bornes de recharge des véhicules électriques, sont connectés en permanence. Ce scénario est amplifié par le fait que la technologie des appareils évolue et qu'elle est potentiellement vulnérable aux cybermenaces nouvelles et inconnues. Les services publics, qui sécurisent un grand nombre de terminaux avec des ressources limitées, sont particulièrement exposés aux risques. Les solutions basées dans le Cloud donnent aux services publics la possibilité d'attirer les clients selon de nouvelles manières, mais apportent des problèmes de sécurité supplémentaires.

Les risques sont une évidence. On estime qu'environ 25 % des services d'électricité aux États-Unis ont été exposés à la violation massive de SolarWinds en 2020-2021. Les attaques de ransomwares sont en hausse de 116 % au cours des cinq premiers mois de 2021, selon l'évaluation de sécurité de Nozomi Networks.

La threat intelligence spécifique à l'industrie représente une composante essentielle de l'arsenal de cyberimmunité pour les entreprises de services publics. Seule des renseignements d'experts peuvent aider les opérateurs à garder une longueur d'avance par rapport aux menaces nouvelles et inconnues. La formation à la reprise après sinistre et à la réponse aux incidents est également essentielle. En outre, avec la prolifération des appareils et des applications, l'analyse du comportement et des anomalies joue un rôle crucial. Ces technologies de cybersécurité combinent l'analyse des données et l'IA pour « apprendre » le comportement des utilisateurs afin d'identifier et de bloquer immédiatement toute anomalie qui indiquerait la présence d'une menace, même si elle est encore inconnue.

Tendance n°3 : Décarbonisation

Un rapport de McKinsey fait référence à la décarbonisation du secteur comme « la prochaine frontière ». Bien sûr, la responsabilité de la décarbonisation de l'industrie ne relève pas exclusivement du secteur des services publics, mais il existe un lien naturel et les opérateurs de services publics ont un rôle central à jouer. Pour parvenir à la décarbonisation, le rapport de McKinsey recommande que « le lien entre le secteur industriel et le secteur énergétique soit considérablement renforcé, étant donné les interdépendances dans les deux sens. »

« Les parties partagent une vision à long terme de l'importance du développement et du transfert des technologies afin d'améliorer la résilience au changement climatique et de réduire les émissions de gaz à effet de serre. »
Article 10 de l'Accord de Paris

Les énergies renouvelables et les ressources énergétiques distribuées jouent un rôle essentiel dans le passage à la décarbonisation, mais c'est l'évolution de la technologie qui rend le changement climatique possible à l'échelle requise par notre planète. L'Accord de Paris, signé par 174 pays et l'UE, comprenait la mise en place d'un Mécanisme technologique, géré par la Convention-cadre des Nations Unies sur les changements climatiques (CCNUCC).

« Le secteur énergétique aux États-Unis est à mi-chemin du zéro émission nette, mais cela devient maintenant plus difficile. »

Bien que les énergies renouvelables représentent plus de 20 % de l'énergie générée en Europe et aux États-Unis, les objectifs sont ambitieux : 33 % d'ici 2025 et une augmentation nette de 95 % de la capacité énergétique mondiale pour 2050. Relever le défi de la décarbonisation nécessite de profondes modifications du fonctionnement des services publics, englobant la collaboration des parties prenantes, l'implication des clients et une considérable révolution technologique impliquant la numérisation, les capteurs, les appareils et la connectivité IoT, pour englober tous les aspects de nos vies, afin d'automatiser les initiatives d'amélioration de l'efficacité.

Trois technologies de développement sont considérées comme essentielles : les véhicules électriques pour supplanter le moteur à combustion, la diminution des coûts de génération et de stockage des énergies renouvelables et la réduction du coût de l'énergie produite localement afin d'éliminer la nécessité de transporter l'énergie. Tous ces éléments représentent des défis permanents pour l'industrie de l'énergie.

Pleins feux sur la menace : « hyper complexité + hyper connectivité + hyper volumes de données = hyper vulnérabilité » (UIT)

Le programme Habitat de l'ONU estime que les villes consomment environ 75 % de l'énergie primaire mondiale et émettent entre 50 et 60 % du total des gaz à effet de serre dans le monde, chiffre s'élevant à environ 80 % une fois que sont incluses les émissions indirectes générées par les habitants urbains. Les villes sont les principaux centres de mise en œuvre des nouvelles technologies que les entreprises de services publics adoptent de plus en plus pour répondre aux exigences et aux directives en matière de changement climatique.

