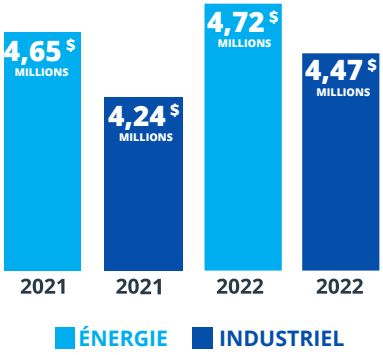
THREATQUOTIENT™

ThreatQ pour les entreprises d'énergie et de services publics

Offrant des services essentiels à la vie quotidienne, le secteur de l'énergie et des services publics constitue le pilier de la société moderne. En effet, cette infrastructure critique alimente non seulement nos maisons, mais sert également de socle à de nombreux secteurs, notamment la santé, les transports et les communications, pour ne citer que quelques exemples. Du fait de son rôle indispensable, le secteur de l'énergie et des services publics est devenu l'un des secteurs les plus ciblés par les cyberattaques. Ce rapport examine les principales menaces auxquelles ce secteur est confronté, en particulier les ransomwares, ainsi que les principaux défis qu'il doit relever pour maintenir une cybersécurité robuste.

La surface d'attaque du secteur de l'énergie et des services publics ne cesse de s'étendre à mesure que de nouveaux services y sont inclus. Si l'intégration des technologies numériques et des infrastructures intelligentes a incontestablement amélioré l'efficacité opérationnelle, elle a également multiplié les moyens à la disposition des cybercriminels pour compromettre les systèmes. Pour lutter efficacement contre ces menaces, il est essentiel de bien comprendre les vulnérabilités et les menaces. Cependant, les services publics manquent souvent de personnel et de ressources en matière de cybersécurité pour identifier les moyens techniques et comprendre les architectures complexes des systèmes et des réseaux nécessaires à la réalisation d'évaluations complètes de la cybersécurité, à la surveillance et aux mises à niveau nécessaires.

COÛT MOYEN D'UNE COMPROMISSION DE DONNÉES PAR SECTEUR D'ACTIVITÉ



IBM Security, Cost of a Data Breach Report 2022[3]

Les installations électriques peuvent être touchées par des cyberattaques tout au long de la chaîne.

GÉNÉRATION

Interférence avec le fonctionnement des centrales électriques et des sources d'énergie renouvelables par le biais d'attaques par ransomware et d'interruptions de service

TRANSMISSION

Déconnexion des services à distance, entraînant des coupures d'électricité à grande échelle pour les clients

DISTRIBUTION

Sabotage de sous-stations entraînant la perte régionale de services d'électricité et des perturbations pour les clients

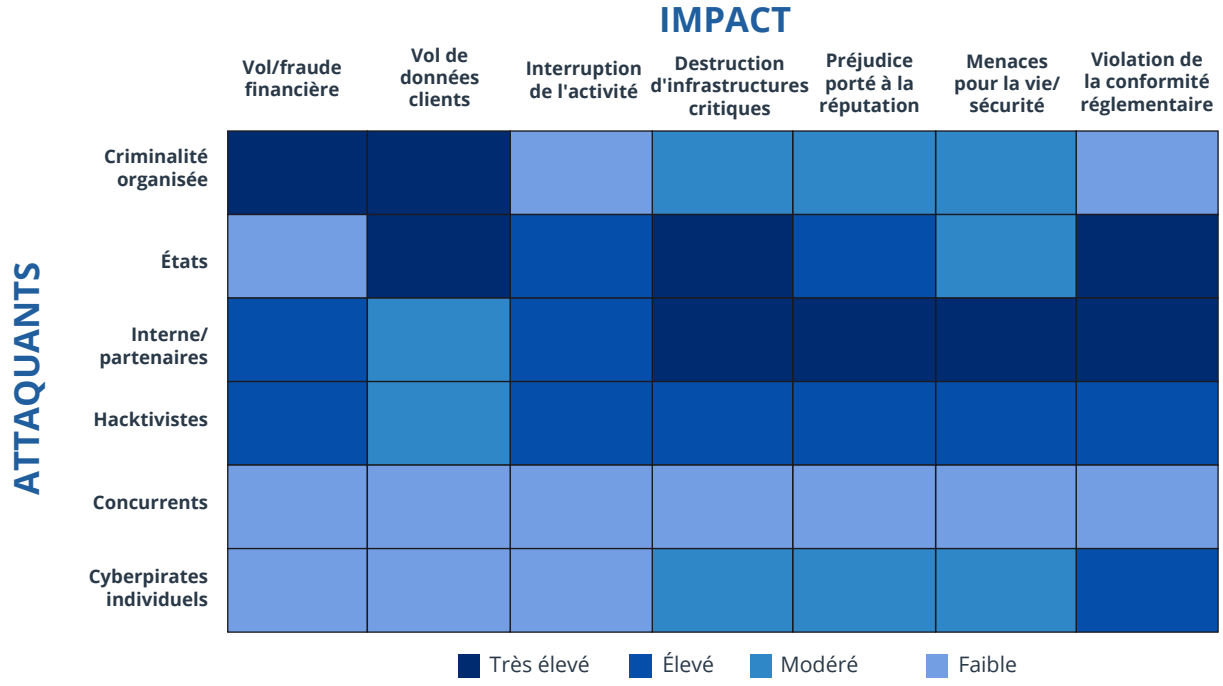
RÉSEAU

Vol de données clients, commission de fraudes et perturbations délibérées des services

