Services d'évaluation de la sécurité de votre réseau pour mise en conformité

Dans un monde en constante évolution, garantir la sécurité de l'infrastructure réseau pour toute organisation qui souhaite se protéger contre les cybermenaces et se conformer aux réglementations telles que le NIS2, est primordial.

La cybersécurité nécessite d'être définie et prise en charge sur l'ensemble de ses aspects pour assurer la sécurité de vos informations et de vos activités. Ils doivent être évalués en fonction des réglementations et des besoins de votre entreprise :

- **Évaluation des risques** : C'est la première étape et elle est fondamentale. Elle permet de définir le périmètre à protéger, les menaces et les impacts potentiels. Si elle n'est pas effectuée correctement par un organisme certifié, les risques et les vulnérabilités de l'environnement de cybersécurité peuvent ne pas avoir été détectés
- **Topologie du réseau** : S'il n'a pas été structuré de manière qu'un appareil ne puisse voir que que les autres appareils correspondant à son activité, le passage de l'un à l'autre est facilité pour tout attaquant
- **Mauvaises configurations et logiciels obsolètes** : ils créent des vulnérabilités que les attaquants peuvent exploiter
- **Accès au réseau** : En l'absence d'un contrôle rigoureux, des entités non autorisées peuvent se glisser dans le réseau sans être détectées, ce qui présente des risques importants
- **Cryptage des données** : si les données ne sont pas cryptées, elles sont vulnérables à l'interception et au vol, en particulier lorsqu'elles sont transmises sur les réseaux
- **Sécurité des terminaux** : il s'agit des ordinateurs portables et de leurs accessoires, des smartphones et des appareils IoT que vos équipes utilisent tous les jours. Ils sont souvent ciblés comme points d'entrée pour les cyberattaques, ce qui les rend vulnérables aux menaces telles que le phishing et les ransomwares. Des terminaux non protégés représentent des vulnérabilités, ils peuvent entraîner des accès non autorisés et des infections généralisées par des logiciels malveillants
- **Intégration OT et IT** : Tous les problèmes pouvant découler des interconnexions entre vos infrastructures cyber et vos infrastructures opérationnelles doivent faire l'objet d'une analyse approfondie
- **Plan d'amélioration** : Un plan clair et réalisable de mise à niveau de votre réseau garantit que votre équipe pourra rapidement comprendre, contenir et récupérer les incidents, minimisant ainsi les temps d'arrêt et l'impact sur vos activités.

En se concentrant sur les domaines critiques, les entreprises développent leurs stratégies de cybersécurité complètes qui protègent leurs organisations contre les menaces tout en assurant la résilience opérationnelle et la conformité de leurs activités.

L'infrastructure réseau Alcatel-Lucent Enterprise étant au cœur de votre cyber environnement, elle doit être correctement designée, installée et gérée pour garantir la sécurité de l'ensemble de votre écosystème.

En engageant une démarche structurée de mise à jour de votre cybersécurité, votre organisation est mieux armée contre les cybermenaces du monde numérique d'aujourd'hui. En restant proactive et informée, votre entreprise peut maintenir une posture de sécurité réseau résiliente qui protège à la fois l'organisation et ses données stratégiques.

Alcatel·Lucent Enterprise

Services d'évaluation de la sécurité d'ALE

Afin de garantir que votre infrastructure réseau est à l'état de l'art en termes de cybersécurité, ALE a conçu une démarche structurée d'analyse, de préconisations et de bonnes pratiques basée sur les fonctionnalités de nos produits qui vous est proposée par le biais de ce service.

Le service d'évaluation de la sécurité d'ALE analyse les performances et la sécurité de votre réseau. En tant que constructeur, nous proposons les configurations et les implémentations à l'état de l'art dans un plan de remédiation qui vous est dédié afin que vous soyez prêt à démontrer votre conformité aux règlementations telles que NIS2, CRA, LM lors d'un audit de sécurité auprès d'un organisme certifié.

Vérifiez votre situation initiale

L'effort de préparation pour pouvoir soumettre votre réseau à un audit de sécurité auprès d'un organisme certifié doit être **sécurisé et optimisé**. Vous devez être en **mesure de cibler les bons aspects avec les bonnes pratiques afin d'aligner les attentes et les obligations** avec vos activités métier. Ainsi, vous rendez accessible votre conformité en matière de sécurité.