Malheureusement, cela crée une cybertempête parfaite, que l'UIT décrit comme « hyper complexité + hyper connectivité + hyper volumes de données = hyper vulnérabilité ». Les entreprises de services publics se trouvent au cœur de cette tempête, naviguant sur d'innombrables appareils connectés et interconnectés, accumulant et traitant d'énormes ensembles de données, et sont confrontées à des réglementations de plus en plus strictes, qui évoluent à un rythme effrené.

L'UIT maintient que la cybersécurité, la protection des informations et la résilience des systèmes sont des problèmes politiques et de gouvernance. Le rapport de l'UIT, « Cybersécurité, protection des données et résilience des données dans les villes intelligentes », souligne « les effets potentiels des attaques malveillantes et des catastrophes sur les systèmes et infrastructures TIC stratégiques, y compris la privation de services essentiels pour les citoyens, allant des transports aux services publics (par ex., réseau intelligent, gestion de l'eau). »

Wired, magazine sur les technologies émergentes, prévoit ceci : « L'infrastructure toujours plus connectée permettra aux pirates informatiques d'abattre plus facilement des villes entières. Et les villes n'en font pas suffisamment pour se préparer… »

Un éditeur de sécurité dans le cloud allemand a identifié l'industrie énergétique comme la cible numéro un des cyberattaques en 2019, suscitant 16 % de toutes les attaques du monde entier. Un plus grand nombre de cyberattaques est prévu sur les chaînes d'approvisionnement concernant les batteries et le solaire. L'intégration massive des réseaux de distribution aux ressources énergétiques distribuées renouvelables devrait rendre les réseaux d'énergie plus vulnérables aux attaques. Dans un contexte d'hyper connectivité et d'interdépendances inévitables avec les systèmes gouvernementaux et municipaux, une forte sécurité périmétrique est absolument essentielle pour les entreprises de services publics.

Tendance n 4 : Ressources énergétiques distribuées

Allant de pair avec l'inévitable passage du carbone aux énergies renouvelables, et l'éventuelle élimination progressive de l'utilisation de combustibles fossiles, on assiste à la croissance de l'adoption par les consommateurs de sources d'énergie décentralisées, qui incluent naturellement les énergies renouvelables. Selon le New Energy Outlook 2019 de Bloomberg, « les décisions des consommateurs en matière d'énergie, telles que les batteries solaires sur les toits et les batteries 'derrière les compteurs', contribuent à façonner un réseau de plus en plus décentralisé dans le monde entier. »

Les ressources énergétiques distribuées impliquent une production d'énergie renouvelable au niveau local, qui contourne l'infrastructure nationale (voire régionale) existante et dépend donc largement du degré de dérégulation sur les marchés énergétiques respectifs. La décentralisation affecte la distribution ainsi que la production. Elle implique la mise en place d'un flux d'énergie bidirectionnel, fournissant le cadre par lequel les consommateurs ordinaires dont les maisons sont équipées, par exemple, de panneaux solaires, peuvent réinjecter toute énergie excédentaire dans le réseau, créant ainsi le nouveau rôle de « prosommateur ». Selon l'UE, cela est facilité par le réseau intelligent, qui « offre aux consommateurs qui produisent leur propre énergie la possibilité de répondre aux prix et de vendre tout excédant au réseau ».

La réunion du G7 de l'été 2021 a souligné l'importance des ressources énergétiques distribuées pour le traitement de la sécurité et des défis climatiques. Les ressources énergétiques distribuées facilitent la décarbonisation en permettant d'utiliser des énergies renouvelables, par exemple le solaire en remplacement des énergies fossiles (la puissance énergétique solaire mondiale a augmenté de 138,2 GW en ce qui concerne les installations en 2020, soit une progression de 18 % sur l'année) et les véhicules électriques qui remplacent le pétrole par l'électricité (les ventes mondiales de véhicules électriques ont augmenté de 41 % depuis 2019 et la part des ventes de véhicules électriques dans le monde a atteint un record de 4,6 % en 2020). À travers le monde, les solutions d'électrification se multiplient avec une fourniture en expansion rapide d'électricité renouvelable propre.

Bloomberg signale que « l'Australie et le Japon sont sur la bonne voie pour développer les deux systèmes électriques les plus décentralisés au monde ». Les États-Unis sont également en phase de décentralisation rapide. En septembre 2020, la Commission fédérale américaine de régulation de l'énergie a adopté l'Ordonnance 2222 ouvrant la porte à un marché de gros des ressources énergétiques distribuées.

