STORMSHIELD

CONFORMITÉ EN MATIÈRE DE CYBERSÉCURITÉ POUR LES ORGANISATIONS DU SECTEUR DU TRANSPORT

Dans le secteur du transport, où la disponibilité du système d'exploitation est essentielle, une cyberattaque peut entraîner des blessures physiques et nuire à l'environnement. Les personnes font face à des risques comme des accidents, des déraillements, la perte de contrôle d'un conteneur, des collisions de navires dans un port, des incendies ou encore des intoxications au monoxyde de carbone dans les tunnels en raison de l'absence de ventilation... L'environnement, quant à lui, fait face à des risques comme les marées noires qui polluent l'eau et ont des effets néfastes sur la faune et la flore.

> RÉGLEMENTATIONS EUROPÉENNES : CONFORMITÉ REQUISE

> OBLIGATIONS DE CONFORMITÉ FACULTATIVES

> RÉGLEMENTATIONS PROPRES À CHAQUE PAYS

> POUR CHAQUE PROBLÈME, IL EXISTE UNE SOLUTION STORMSHIELD

> LA CONFORMITÉ NE FAIT PAS TOUT

> RÉGLEMENTATIONS EUROPÉENNES : CONFORMITÉ REQUISE

Les organisations du secteur du transport doivent se conformer aux réglementations de cybersécurité européennes suivantes :

Règlement général sur la protection des données (RGPD)

Le RGPD est une réglementation de l'Union européenne conçue pour unifier les lois relatives à la confidentialité des données en Europe, protéger et responsabiliser l'ensemble des citoyens européens en ce qui concerne la confidentialité de leurs données, et repenser l'approche des organisations en matière de confidentialité des données. Cela crée de nouvelles contraintes et exigences pour les responsables informatiques et opérationnels, les directeurs de l'information et les directeurs de la sécurité informatique.

L'exigence principale de cette réglementation est la « protection des données par défaut », qui définit la protection des données personnelles comme un élément intrinsèque des systèmes et services. Les produits Stormshield aident les organisations à se conformer à ces exigences en améliorant la cyber-résistance de leur infrastructure. De plus, Stormshield Data Security fournit des fonctionnalités de chiffrement des données, qui est considéré par le RGPD comme une mesure technique appropriée pour garantir le niveau de sécurité adapté selon le risque.

Directive sur la sécurité de l'information et des réseaux (NIS, Network and Information Security)

La Directive NIS, première législation européenne sur la cybersécurité, est conçue pour accroître le niveau général de cybersécurité au sein de l'Union européenne, et doit être transposée dans le droit de chaque État membre. Dans le cadre de la Directive NIS, chaque pays doit désigner des Opérateurs de Services Essentiels (OSE) dans les secteurs comme l'énergie, le transport, l'eau, la banque, la santé et l'infrastructure numérique. Les OSE désignés doivent ensuite se conformer à la Directive. Après la transposition en droit français en 2018, l'ANSSI a publié un guide de recommandations pour la protection des systèmes d'information essentiels. Un guide pour accompagner la mise en œuvre technique des règles relatives à la protection des réseaux et systèmes d'information.

Les produits Stormshield de confiance et certifiés permettent aux Opérateurs de Services Essentiels (OSE) de déployer des solutions de sécurité qui améliorent le niveau de protection des Systèmes d'Information Essentiels (SIE). À titre d'exemple, Stormshield Network Security assure la segmentation des réseaux, la sécurisation des accès distants, l'authentification des utilisateurs et la gestion des vulnérabilités. Déployé en complément d'un antivirus (le cas échéant), Stormshield Endpoint Security (SES) propose une protection en profondeur des postes de travail contre les attaques sophistiquées. SES peut également améliorer la protection des systèmes d'exploitation obsolètes, détecter et gérer les incidents, et assurer une protection contre les attaques par rebond.

> **RÉGLEMENTATIONS EUROPÉENNES : CONFORMITÉ REQUISE**

Payment Card Industry Data Security Standard (PCI-DSS)

La norme de sécurité de l'industrie des cartes de paiement, PCI-DSS, est un ensemble de normes relatives à la sécurité de l'information pour les organisations qui traitent des cartes de crédit de marque émises par des entreprises majeures de cartes de crédit. Chaque commerçant, institution financière ou autre entité qui stocke, traite ou transmet des données de titulaires de carte doit se conformer à ces normes, qui incluent des dispositions en lien avec la sécurité du réseau, le chiffrement des données, la gestion des vulnérabilités et le contrôle renforcé des accès.

