**Email – Guide de durcissement**

Sujet : Renforcez la sécurité de votre réseau avec le Guide de durcissement 2N

**En-tête :** Téléchargement

Cher [Nom du destinataire],

Dans le paysage actuel de la cybersécurité, qui évolue rapidement, **assurer la sécurité de vos dispositifs IP n'est plus facultatif, c'est essentiel**. Les cybermenaces étant de plus en plus sophistiquées, la nécessité de protéger les systèmes n'a jamais été aussi urgente.

Pour vous aider à garder une longueur d'avance, nous vous proposons le Guide de durcissement 2N, une ressource complète qui présente les meilleures pratiques essentielles pour améliorer la sécurité des périphériques réseau 2N.

Que vous gériez des périphériques dans un environnement de haute sécurité comme les soins de santé ou le gouvernement, ou que vous cherchiez simplement à sécuriser un bâtiment résidentiel ou multifonctionnel, ces recommandations sont conçues pour minimiser les vulnérabilités et renforcer vos défenses.

**Ce que vous apprendrez**

* **Définir des mots de passe forts :** Établir des identifiants robustes pour empêcher les accès non autorisés
* **Mises à jour régulières des microprogrammes :** Mise à jour des vulnérabilités connues pour garder une longueur d'avance sur les menaces
* **Protocoles de communication sécurisés :** Assurer une communication sûre entre les appareils
* **Activation du cryptage :** Protéger les données sensibles pendant la transmission
* Désactiver les services inutiles : Minimiser les surfaces d'attaque potentielles
* **Limiter l'accès au réseau** : Réduire l'exposition en limitant l'accès aux utilisateurs de confiance
* **Segmentation du réseau :** Isoler les dispositifs critiques du trafic réseau général pour renforcer la sécurité

N'attendez pas qu'une faille se produise. Renseignez-vous et protégez votre système dès maintenant. Le Guide de durcissement 2N est votre ressource essentielle pour maintenir un réseau robuste et sécurisé.

[Télécharger]

Meilleures salutations,

**Bannière - article tendance**

Aperçu de 2N sur la directive NIS2

Vous recevez de plus en plus de questions sur la future directive européenne NIS2 et son impact sur les entreprises ? Découvrez ce qu'elle signifie, qui elle affecte et comment 2N, l'un des principaux fournisseurs de systèmes de contrôle d'accès, s'y prépare dans cet article perspicace.

>>Lire la suite

**NIS2 – Trend article**

**La voie de la sécurité numérique : un aperçu de la directive NIS2 de l'UE**

**Les cybermenaces et la réponse européenne**

La numérisation croissante n'est pas seulement synonyme de progrès. Elle présente également un risque croissant : les cyberattaques. Pour y faire face, l'Union européenne a introduit la directive NIS (Network and Information Security) en 2016. L'objectif était de renforcer la cybersécurité dans les secteurs stratégiques et essentiels : en particulier l'énergie, les transports, les banques, les marchés financiers, les soins de santé, l'eau et les infrastructures numériques.

Depuis lors, cependant, la société a connu des changements fondamentaux, en particulier après l'adoption de la directive COVID. Le déploiement massif d'outils de vidéoconférence (tels que MS Teams, Zoom ou Google Meet), associé à une demande accrue en matière de commerce électronique et de services de livraison, a intensifié la transition vers le monde numérique. En fait, McKinsey estime que la pandémie a accéléré la numérisation de 3 à 4 ans. Ces évolutions ont entraîné de nouveaux défis en matière de cybersécurité, et l'UE a donc dû mettre à jour sa directive.

**NIS2 : des règles plus strictes pour un monde plus sûr**

L'UE a adopté la nouvelle directive NIS2 en novembre 2022. Cette directive élargit considérablement le champ d'application de la législation initiale et renforce les mesures de sécurité. En plus des sept secteurs initiaux, le NIS2 couvre désormais de nouveaux domaines tels que l'industrie manufacturière, les services postaux et de courrier, la science, la recherche et l'éducation.

Le NIS2 exige des entreprises et des organisations de tous ces secteurs qu'elles identifient et gèrent les cyber-risques, qu'elles sécurisent leurs systèmes d'information et qu'elles forment régulièrement leur personnel. L'un des nouveaux règlements prévoit même l'obligation de signaler les incidents de sécurité graves dans les 24 heures suivant leur découverte, avec un rapport détaillé dans les 72 heures et un rapport final dans les 30 jours.

La directive divise également les organisations en deux catégories : les entités « essentielles » et les entités « critiques », chaque catégorie ayant des obligations spécifiques. Les sanctions en cas de non-respect des règles peuvent être très sévères. Les entités essentielles s'exposent à des amendes pouvant aller jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu. Les entités majeures peuvent se voir infliger une amende allant jusqu'à 7 millions d'euros ou 1,4 % de leur chiffre d'affaires.

Le NIS2 joue donc un rôle clé dans la garantie de la cybersécurité dans l'UE. L'organisation s'est engagée à introduire de nouvelles mesures et à respecter des règles strictes pour protéger les infrastructures critiques telles que les réseaux d'énergie, l'eau et les soins de santé. Cela permet de garantir que les services essentiels dont dépendent les citoyens restent opérationnels et sûrs en cas de cyberattaque.

**Comment 2N se prépare-t-elle à NIS2 ?**

2N doit se conformer à la NIS2 : elle est considérée comme une entité obligée (plus de 250 employés et un chiffre d'affaires annuel de plus de 10 millions d'euros) et relève de plusieurs secteurs réglementés tels que la « fabrication d'appareils et d'équipements électroniques », la « fourniture de services de communications électroniques accessibles au public » et le « fournisseur de services d'informatique en nuage ».

L'entreprise est active depuis longtemps dans le domaine de la cybersécurité et détient la certification ISO 27001, qu'elle maintient régulièrement lors des audits de surveillance et de recertification. Cette année, 2N a également obtenu la certification de sécurité IEC 62443-4-1, qui s'applique à ses produits d'ascenseur.

Mais quelle est la prochaine étape ? 2N doit se conformer aux règles strictes du NIS2 et revoir régulièrement et en profondeur les mesures de sécurité existantes. Elle procède donc à une analyse des lacunes afin de déterminer les obligations NIS2 qu'elle respecte déjà (grâce à la certification ISO 27001) et celles qui doivent encore être mises en œuvre. La cybersécurité étant l'une des principales priorités de 2N, l'entreprise s'attend à ce que la mise en conformité avec les exigences restantes se fasse sans heurts et dans les délais légaux. Vous pouvez être certain qu'en choisissant 2N, vous ne risquez pas de ne pas respecter les directives de l'UE.

**Connaissance, confiance et transparence : des valeurs clés**

2N s'appuie depuis longtemps sur les connaissances et l'expérience approfondies en matière de cybersécurité de sa société mère AXIS. Les experts des deux sociétés sont en contact quotidien et partagent les meilleures pratiques et les idées en matière de développement sécurisé.

L'un des principaux outils adoptés par 2N est le modèle de développement de la sécurité d'Axis (Axis Security Development Model - ASDM), qui décrit 13 processus et pratiques de sécurité axés sur la mise en œuvre (et la vérification ultérieure) de mesures de sécurité à chaque étape du développement. Cette approche minimise le risque d'incidents de sécurité et renforce la confiance et la satisfaction de ses clients.

La confiance et la transparence entre l'entreprise et ses clients sont des valeurs clés pour 2N. L'entreprise publie tous les documents et informations relatifs à la cybersécurité sur son site web, ce qui garantit non seulement la sécurité de ses produits et services, mais renforce également votre confiance en leur fiabilité.