96,7 milliards de dollars

« Le marché mondial des pompes à chaleur devrait passer de 60,4 milliards de dollars en 2021 à 96, 7 milliards d'ici 2026, avec un taux de croissance annuel de 9,9 % pour la période 2021-2026. »
Recherche et Marchés

Un autre avantage impressionnant des ressources énergétiques distribuées est que, en autorisant un type d'énergie efficace, des solutions de demande localisée utilisant des batteries et l'énergie solaire, elle offre une autonomisation (dans les deux sens du terme) aux populations des pays en développement, leur permettant d'accéder à l'énergie, et même de la produire (en tant que prosommateurs), au niveau local, en contournant toute défaillance dans les infrastructures nationales, régionales ou locales. La Banque mondiale calcule que 760 millions de personnes dans le monde n'ont toujours pas accès à l'électricité chez elles, par rapport à plus d'un milliard il y a 10 ans. « Électrification par le biais de solutions basées sur des énergies renouvelables décentralisées dans une intensification particulière. » Toutefois, la répartition entre les pays est également terriblement inégale. Seuls 6,7 % des habitants du Soudan du Sud, 8,4 % du Tchad, 11,1 % du Burundi, 11,2 % du Malawi et 14,3 % en République Centrafricaine ont accès à l'électricité.

Toutefois, les ressources énergétiques distribuées mettent en évidence la transition pour les sociétés de services publics traditionnels qui ont du mal à passer d'un modèle hérité du XXe siècle, constitué de gros générateurs centralisés et unidirectionnels connectés à des réseaux répondant à une demande stable et offrant une flexibilité de prix presque nulle. Le flux d'électricité bidirectionnel est un défi pouvant entraîner un débordement de la capacité des lignes électriques. Les appareils pour l'utilisation finale représentent une charge que l'on n'évalue encore pas précisément sur les réseaux. Les consommateurs allument tous les pompes à chaleur ou chargent tous les véhicules électriques en même temps, ce qui est susceptible de provoquer des pointes d'utilisation de l'alimentation impossibles à gérer. L'adaptation vers des flux bidirectionnels force les services publics à investir de manière conséquente pour modifier les réseaux.

Pleins feux sur la menace : les vulnérabilités des réseaux multinœuds complexes et automatisés

En général, le réseau électrique et l'infrastructure énergétique n'ont pas été conçus pour un flux bidirectionnel et certainement pas pour un flux entre des centres de production et de distribution de plus en plus petits. Au lieu du flux d'énergie unidirectionnel précis et étroitement contrôlé, du réseau au domicile (ou au bureau), la décentralisation crée un réseau interconnecté très complexe de nœuds d'extrémité, de contrôles avancés, de capteurs numériques, de logiciels et d'architectures réseau, avec ses propres vulnérabilités et ses problèmes potentiels de sécurité de connexion. Des réseaux aussi complexes s'appuient de plus en plus sur l'automatisation pour fonctionner, ce qui introduit d'autres vulnérabilités liées à l'utilisation de l'IA sur du matériel et des logiciels anciens.

Des centrales électriques virtuelles utilisant une infrastructure réseau intelligente pour connecter de petites quantités de ressources d'énergie dans un seul générateur permettent aux consommateurs de devenir des fournisseurs (prosommateurs) concentrant l'énergie en excès dans le réseau intelligent. Le modèle est séduisant et le secteur de l'énergie prévoit une augmentation massive des appareils numériques décentralisés canalisant l'alimentation en énergie distribuée vers des centrales électriques virtuelles. Cependant, la dépendance à l'égard d'une infrastructure réseau intelligente augmente clairement le risque de cybersécurité. Dans la mesure où des sources d'énergie très répandues et décentralisées sont alimentées par des terminaux reliés au réseau, le processus centralisé de centrale électrique virtuelle est vulnérable aux cybercriminels pouvant ouvrir une brèche dans le réseau via un terminal unique. Par exemple, un pirate pourrait théoriquement perturber un nombre important de batteries de stockage ou des chargeurs de véhicules électriques contre une rançon. L'augmentation des logiciels malveillants et des ransomwares ciblant les services d'infrastructures critiques n'est pas une coïncidence. La gestion des risques traditionnels n'est plus suffisante. Les ressources énergétiques distribuées affaiblissent clairement le contrôle et la surveillance que les services publics avaient auparavant sur les ressources en énergies stockées sur leurs réseaux.

La régulation de ce nouveau réseau est un défi compliqué, d'autant plus en raison de l'immaturité du secteur décentralisé. La configuration actuelle fournit peu de transparence aux services publics. La nécessité de disposer de normes et de réglementations universelles robustes est claire. Les questions concernant la responsabilité en matière de cybersécurité jouent également un rôle important.

