convergint | utilities

Guide des bonnes pratiques, **2024 : Services publics**

Le secteur des services publics est confronté à **une escalade des risques physiques et cybernétiques à l'échelle nationale et mondiale**, ce qui impose de donner la priorité à la planification de la sécurité et à l'atténuation des procédures. L'équipe de Convergint dédiée aux services publics propose des stratégies de protection de haute sécurité, une mise en œuvre méthodique des programmes et des solutions complètes axées sur la sécurité et l'efficacité opérationnelle dans ce secteur. Grâce à sa connaissance approfondie des menaces qui pèsent sur l'industrie et des exigences en matière de conformité réglementaire, Convergint déploie une conception en couches pour garantir des performances et des fonctionnalités optimales.

Incidents et risques liés à la sécurité des services publics

Les sites d'opérations critiques présentent depuis longtemps un risque plus élevé pour les entreprises de services publics en raison de l'abondance de leurs actifs. Cependant, même les sites situés en aval se sont avérés nécessiter une protection et une atténuation des risques en raison de l'impact sur les entreprises et les communautés et de l'attention des médias nationaux qui accompagne un incident de sécurité.

En définitive, lorsqu'il s'agit d'évaluer les risques pour l'identification des actifs, la stratégie de protection et la planification de l'atténuation des risques, **il est essentiel de procéder à des évaluations sous-verticales** afin d'adapter les solutions aux actifs, aux réglementations, aux opérations commerciales et aux risques propres à un secteur d'activité spécifique.

Énergie nucléaire Services publics

L'énergie nucléaire est unique en ce sens qu'elle est intensément réglementée et hautement surveillée. Le raisonnement est clair. Une attaque réussie, qu'elle soit physique ou cybernétique, pourrait entraîner une libération incontrôlée de radioactivité ayant des conséquences importantes sur l'environnement et la santé, y compris la possibilité de décès à court et à long terme. La réglementation de la NRC (Nuclear Regulatory Commission) oblige les installations nucléaires à adopter une approche très normative de la sécurité afin de prévenir ou d'atténuer l'impact des incidents.

Les centrales nucléaires sont structurellement robustes et dissuadent les intrusions physiques de par leur conception. En outre, une approche rigoureuse de la protection physique par couches permet de la renforcer et comprend une force d'intervention humaine de type militaire. Les cybermenaces sont également traitées avec diligence et des protocoles exhaustifs mis en place pour gérer les risques, surveiller en permanence les événements et assurer un niveau de séparation avec les réseaux extérieurs. En fin de compte, ce sous-secteur est bien protégé, mais il fait l'objet de tests réguliers afin que les équipements et les protocoles soient continuellement réévalués pour garantir la protection et l'évolution des menaces.

Services d'électricité

Les compagnies d'électricité font appel à des agences d'intervention sur place ou à l'extérieur pour interdire l'accès aux mauvais acteurs potentiels de la menace. L'augmentation des risques pourrait entraîner une réévaluation de cette stratégie. Selon le ministère de l'énergie, 95 incidents d'origine humaine, y compris des actes de vandalisme et des cyber-événements, ont eu lieu au cours du premier semestre 2023, ce qui est supérieur à toute autre période de l'histoire.

Les attaques physiques restent la principale préoccupation de ce secteur. Le terrorisme national, en particulier, a semé le trouble dans les opérations sur le terrain et dans les communautés desservies par les stations de transport d'électricité. Le sud des États-Unis et le nord-ouest du Pacifique ont été particulièrement touchés depuis 2022, et la situation ne semble pas vouloir s'améliorer. Il est donc nécessaire de mettre en place une défense multicouche, de plus en plus adoptée par les sous-stations partout dans le monde.

Services de l'eau

Les menaces physiques se multiplient pour les compagnies des eaux, ce qui incite à se concentrer sur la protection des actifs les plus vulnérables aux attaques. Comme pour les installations électriques, une approche de défense en profondeur semble la plus prudente.