Les produits Stormshield permettent aux organisations de se conformer à la plupart des principales exigences PCI-DSS. À titre d'exemple, Stormshield Network Security (SNS) peut segmenter les réseaux et chiffrer le trafic sortant, gérer les vulnérabilités et authentifier les utilisateurs. Stormshield Data Security peut chiffrer les données de titulaires de carte pour garantir l'intégrité et la confidentialité des données. Déployé en complément d'un antivirus, Stormshield Endpoint Security (SES) renforce la protection des stations de travail contre les menaces sophistiquées. SES peut également améliorer la protection des systèmes d'exploitation obsolètes, détecter et gérer les incidents, et assurer une protection contre les attaques par rebond.

Directive sur la réutilisation des informations du secteur public (PSI, Public Sector Information)

La Directive PSI établit un cadre législatif commun qui encourage les États membres de l'UE à mettre à disposition autant d'informations du secteur que possible pour réutilisation. PSI inclut toutes les informations que les organismes publics produisent, collectent et achètent. La Directive PSI, transposée dans la législation propre à chaque pays, constitue la base de la politique de l'open data de l'UE. Toutes les organisations qui gèrent des informations publiques ou génèrent des données de projets d'étude bénéficiant de financements publics doivent fournir un accès public à ces données, sous réserve de certaines contraintes.

Les produits Stormshield peuvent aider les organisations à se conformer à la Directive PSI. Stormshield Network Security (SNS) permet notamment la micro-segmentation du réseau, afin que la zone de stockage des données publiques puisse être isolée. De plus, avec sa gestion intuitive des politiques de sécurité, SNS facilite l'identification des réseaux, la gestion des accès par utilisateur ou par groupe, et l'établissement de restrictions temporelles.

> **RÉGLEMENTATIONS EUROPÉENNES : CONFORMITÉ REQUISE**

CEI 62443

La norme ISA-99/CEI 62443, créée par la société internationale d'automatisation (ISA, International Society of Automation), est la norme internationale pour les systèmes de contrôle industriels (ICS, Industrial Control System) et vise à gérer le volume croissant de cybermenaces. La norme permet aux organisations d'améliorer la sécurité numérique de leurs processus et systèmes de contrôle, comme DCS, PLC, SCADA, etc. La norme provient de la série ISO/CEI 27000 et a été entièrement adaptée pour se concentrer sur les environnements de systèmes de contrôle industriels.

L'amélioration de la cybersécurité est une tâche à plusieurs niveaux qui inclut la gouvernance, des politiques de sécurité et des procédures organisationnelles. Dans ce contexte, les solutions Stormshield à l'indice de confiance élevé et certifiées « Restreint UE » peuvent aider les organisations à se protéger des cybermenaces.

Stormshield Network Security (SNS) peut notamment segmenter les réseaux, contrôler les commandes PLC et sécuriser l'accès distant pour maintenance. De plus, lorsqu'il est déployé en complément d'un antivirus (le cas échéant), Stormshield Endpoint Security (SES) fournit une protection en profondeur des stations de travail contre les menaces sophistiquées. SES peut également améliorer la protection des systèmes d'exploitation obsolètes, détecter et gérer les incidents, et assurer une protection contre les attaques par rebond.

Cybersecurity Act

Le règlement européen Cybersecurity Act constitue une réponse à la menace croissante des cyberattaques en renforçant les prérogatives de l'agence européenne pour la cybersécurité (ENISA) et en se dotant d'un cadre européen de certification de cybersécurité. Le cadre européen de certification de cybersécurité vise à renforcer la sécurité des produits connectés, des appareils de l'Internet des objets et des infrastructures critiques au moyen de certificats. Une certification des produits, des procédés et des services qui sera valable dans l'ensemble des États membres. Les 3 niveaux définis (« Élémentaire », « Substantiel » et « Élevé ») permettront aux utilisateurs de déterminer le niveau d'assurance de la sécurité et garantiront que les éléments de sécurité auront été vérifiés de manière indépendante.

Les produits Stormshield ont déjà atteint le niveau « Qualification Standard » décerné par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en France. Sachant que le niveau « Élevé » du cadre européen correspond au niveau de « Qualification Élémentaire » de l'ANSSI – qui est inférieur au niveau de « Qualification Standard » –, les produits Stormshield répondent donc déjà aux attentes de l'ENISA en matière de cybersécurité.

Vous voulez en savoir plus ? C'est parti !

> OBLIGATIONS DE CONFORMITÉ FACULTATIVES

Si elles le souhaitent, les organisations du secteur du transport peuvent se conformer aux normes suivantes pour améliorer leur niveau de cybersécurité. Toutefois, ces normes ne revêtent aucun caractère obligatoire en vertu de la législation actuelle.