Ces risques font des analyses de vulnérabilité et des dispositifs de réponse d'urgence spécifiques au secteur un impératif absolu pour les entreprises de services publics. Il vaut mieux prévenir que guérir et, si le pire se produit (peut-être en raison d'une vulnérabilité au sein d'une architecture distincte mais connectée), agir rapidement et de manière appropriée peut stopper la catastrophe.

Tendance n° 5 : Défis réglementaires

Étant donné la nature vitale des services publics, le secteur est l'un des plus réglementés de la planète ; il est soumis à un large éventail de réglementations, à l'échelle internationale, nationale, régionale et locale. Ces réglementations sont liées en grande partie au fait que les entreprises de services publics sont souvent des monopoles naturels, en particulier dans les pays où les sociétés privées ont remporté des appels d'offres pour la seule fourniture de services publics régionaux (ou même nationaux). Cependant, les réglementations de monopole ne sont que le début de l'histoire. Les opérateurs de services publics doivent suivre les réglementations couvrant un énorme éventail de préoccupations, notamment l'exploitation, la distribution, la maintenance, l'interconnexion, la facturation/la tarification, la concurrence, l'approvisionnement, la protection des données et, bien sûr, l'atténuation des changements climatiques. Toute non-conformité entraîne un accroissement du risque du système et des pénalités financières conséquentes.

Sans surprise, la cybersécurité et la résilience dans le secteur des services publics sont étroitement contrôlées. Par exemple, la Commission fédérale américaine de régulation de l'énergie exige que les opérateurs fournissent des réponses détaillées aux questions relatives à leurs risques de résilience unique, à la probabilité d'impact, à l'identification des menaces, à la planification des incidents, à l'atténuation des menaces, aux analyses des événements passés, aux équipements, ainsi qu'aux actifs d'ingénierie et physiques. Dans tous les cas, les risques de cybersécurité sont répertoriés en même temps que les événements naturels, tels que la sécheresse, depuis l'Ordonnance de janvier 2018 de la Commission.

« Comme les sociétés d'énergie adaptent leurs modèles d'activité pour s'adapter à l'environnement dynamique du marché actuel, leurs fonctions juridiques et de conformité doivent également s'adapter. Les moyens numériques des processus de surveillance de la réglementation et de la conformité de l'énergie peuvent aider à résoudre ces problèmes à l'aide d'une solution unifiée. »
Deloitte

En 2021, des gouvernements du monde entier ont recherché de manière urgente des mesures pour faire appliquer des mesures de cyber-résilience dans les sociétés de services publics essentielles. Le 6 mai 2021, l'attaque portée contre Colonial Pipeline, apparemment par un groupe de cybercriminels basés en Russie, a mis à l'arrêt près de 9 000 km de pipeline, transportant 45 % de l'alimentation en carburant de la côte est des États-Unis. Un état d'urgence a été déclaré dans quatre États aux États-Unis. Pour les régulateurs, cela a été un coup de semonce. Était-ce un manquement à la conformité ? Était-ce une attaque évitable ? Le département de la Sécurité intérieure a rapidement présenté des exigences en matière de sécurité plus strictes afin « de mieux identifier, offrir une protection et répondre aux menaces visant les sociétés critiques dans le secteur des pipelines ».

« Les PDG signalent une pression réglementaire sur l'environnement, le social et les questions de gouvernance dans l'enquête. »
KPMG

À l'heure actuelle, les États-Unis élaborent un projet de loi (remplaçant la loi de 2018) pour intensifier les exigences en matière de cybersécurité pour les fournisseurs d'électricité et d'énergie. Adoptant une approche différente, la Commission fédérale américaine de régulation de l'énergie propose une modification de la loi afin d'offrir des mesures incitatives de subventions fédérales (report du recouvrement des coûts) pour les sociétés d'électricité mettant en œuvre des mesures de cybersécurité dépassant les normes des réglementations actuelles.

De plus, les réglementations introduites récemment ne se rapportant pas à la cybersécurité ont néanmoins eu une incidence considérable sur les demandes en matière de cybersécurité. Un bon exemple de cela est donné par l'Ordonnance 2222 de la Commission fédérale américaine de régulation de l'énergie, transformant potentiellement le secteur de l'énergie en libéralisant le marché pour les fournisseurs de vente en gros de ressources énergétiques distribuées.