Crédit : McKinsey & Company[2]

> Il est peu probable d'avoir connaissance à tout moment de l'intégralité des vulnérabilités et des menaces, mais faute d'équipes et/ou ressources de cybersécurité suffisantes, les services publics n'ont souvent pas les moyens d'identifier les actifs numériques et de maîtriser pleinement les architectures système et réseau nécessaires pour effectuer les évaluations de cybersécurité, assurer la surveillance et procéder aux mises à niveau.
>
> **- Idaho National Laboratory[1]**

Pour le secteur américain de l'énergie électrique, le risque de cybermenace le plus élevé provient de trois principaux types d'attaquants



Deloitte Insights[4]

PRINCIPAUX DÉFIS

Le secteur de l'énergie et des services publics est confronté à plusieurs défis majeurs en matière de protection de ses infrastructures critiques et de ses actifs numériques. Ces défis concernent non seulement les ransomwares, mais également les attaques de la chaîne logistique, l'intégration incomplète des systèmes, les inefficacités de la gestion des identités et des accès (IAM) et le problème croissant du phishing des appareils mobiles[5].

Ransomwares : Les ransomwares, des logiciels malveillants qui chiffrent les données d'une victime et exigent une rançon en échange d'une clé de déchiffrement, représentent l'une des menaces les plus importantes pour le secteur de l'énergie et des services publics. En 2021, la gravité de ce type de menace est apparue au grand jour lorsque le Colonial Pipeline a été victime d'une cyberattaque[6]. Cet incident a été considéré comme une menace pour la sécurité nationale, car il a perturbé le transport de carburant dans une grande partie des États-Unis, provoquant des achats de panique et des pénuries de carburant. Bien que la situation ait été résolue en moins d'une semaine, elle a mis en évidence la gravité de la menace que représentent les ransomwares. Les attaques par ransomware ne perturbent pas seulement les opérations, elles créent également un sentiment d'impuissance chez les victimes, qui les pousse à envisager de payer une rançon au cybercriminel en échange de la clé de déchiffrement et d'une chance de restaurer leurs systèmes critiques.

Attaques de la chaîne logistique : le secteur des services publics est sensible aux attaques de la chaîne logistique, qui visent les composants logiciels et matériels sur lesquels reposent ses opérations. Les cybercriminels peuvent compromettre ces chaînes logistiques afin d'introduire des vulnérabilités dans l'infrastructure, ce qui pourrait affecter de nombreux services publics simultanément.

Intégration incomplète des systèmes : l'adoption rapide des technologies numériques par le secteur a souvent entraîné une intégration incomplète des systèmes. Cette architecture fragmentée peut engendrer des failles et faiblesses de sécurité susceptibles d'être exploitées par les cybercriminels, car les systèmes interconnectés du secteur dépendent fortement de la communication et des flux de données.

Inefficacités de la gestion des identités et des accès (IAM) : les solutions de gestion des identités et des accès (IAM) sont essentielles pour garantir que seul le personnel autorisé accède aux systèmes sensibles. Les inefficacités, erreurs de configuration ou mécanismes d'authentification faibles des solutions IAM peuvent exposer le secteur à des accès non autorisés, des compromissions de données ou d'autres activités malveillantes.

Phishing des appareils mobiles : la prolifération des appareils mobiles dans les opérations du secteur introduit un autre vecteur d'attaque. Les attaques de phishing ciblant les appareils mobiles peuvent compromettre des informations sensibles et l'accès à des systèmes critiques, éprouvant encore davantage la cybersécurité du secteur.

Le secteur de l'énergie et des services publics joue incontestablement un rôle vital dans la société moderne, ce qui en fait une cible privilégiée pour toute une série de cybermenaces. Bien que le secteur soit confronté à une multitude de dangers, les ransomwares apparaissent comme un problème particulièrement urgent en raison de leur nature perturbatrice et de leur impact financier. Le secteur doit rester vigilant, évaluer en permanence les vulnérabilités et investir dans des mesures de cybersécurité robustes pour protéger les services essentiels qu'il fournit à la vie quotidienne. Dans un monde de plus en plus dépendant du numérique, il ne pourra protéger les infrastructures critiques du secteur contre l'évolution des menaces que s'il relève les principaux défis mentionnés, de la sécurité de la chaîne logistique à la gestion des identités et des accès. Pour assurer sa stabilité et la fourniture ininterrompue des services essentiels, le secteur doit travailler sans relâche pour se défendre contre les menaces persistantes en constante évolution auxquelles il est confronté.