Malheureusement, les cybermenaces s'intensifient en même temps pour les services publics de l'eau. Les systèmes SCADA (Supervisory Control and Data Acquisition) sont essentiels à la surveillance opérationnelle et au contrôle des actifs clés pour maintenir le stockage propre et la distribution de l'eau aux consommateurs. Le maintien d'un contrôle et d'une observation stricts de ces systèmes, ainsi que de bonnes pratiques de cybersécurité sur les systèmes d'entreprise, est essentiel pour prévenir ou atténuer les cyberattaques. Cette nécessité est illustrée par la récente attaque d'un bâtiment de l'autorité de l'eau dans le comté rural d'Allegheny, en Pennsylvanie, apparemment perpétrée par un acteur d'un État-nation. L'autorité a pu se déconnecter et reprendre ses activités manuellement sans incident, mais le message a été reçu haut et fort : les efforts en matière de sécurité physique doivent être menés en parallèle avec les cyberprotections.

Énergies renouvelables : Énergie solaire, énergie éolienne et bioénergie

Bien qu'elles soient moins présentes dans le paysage des services publics, les énergies renouvelables ont une empreinte nationale croissante, ce qui signifie une augmentation des cibles et des risques potentiels. Les énergies renouvelables ont des actifs également vulnérables et ont été incitées à préparer des défenses physiques et cybernétiques. L'incendie d'une installation solaire à Las Vegas en 2023, à titre de "déclaration politique", n'est qu'une indication de ce qui pourrait arriver si ce sous-segment n'est pas préparé à répondre de manière appropriée aux menaces émergentes.

L'ensemble du secteur

La sécurité physique semble être la principale préoccupation des entreprises de services publics, et ce à juste titre. Le coût des intrusions fait la une de l'actualité nationale. Cela dit, **les cybermenaces sont de plus en plus importantes, car les systèmes obsolètes** et les réseaux ouverts offrent des possibilités d'accès évidentes. De plus, les acteurs des États-nations deviennent une menace de plus en plus importante, ce qui accroît le risque au-delà du simple piratage.

Il est essentiel que le secteur adopte une position ferme face à la cybercriminalité et investisse de manière appropriée pour dissuader et atténuer les menaces, tout en mettant en œuvre des stratégies globales de sécurité physique.

Le coût des attaques physiques ou cybernétiques

Il existe quatre catégories principales de pertes résultant d'une intrusion physique ou cybernétique pour les services publics :

1. **Réputation/confiance :** Même si les services publics n'invitent pas à des incidents, un manque apparent de préparation peut éroder la confiance des clients et nuire à leur réputation au sein de la communauté. Dans de nombreux cas, il n'est pas possible de passer à un concurrent, mais l'atteinte à la perception de la marque est tout de même significative pour une entreprise de services publics.
2. **Perte d'activité** : Les fermetures de services publics provoquées par des attaques physiques ou cybernétiques entraînent une perte commerciale tangible et une baisse mesurable des flux de revenus.
3. **Amendes :** Les amendes pour non-conformité physique imposées aux compagnies d'électricité peuvent dépasser 1 million de dollars par jour et par site et, compte tenu de la visibilité des compagnies d'électricité, les réglementations sont appliquées avec fermeté. Par la suite, il y a eu des cas documentés d'amendes de plus de 50 millions de dollars pour un seul site. D'autres sous-produits ont une structure d'amendes similaire.

Les sanctions dans le domaine de la cybernétique ne sont pas aussi codifiées, mais le non-respect de la réglementation reste une entreprise coûteuse compte tenu des sanctions.

4. La **vie humaine** : La perte de vies humaines est évidemment la conséquence la plus préoccupante d'une attaque physique. Les ramifications en aval sont clairement illustrées par un incident survenu en Caroline du Nord, où un actif de niveau inférieur a fait l'objet d'une attaque physique qui a eu des répercussions importantes sur une communauté de plus de 50 000 habitants. Des personnes ont perdu la vie en raison de l'impossibilité d'alimenter la climatisation pendant une vague de chaleur étouffante.