En fonction de votre maturité sur votre réseau, vous pouvez avoir besoin de conseils, d'informations et de la définition d'un plan d'amélioration.

Avec notre atelier préliminaire ou éventuellement le questionnaire préliminaire sur notre portail WEB, notre expert clarifie votre situation de départ. Cette phase préliminaire est gratuite. C'est aussi le moment pour nous de vous indiquer l'effort à fournir et de vous proposer une prestation dédiée pour une évaluation de votre réseau si nécessaire.

Obtenez une évaluation de votre réseau

Si vous optez pour cette prestation, nous engageons l'évaluation de votre réseau. Notre expert analyse la topologie de votre réseau, les configurations, l'utilisation des fonctionnalités, les intégrations, les vulnérabilités potentielles internes/externes et identifie les problèmes de performance, les besoins d'optimisation et les meilleures pratiques à appliquer pour que vous puissiez vous conformer à vos obligations.

Obtenez un rapport avec une description du plan d'amélioration

À partir de cette analyse, notre expert consolide les conclusions, les points ouverts et les questions, il intègre les recommandations et les meilleures pratiques à appliquer dans un **rapport unique**. Il présente ce rapport à vos équipes avec votre partenaire ALE et s'assure que vous comprenez votre niveau d'exposition et les risques qu'il implique.

Exécutez le plan d'amélioration avec notre partenaire pour atteindre la conformité

Le plan de remédiation est décrit dans le rapport remis par notre expert. Il montre la voie à suivre pour obtenir des configurations de sécurité à la pointe de la technologie et pour se conformer aux normes. Des étapes et des activités sont recommandées et décrites, elles peuvent être réalisées généralement par le partenaire. L'exécution du plan de remédiation vous permet de bénéficier de la valeur réelle de notre expertise en matière de performances et de sécurité sur votre réseau et de vous préparer à la conformité aux réglementations.

Politique de sécurité récurrente

L'exécution du plan de remédiation est indispensable, mais elle ne constitue pas la fin de l'histoire. Les menaces de sécurité évoluent, votre entreprise évolue et les réglementations évoluent, de sorte que des évaluations régulières sont nécessaires. Nous vous recommandons **un rythme pour les évaluations régulières**, partielles ou complètes. Entre-temps, conformément à nos processus standard, nous émettons régulièrement des alertes et des recommandations en matière de sécurité sur nos produits et, grâce à des contrats d'assistance actifs pour tous vos équipements, vous êtes assuré de recevoir les correctifs et les mises à jour de sécurité en temps voulu.

La contribution de l'infrastructure de votre réseau ALE à l'ensemble de votre cybersécurité est vitale et peut se composer des éléments suivants :

- une **infrastructure de réseau robuste**
- une **architecture segmentée** où les couches et les séparations sont définies, mises en œuvre et testées
- une **politique de confiance zéro** où aucune connexion d'appareil ne peut avoir lieu sans un processus d'approbation dédié
- des versions actualisées et des **configurations à l'état de l'art** de la technologie
- une **détection** des événements et des notifications aux administrateurs
- une **intégration** avec un système de gestion des informations et des événements de sécurité (SIEM)
- des programmes de **formation et de sensibilisation du personnel** à l'utilisation et à la gestion du réseau
- une adhésion aux normes industrielles en matière de conformité et de gouvernance

Comprendre l'impact de votre posture de sécurité sur votre activité

Obtenez les descriptions détaillées et des clarifications sur les problèmes de configuration et les vulnérabilités à partir de notre analyse de la topologie du réseau.

Sécurisez votre réseau pour protéger votre activité

Alignez votre réseau sur les recommandations constructeur d'ALE, les caractéristiques de sécurité les plus récentes,
nos meilleures pratiques et nos recommandations.

Assurez la conformité à la réglementation et soyez prêt pour un audit de cybersécurité

Alignez votre réseau sur les réglementations applicables, assurez-vous que la topologie et les configurations de votre réseau sont conformes aux exigences réglementaires.

Pour plus d'informations, visitez notre page Services Professionnels.

© 2025 ALE International, ALE USA Inc. Tous droits réservés pour tous pays. Le nom et le logo d'Alcatel-Lucent sont des marques commerciales de Nokia utilisées sous licence par ALE. Pour voir la liste des marques de commerce d'ALE, veuillez consulter : www.al-enterprise.com/fr-fr/documentation-juridique/marques-copyright. DID250218FR (mars 2025)

Alcatel·Lucent Enterprise