ASSALA ENERGY

2024

ÉTUDE DE CAS : LA CYBERSÉCURITÉ

Étude de cas : l'évaluation des risques liés à la cybersécurité

Dans un monde et un environnement professionnel de plus en plus dépendants de l'infrastructure numérique, la cybersécurité revêt une importance stratégique cruciale pour Assala. De nouveaux risques apparaissent en permanence par la présence d'acteurs nationaux et internationaux. Bien qu'il n'y ait pas eu d'impact significatif sur l'infrastructure informatique d'Assala en 2024, nous savons que nous devons rester vigilants et adopter une approche proactive face aux cybermenaces.

En 2024, nos équipes informatiques se sont concentrées sur les risques continus de cybersécurité par le biais de programmes d'identification, d'évaluation et d'atténuation, en appliquant les cadres et les bonnes pratiques du secteur. Un programme complet de formation et de sensibilisation des utilisateurs finaux et un centre d'opérations de sécurité fonctionnant 24 heures sur 24, 7 jours sur 7 ont également été mis en place.

Lors de la mise en œuvre de nos contrôles de cybersécurité, nos équipes informatiques prennent en compte les implications environnementales, sociales et de gouvernance de leurs initiatives, permettant l'amélioration durable et continue de nos processus et systèmes informatiques afin de soutenir la préparation opérationnelle.

Atténuation : sensibilisation des utilisateurs finaux à la sécurité

L'un des principaux risques identifiés pour notre entreprise est une attaque visant notre personnel ou notre infrastructure informatique, susceptible d'entraîner des temps d'arrêt pour l'entreprise et des incidents liés à la sécurité des personnes ou des processus au cours des opérations. En outre, de telles attaques pourraient entraîner une violation de la sécurité de l'information et des fuites de données personnelles sensibles ou de données exclusives.

À ce titre, nous encourageons une culture de la sécurité informatique afin de responsabiliser les utilisateurs quant à leur rôle dans la protection de l'entreprise, de ses salariés et de l'environnement contre de telles attaques. Nous veillons à ce que tous les usagers des systèmes informatiques d'Assala suivent des formations régulières afin de les sensibiliser aux dernières menaces en matière de sécurité et aux bonnes pratiques pour y faire face. Dans le cadre de son programme de formation, le personnel reçoit un retour d'information immédiat sur ses performances, ce qui lui permet d'identifier rapidement les besoins supplémentaires en matière d'assistance ou de formation, et de continuer à réduire les risques associés à l'utilisateur.

Atténuation : un cadre de cybersécurité solide

Conformément aux Valeurs d'Assala, nos équipes informatiques appliquent les normes et bonnes pratiques internationales et mettent en œuvre le cadre de cybersécurité du *National Institute of Standards and Technology (NIST)*, qui fournit une structure complète pour gérer les risques de cybersécurité, adopter les bonnes pratiques et se concentrer sur l'amélioration continue.

Atténuation : sécurité à plusieurs niveaux et centre d'opérations de sécurité fonctionnant 24 heures sur 24, 7 jours sur 7

Assala a mis en place des contrôles de cybersécurité à plusieurs niveaux ainsi qu'un centre d'opérations de sécurité (SOC), ce qui signifie que si une couche de sécurité est compromise, d'autres couches sont en place pour protéger les données, les systèmes et les utilisateurs d'Assala. Le SOC surveille et analyse en permanence les alertes de sécurité d'Assala, qui sont cruciales pour notre architecture de cybersécurité.

Grâce à la surveillance et aux alertes en temps réel du SOC ainsi qu'à nos défenses multicouches, nous nous adaptons rapidement à l'évolution du contexte des cybermenaces, ce qui garantit une sécurité accrue, la protection des données et la continuité des activités. Cette approche proactive est essentielle pour atténuer les risques et réduire l'impact des cybermenaces.

Résultats

Grâce à cette approche tridimensionnelle, Assala :

- **Garantit la conformité** en alignant notre processus sur les exigences réglementaires en matière de protection des données, ainsi que sur les normes et bonnes pratiques internationales.
- **Responsabilise l'ensemble de l'organisation vis-à-vis de la cybersécurité** en mettant en évidence et en formant les parties prenantes à une gestion efficace de la technologie, de l'information et du matériel.
- **Facilite l'évaluation des risques globale** en encourageant l'identification, l'évaluation et l'atténuation des risques de manière proactive.
- **Protège les données des parties prenantes** en suivant les bonnes pratiques internationales en matière de gestion des informations sensibles.
- **Renforce notre réputation d'opérateur responsable** en démontrant notre engagement à atténuer les risques associés à une cybersécurité inefficace.
- **Optimise les ressources,** susceptibles d'entraîner un gaspillage de l'énergie et des ressources nécessaires à la résolution des violations.
- **Réduit les déchets électroniques** en limitant la probabilité que le matériel devienne obsolète en raison de dommages causés par les logiciels malveillants et les virus.

ASSALA ENERGY

www.assalaenergy.com

www.linkedin.com/company/assala-energy/

Création, conception et production : You Are Stories (www.youarestories.com).