Risques futurs les plus menaçants

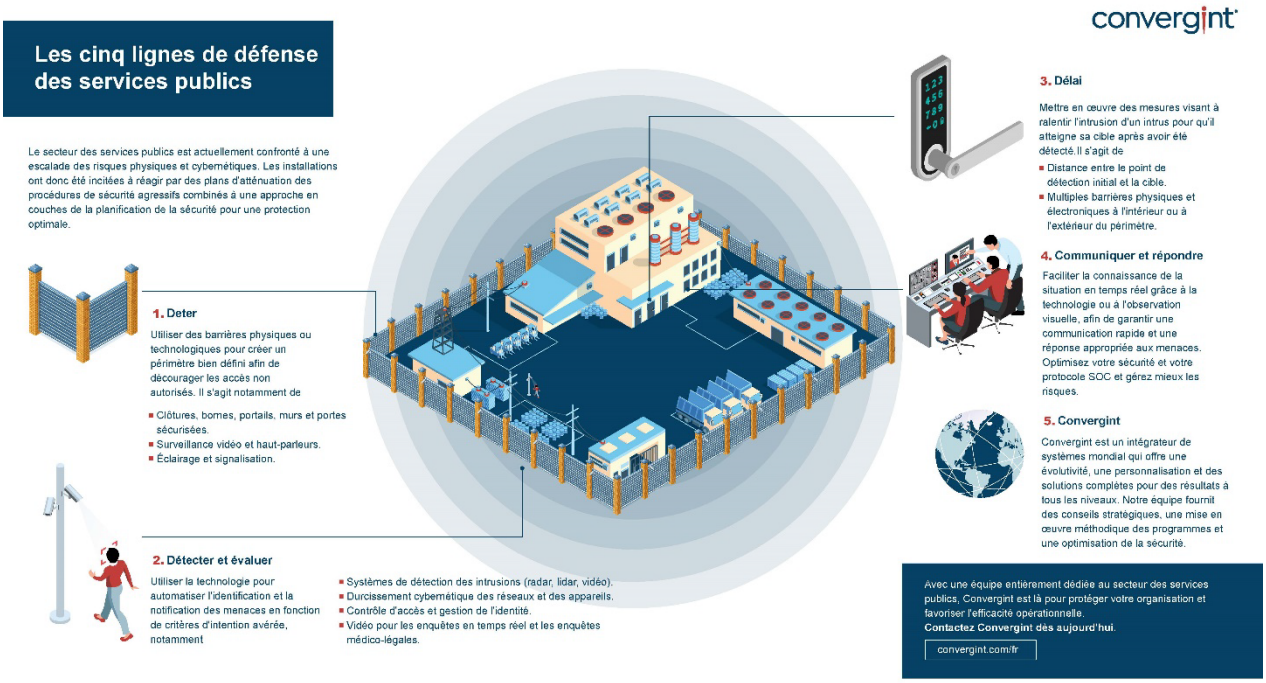
Les menaces physiques ont déjà eu des conséquences tangibles, et la réaction de plus en plus fréquente des services publics et des autorités de surveillance témoigne de la gravité de ce problème en constante évolution. Et comme les cybermenaces deviennent de plus en plus importantes, nous verrons probablement plus d'orientations, plus de restrictions et plus d'exigences en matière de protection. L'escalade rapide de la menace cybernétique imposera une réponse adaptée. Cela dit, la nature fluide de la cybermenace se traduit par une réponse technologique moins normative et plus proactive.

Dans l'ensemble, les réglementations en matière de sécurité et les recommandations relatives à l'atténuation des risques pour les services publics seront continuellement adaptées pour fournir des orientations adéquates face à l'augmentation du nombre d'attaques et de leur degré de sophistication. Cela concernera même les actifs précédemment considérés comme des actifs de niveau inférieur en termes de risque. En fin de compte, des mesures de sécurité minimales seront établies, et elles ne seront pas négociables.