UNE PLATE-FORME DE THREAT INTELLIGENCE DE POINTE

Une plate-forme de Threat Intelligence robuste orientée sur les données fournit aux fournisseurs d'énergie et de services publics le contexte et la priorisation dont ils ont besoin pour prendre des décisions plus avisées, accélérer la détection et la réponse à incident, et favoriser l'apprentissage et la collaboration entre équipes pour une amélioration continue. La plate-forme ThreatQ, qui sert de centre d'opérations de renseignement pour de nombreux secteurs, agrège et corrèle les données structurées et non structurées issues d'une multitude de sources, internes comme externes. Dans la mesure où tous les outils et technologies s'intègrent et fonctionnent en toute transparence avec l'architecture ouverte de ThreatQ, il n'est pas nécessaire de modifier l'infrastructure ou les workflows de sécurité existants. L'automatisation élimine les tâches répétitives et chronophages, permettant ainsi aux analystes de se concentrer sur des opérations prioritaires et stratégiques. La plate-forme permet en outre de partager rapidement des données de Threat Intelligence organisées, des conseils et des rapports avec un large éventail de parties prenantes internes et externes, y compris des secteurs de l'énergie et des services publics.

PRINCIPAUX ATOUTS DE THREATQ :

- **CONSOLIDATION** au sein d'un référentiel central de toutes les sources de renseignements sur les menaces et les vulnérabilités, tant externes (p. ex. E-ISAC et OSINT) qu'internes (p. ex. SIEM)
- **ÉLIMINATION** des nombreuses données parasites, pour mieux cibler les renseignements sur les menaces pertinents et se concentrer sur les ressources et les vulnérabilités critiques
- **PRIORISATION** des mesures et ressources primordiales pour votre environnement
- **TRAQUE PROACTIVE** des activités malveillantes pouvant indiquer des attaques par déni de service ou d'autres perturbations susceptibles de nuire aux clients, aux collaborateurs et aux parties prenantes
- **HIÉRARCHISATION** des vulnérabilités de sécurité connues et exploitées de manière active, risquant d'affecter la conformité réglementaire et la sécurité
- **ANALYSE ET RÉPONSE ACCÉLÉRÉES** permettant de contrer les attaques par une analyse collaborative des menaces, permettant une compréhension commune et une réaction coordonnée
- **AUTOMATISATION** de la détection des menaces et des interventions

Rendez-vous sur threatq.com/demo pour demander une démonstration en direct de la plate-forme ThreatQ et de ThreatQ TDR Orchestrator.

1. https://www.energy.gov/policy/articles/cyber-threat-and-vulnerability-analysis-us-electric-sector
2. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities
3. https://www.ibm.com/downloads/cas/3R8N1DZJ
4. https://www2.deloitte.com/content/dam/insights/us/articles/4921_Managing-cyber-risk-Electric-energy/DI_Managing-cyber-risk.pdf
5. https://energydigital.com/technology-and-ai/the-top-5-cyber-threats-to-the-energy-sector
6. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

À PROPOS DE THREATQUOTIENT™

ThreatQuotient améliore les opérations de sécurité en regroupant des sources de données, des outils et des équipes disparates afin d'accélérer la détection des menaces et la réponse à incident. La plate-forme d'opérations de sécurité orientée sur les données de ThreatQuotient permet aux équipes de prioriser les menaces, d'automatiser les tâches et de collaborer pour résoudre les incidents de sécurité. Elle permet une prise de décision plus ciblée et optimise les ressources limitées en intégrant les processus et technologies existants dans un espace de travail unifié. Résultat : une réduction des informations parasites, des menaces prioritaires claires et la possibilité d'automatiser les processus avec des données extrêmement fiables. Les fonctionnalités de pointe en matière de gestion, orchestration et automatisation des données de ThreatQuotient prennent en charge de nombreux scénarios d'utilisation, notamment la réponse à incident, le Threat Hunting, la lutte contre le spear phishing, le tri des alertes et la priorisation des vulnérabilités. Par ailleurs, elles peuvent également servir de plate-forme de Threat Intelligence. ThreatQuotient est basé dans le nord de la Virginie, et possède des filiales chargées des opérations internationales en Europe, en Asie-Pacifique et dans la région Moyen-Orient/Afrique du Nord. Pour plus d'informations, consultez le site www.threatquotient.com.

THREATQUOTIENT™

20130 Lakeview Center Plaza, Suite 400 Ashburn, VA 20147, États-Unis • ThreatQ.com
Sales@ThreatQ.com • +1 703 574-9885

TQ-IDB08-1223-01