illumio

BRIEF SECTORIEL

Maintenir la sécurité énergétique

Comment la segmentation Zero Trust peut offrir une cyber-résilience sur le marché de l'énergie

Transformation numérique et nouvelles cybermenaces

L'énergie, et en particulier l'électricité, est la base de toutes les activités dans le monde d'aujourd'hui. Il existe une liste de plus en plus importante de difficultés en matière de sécurité énergétique dans de nombreux pays, notamment :

- Le changement climatique oblige à repenser la façon dont l'énergie est générée
- Augmentation des prix créant une pauvreté énergétique
- La transformation en arme de l'énergie dans les conflits physiques et cybernétiques mondiaux
- Le « tsunami » de la demande causé par le transport électrique et le cloud

En transformant numériquement de nombreuses parties de l'activité, la demande et l'offre peuvent être optimisées pour s'assurer que les besoins des consommateurs peuvent être satisfaits. Les opérateurs énergétiques peuvent effectuer de petits ajustements à l'aide de l'analyse des Big Data et, à l'avenir, de l'IA pour maintenir la cohérence du flux.

Cela peut inclure la réaffectation d'une alimentation en gaz ou l'engagement d'un système hydroélectrique de stockage de pompe aux heures de pointe. Une infrastructure beaucoup plus intelligente est nécessaire afin de collecter suffisamment de données pour effectuer ces analyses, et nous voyons donc le déploiement de nouveaux systèmes avec des capacités de collecte de données intégrées ou l'ajout de ces fonctions.

Toutes ces étapes augmentent potentiellement la surface d'attaque disponible pour les acteurs malveillants qui infiltrent le système et provoquent des perturbations majeures. La responsabilité principale des équipes de sécurité est maintenant de réduire ce risque et de survivre à toute attaque qui pourrait survenir.

La résilience et la menace cyberphysique

« Le caractère des cybermenaces a changé. Les répondants pensent désormais que les cyberattaques sont plus susceptibles de se concentrer sur la perturbation de l'activité et les atteintes à la réputation. »

Perspectives du Forum économique mondial 2023 sur la cybersécurité

« Lors de la mise en œuvre des exigences de cybersécurité, les planificateurs de réseau et de DER doivent construire des cyberdéfenses dans le but de survivre à une attaque tout en maintenant la fonctionnalité essentielle. »

Ministère de l'Énergie des États-Unis

Les attaques contre les entreprises énergétiques se divisent en trois groupes distincts :

- Vol de données critiques pour le client ou l'entreprise
- Un rançongiciel générique qui peut être dirigé, ou viral pour attaquer les systèmes d'information ou la technologie opérationnelle
- Une attaque cyberphysique ciblée sur un système spécifique pour provoquer une perturbation maximale

Une grande majorité de ces attaques commenceront par des attaques d'hameçonnage et se propagent rapidement à la cible prévue. La réduction de ce mouvement peut réduire l'impact d'une attaque.

Défis

Les exigences de cybersécurité de haut niveau pour les opérateurs de services essentiels comprennent :

- Identification des appareils TI et TO hérités et inconnus
- Cartographie des communications entre les applications, les systèmes et les appareils TI et TO
- Confinement des attaques de rançongiciel
- Atténuation du risque des vulnérabilités connues et inconnues

La clé pour survivre à une attaque est de réduire l'impact et de s'assurer qu'elle n'atteint pas les parties les plus critiques du réseau.

Après quelques attaques récentes, les régulateurs nationaux du monde entier émettent de nouvelles directives pour tous les domaines du marché de l'énergie. Cela inclut l'AESCSF en Australie et la directive TSA sur les pipelines aux États-Unis.

De nombreux régulateurs recommandent de suivre les étapes du cadre de cybersécurité du NIST :

1. **Identifier**
   Illumio génère une simple carte montrant tous les appareils et le flux de leurs communications vers des ressources informatiques externes, telles que les applications, les serveurs, les bases de données, Internet ou même les appareils intelligents. Grâce à ces connaissances, la génération des politiques de sécurité requises est un processus beaucoup plus simple.

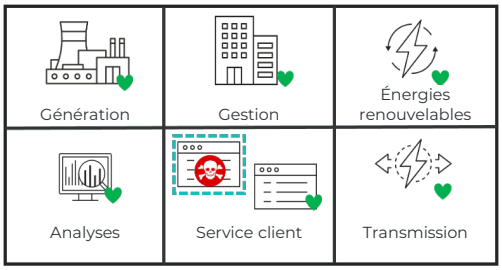
2. **Protéger**
   Pour éviter la contamination croisée des logiciels malveillants des environnements TI aux environnements TO et vice versa, il est important de ne permettre que la communication entre les appareils nécessaires. Avec Illumio, vous pouvez bloquer les ports spécifiques que les cyber agresseurs et les rançongiciels utilisent généralement.

   Cependant, la limitation des correctifs peut être gérée en limitant les systèmes qui peuvent communiquer et les protocoles qu'ils utilisent.

3. **Détecter**
   La détection d'une attaque est essentielle pour neutraliser la menace, et plus elle est rapide, mieux c'est. On a montré que la segmentation du réseau améliore les performances des systèmes détection des points de terminaison et réponse (EDR) en limitant la propagation d'une attaque, réduisant ainsi la zone requise pour la détection.

4. **Répondre**
   Une fois qu'une attaque est détectée, vous devez réagir instantanément. Dès qu'une attaque commence, elle doit être arrêtée. Avec une segmentation Zéro Confiance (Zero Trust Segmentation, ZTS), vous pouvez confiner efficacement les attaques pour réparer les services plus efficacement pendant que le logiciel malveillant est supprimé.

5. **Restaurer**
   Les équipes de sécurité et d'informatique peuvent mettre en place une protection autour des services et systèmes individuels afin de pouvoir reprendre les opérations tout en étant à l'abri de l'attaque. Avec les connaissances acquises lors de l'attaque infructueuse, vous pouvez ajuster vos politiques pour resserrer l'accès et renforcer la cyber-résilience de votre organisation.



Arrêter la propagation des violations

Sécurisez votre fonctionnement énergétique avec ZTS

Rendez-vous sur : illumio.com/products

À propos d'Illumio

Illumio, pionnier et leader du marché de la segmentation Zero Trust, empêche les violations de devenir des cyber-catastrophes. Illumio protège les applications critiques et les actifs numériques précieux grâce à une technologie de segmentation éprouvée, spécialement conçue pour le modèle de sécurité Zero Trust. Les solutions d'atténuation et de segmentation des rançongiciels Illumio détectent les risques, isolent les attaques et sécurisent les données sur les applications natives du cloud, les clouds hybrides et multiclouds, les centres de données et les terminaux, permettant ainsi aux plus grandes organisations mondiales de renforcer leur cyber-résilience et de réduire les risques.