Contre-mesures en matière de technologie de sécurité

Convergint recommande aux **entreprises de services publics de contrer les nouvelles menaces physiques et cybernétiques en adoptant une approche de défense en profondeur de la sécurité**. Tout système de sécurité peut être remis en question si l'on dispose de suffisamment de temps et d'argent ; l'état de préparation dépend donc de la complexité et d'une stratégie globale. Les événements actuels incitent les services publics à réagir en adoptant des plans d'atténuation des procédures agressifs et des solutions de sécurité à plusieurs niveaux pour :

- **Dissuader :** En utilisant des barrières physiques ou technologiques pour créer un périmètre bien défini afin de décourager les accès non autorisés.
- **Détecter et évaluer** : En utilisant la technologie pour automatiser l'identification et la notification des menaces à l'aide de critères définis pour les intentions démontrées.
- **Retard.** La mise en œuvre de mesures visant à ralentir l'intrusion d'un intrus pour lui permettre d'atteindre les actifs ciblés devrait permettre de surmonter la dissuasion.
- **Communiquer et réagir :** En tirant parti de la connaissance en temps réel grâce à la technologie et à l'observation visuelle pour assurer une communication rapide et une réponse appropriée aux menaces.



En fin de compte, les **mesures de défense en profondeur permettent d'arrêter les auteurs d'infractions ou de fournir des alertes et des notifications afin de coordonner une réponse**. Les infiltrations physiques ou cybernétiques qui parviennent à franchir une couche sont ralenties ou bloquées par la suivante, ce qui donne encore plus de temps pour atténuer ou prévenir les conséquences négatives pour un bien ou des opérations.

Améliorer l'efficacité du personnel de sécurité/réduire les coûts

Les services publics sont uniques en ce qui concerne les défis opérationnels qu'ils doivent relever. Nombre d'entre eux gèrent à la fois une infrastructure et une main-d'œuvre vieillissantes. Il est donc essentiel qu'ils améliorent l'efficacité du personnel de sécurité en augmentant la technologie de sécurité physique et électronique.

L'évolution des menaces rend nécessaire la réévaluation des processus politiques, des procédures, des stratégies de mise en œuvre, de la caractérisation des actifs et de la classification de chaque impact sur l'activité. En outre, les entités ont besoin d'un effet de levier croisé entre les dépenses de plusieurs départements pour chaque site, en assemblant les opérations de sécurité pour une sécurité optimale et des résultats commerciaux plus percutants. L'inclusion et la participation de toutes les unités opérationnelles dans un service public pour une stratégie de sécurité organisationnelle permet une plus grande sensibilisation à la sécurité, une meilleure appropriation et une plus grande responsabilité, ce qui **se traduit par un programme d'entreprise plus solide**.

Gestion du budget de la sécurité

Les budgets doivent tenir compte des conditions environnementales, des risques et du classement des actifs. En outre, nous recommandons :

1) **À court terme :** Les services publics cessent de se concentrer exclusivement sur la réduction des coûts du budget de la sécurité et cherchent plutôt à tirer un meilleur parti de ces dépenses. Il est plus intéressant de repenser la sécurité en termes d'avantages opérationnels et d'efficacité accrue. - Ajouter un graphique d'efficacité opérationnelle
2) **À long terme :** Les services publics envisagent de tirer parti de la "ville" desservie - gouvernement, soins de santé, écoles, etc. Demandez à vos clients/adjoints ce qu'ils font en matière de sécurité et comment l'intégration peut rendre tout le monde plus efficace. Évaluez s'il existe une dualité entre la sécurité et les opérations, voire la sûreté, que vous pourriez faciliter en combinant vos efforts. Pensez à la capacité proactive de tirer parti de la technologie de sécurité dans tous les secteurs verticaux, en particulier compte tenu du rythme des progrès. Les données bidirectionnelles et l'intégration permettraient aux services publics d'aller au-delà d'une approche cloisonnée de la sécurité, en améliorant l'efficacité d'une manière très efficiente. La sécurité pourrait devenir moins un centre de coût et plus un centre de profit avec des choses comme le partage des SOC. Il peut être difficile d'envisager cela à l'heure actuelle. Cela dit, à mesure que les cybermenaces sont gérées, il est inévitable de passer à un environnement basé sur le cloud, ce qui facilitera l'intégration.