Pour conclure, la cybervulnérabilité des ressources en énergie intégrées numériquement doit encore être complètement testée. **Une enquête KPMG a déterminé que 48 % des PDG de services publics pensaient que la question d'être victime d'une cyberattaque ne posait pas en termes de « si », mais de « quand ».**

Pleins feux sur la menace : le non-respect des réglementations entraîne des conséquences fatales

Le non-respect des réglementations peut entraîner deux conséquences fatales. Tout d'abord, lorsque les réglementations fournissent un cadre directeur des normes de cybersécurité, la non-conformité peut entraîner une intrusion dévastatrice. Deuxièmement, côté gouvernance, le non-respect de ces règles peut entraîner la perte de licence. Les deux conséquences peuvent mettre un opérateur de services publics à genoux.

La succession de cyberattaques en 2021 visant les services publics dans le monde entier montre l'ampleur du problème. Prenons simplement deux exemples : en août 2021, une violation chez T-Mobile a conduit à un accès non autorisé aux informations personnelles de plus de 50 millions de personnes. En mai 2021, Volue, société norvégienne dans les technologies liées à l'énergie, a été touché par une attaque de ransomware la forçant à mettre à l'arrêt des installations essentielles d'eau et de traitement des eaux. Les retombées de violations telles que celles décrites ci-dessus signifient que les régulateurs sont contraints de continuer à renforcer leurs règles.

Les sanctions deviennent également plus dures. En 2019 Duke Energy a dû faire face à une amende de 10 millions de dollars imposée par les autorités fédérales après une exposition à d'importants risques de cybersécurité supposée avoir « représenté un risque sérieux » pour la sécurité et la fiabilité du réseau. La Loi sur la sécurité des données (septembre 2021), récemment signée en Chine, contient des dispositions réglementant la collecte, l'utilisation et la protection des données et des mesures sévères en cas de non-respect de ces dispositions, incluant une éventuelle suspension de l'activité.

Le non-respect des consignes n'est pas l'unique enjeu en matière de réglementations. Compte tenu des conséquences drastiques de la non-conformité, l'éventail vertigineux de réglementations affectant les opérateurs de services publics du monde entier est épuisant, en particulier pour les entreprises opérant sur plusieurs marchés. À cela s'ajoutent l'émergence constante de nouvelles technologies et les incertitudes quant aux nouvelles réglementations qui vont les régir.

Pour les sociétés de services publics, la préparation de l'adaptation aux réglementations passe également par l'adoption d'une cybersécurité adaptée à l'activité.

Résumé

Les cinq tendances exposées ci-dessus soulignent les énormes opportunités et les défis considérables avenir pour les entreprises de services publics. Il est impératif de ne pas simplement adopter les nouvelles technologies, il est également nécessaire de les sécuriser. Le développement d'une culture de la cyberimmunité va permettre aux entreprises de service public de bénéficier pleinement des avantages des hauts niveaux de connectivité et d'automatisation, en minimisant les impacts négatifs et en optimisant le retour sur investissement. Dans l'environnement actuel instable et en évolution rapide, Kaspersky a parfaitement conçu des solutions et des services sur mesure, reposant sur une veille stratégique leader du marché, afin de protéger les données et la continuité de l'activité 24h/24, 7j/7 contre les menaces avancées et les attaques ciblées, permettant d'atténuer les risques, de détecter précocement les attaques, de neutraliser les attaques en direct et de renforcer la protection dans le futur.

Kaspersky propose une **approche par étapes en matière de cybersécurité** conçue pour clarifier le niveau de sécurité et les solutions spécifiques les mieux adaptés à votre organisation. Ces étapes fournissent un ensemble 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 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 organisation, assurant la sécurité et la protection des citoyens et des clients.
Kaspersky Industrial CyberSecurity	KICS propose une approche holistique de la cybersécurité industrielle. En effet, la solution apporte une valeur ajoutée à n'importe quelle étape du processus de sécurité OT du client, des évaluations de la cybersécurité et de la formation aux technologies avancées et à la réponse aux incidents. Un écosystème de produits et de services intégrés permet de sécuriser les couches et composants technologiques de votre organisation (serveurs SCADA, interfaces HMI, postes de travail des ingénieurs, API, connexions réseau et ingénieurs), sans affecter la continuité des opérations ni la cohérence du processus industriel.
Kaspersky ICS Security Assessment	Pour les organisations préoccupées par les effets potentiels de la sécurité informatique et celle des technologies opérationnelles sur leur activité, Kaspersky propose une évaluation peu invasive de la cybersécurité avant l'installation. Il s'agit d'une première étape cruciale dans la mise en place de la sécurité, en tenant compte des besoins opérationnels. Cette évaluation peut également fournir de nombreuses informations relatives aux niveaux de cybersécurité, sans avoir à déployer d'autres technologies de protection.

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