Utiliser les technologies de sécurité pour améliorer la compétitivité des entreprises ou des marques

En fin de compte, l'utilisation d'une technologie de sécurité de pointe pour renforcer la sécurité et soutenir l'efficacité opérationnelle améliore les performances globales de l'entreprise et garantit une expérience optimale pour le client. En outre, la sécurité et la satisfaction des employés s'en trouvent renforcées.

Résumé des recommandations, 2024

Alors que l'empreinte physique et numérique du secteur des services publics continue de s'étendre et d'évoluer pour répondre à la demande croissante des consommateurs, il en va de même pour la protection des actifs existants et nouveaux. Les menaces qui pèsent sur le secteur sont permanentes, et la bataille constante entre le secteur des services publics, ses partenaires en matière de sécurité et les mauvais acteurs signifie qu'il doit y avoir un processus continu d'audit et d'évaluation du cycle de vie. Cela se traduit par une réévaluation constante des politiques, des processus, des procédures et des technologies pour s'assurer que le service public maintient un niveau élevé de sensibilisation aux menaces et un programme de sécurité solide qui peut répondre aux impacts ou atténuer les risques pour les opérations commerciales et le personnel. Cette démarche est complétée par une caractérisation récurrente des actifs, des évaluations de la vulnérabilité et des évaluations des menaces qui doivent tester en profondeur les stratégies d'atténuation, y compris les améliorations et les modifications technologiques.

Le fardeau financier que représente l'élaboration d'une stratégie de protection plus robuste et stratifiée ne doit pas être couvert par les seuls budgets des départements de sécurité. Les

dépenses de plusieurs départements peuvent être utilisées à l'adresse en employant des technologies à usages multiples qui favorisent l'efficacité opérationnelle et renforcent la sécurité. Les systèmes vidéo et de contrôle d'accès au niveau de l'entreprise peuvent servir de plate-forme intégrée pour recueillir toutes sortes d'informations à des fins opérationnelles. Les systèmes comprenant la surveillance des actifs, les capteurs environnementaux, la qualité de l'air, les systèmes de sécurité des personnes et d'autres systèmes de sécurité peuvent tirer parti d'une plateforme unique pour la diffusion d'informations aux différentes parties prenantes et aux différents services. Les notifications rapides et en temps réel qui s'ensuivent peuvent réduire la demande de ressources sur le terrain pour la maintenance et faciliter les pistes d'audit.

En fin de compte, la communication est essentielle et aucun problème ne doit être résolu en vase clos. Une collaboration constante avec d'autres secteurs ou entreprises confrontés à des menaces similaires peut aider à déterminer les solutions qu'il est réaliste de mettre en œuvre pour répondre aux besoins des entreprises et les sécuriser. L'analyse comparative et les forums d'utilisateurs permettent d'obtenir des informations opérationnelles sur les cas d'utilisation pertinents et les meilleures pratiques, qui peuvent à leur tour être utilisées pour les demandes de financement et l'élaboration d'une stratégie de déploiement de l'innovation. La communication avec les organismes d'intervention, tels que les forces de l'ordre locales ou les organismes de réglementation du secteur, peut aider une entreprise à se tenir au courant des menaces locales ou spécifiques au secteur.

Une stratégie de sécurité doit être multicouche et conçue en tenant compte des besoins opérationnels et commerciaux spécifiques, en utilisant toutes les ressources disponibles et l'expérience pertinente. Convergint est le guide idéal pour guider les entreprises de services publics tout au long de ce parcours. Nous **nous appuyons sur des analyses comparatives de l'industrie, des partenaires technologiques et des experts en sécurité dédiés à** tous les sous-secteurs des services publics pour développer une solution optimisée et personnalisée afin de répondre à ces besoins.