Critères Communs / Niveaux d'assurance d'évaluation (EAL3+, EAL4+, etc.)

Les Critères Communs pour l'évaluation de la sécurité des technologies de l'information constituent une norme internationale (ISO/CEI 15408) pour la certification de la sécurité informatique. Cette norme garantit que le processus de spécification, de mise en place et d'évaluation d'un produit de sécurité informatique a été mené de façon rigoureuse, standard et répétable à un niveau correspondant à l'environnement prévu pour l'utilisation. Dans le cadre de cette norme, le niveau d'assurance d'évaluation (Evaluation Assurance Level – EAL3+, EAL4+, etc.) du produit indique avec quel degré de minutie celui-ci (p. ex. un pare-feu) a été testé. Cette certification est reconnue par une trentaine de pays à l'échelle mondiale (en Europe, en Amérique du Nord, en Asie et au Moyen-Orient).

Les produits Stormshield n'ont pas simplement reçu la certification Critères Communs : ils ont atteint le niveau « Qualification standard » beaucoup plus élevé, décerné par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en France. Pour obtenir ce statut à l'indice de confiance très élevé, le produit doit :

- Obtenir une certification de haut niveau avec un objectif de sécurité défini et validé par l'ANSSI
- Obtenir de bons résultats à l'analyse complémentaire effectuée par l'ANSSI, y compris à l'audit du code source du produit.

Veuillez noter que la « Qualification Standard » est un prérequis pour qu'un produit soit classé dans la catégorie « Diffusion Restreinte OTAN » ou « Restreint UE » nécessaire à la manipulation des informations classées.

Technologie de l'information ISO/CEI 27000 – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information

La série ISO/CEI 27000 est une famille de normes de sécurité de l'information qui fournit un cadre reconnu à l'international relatif aux meilleures pratiques de gestion de la sécurité de l'information. Avec son champ d'action très large, cette série s'applique aux organisations de toute taille dans tous les secteurs.

Le système de gestion de la sécurité de l'information (ISMS, Information Security Management System) fournit une approche systématique pour assurer en continu la sécurité de l'infrastructure sensible. Étant donné la nature dynamique de la sécurité et du risque liés aux informations, le concept ISMS intègre un système d'analyse et d'amélioration continues pour répondre aux évolutions des menaces, des vulnérabilités ou des impacts des incidents.

Les produits Stormshield sont conçus pour assurer la sécurité de l'infrastructure sensible. Un journal standard permet aux organisations de centraliser toutes les informations, afin d'identifier les tendances et les vulnérabilités potentielles. Une interface hautement intuitive permet aux utilisateurs de facilement mettre en place les améliorations.

> RÉGLEMENTATIONS PROPRES À CHAQUE PAYS

FRANCE

Loi de Programmation Militaire (LPM)

La Loi de programmation militaire (LPM) fixe les orientations relatives à la politique de défense de la France. Face à la multiplication des cyberattaques menées par des hackers, des terroristes, voire des États, assurer la cyber-résistance des systèmes d'information des Opérateurs d'Importance Vitale (OIV) constitue un axe clairement défini dans la LPM. Elle intègre donc un volet de cybersécurité et liste les OIV répartis dans 12 secteurs d'activité, dont le secteur du transport.

Étant tous qualifiés par l'ANSSI, cette confiance dans les produits Stormshield permettent aux OIVs de déployer ces solutions de sécurité afin d'augmenter le niveau de protection des Systèmes d'Information d'Importance Vitale (SIIV). À titre d'exemple, Stormshield Network Security assure la segmentation des réseaux, la sécurisation des accès distants, l'authentification des utilisateurs et la gestion des vulnérabilités. Déployé en complément d'un antivirus, Stormshield Endpoint Security (SES) propose une protection en profondeur des postes de travail contre les attaques sophistiquées. SES peut également améliorer la sécurité des systèmes d'exploitations obsolètes ; détecter et gérer les incidents et assurer une protection contre les attaques par rebond.

Guides de bonnes pratiques de l'ANSSI

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) est un véritable organe moteur en matière de cybersécurité en France et produit régulièrement des guides de bonnes pratiques. Il ne s'agit pas ici de réglementations à proprement parler mais davantage d'aides à la décision dans la sélection de vos prestataires, de vos solutions de cybersécurité voir de mise en place de ces dernières. De la cryptologie aux postes de travail en passant par les réseaux, une bibliographie riche et passionnante.

> RÉGLEMENTATIONS PROPRES À CHAQUE PAYS

ALLEMAGNE

IT-Grundschutz

IT-Grundschutz est un ensemble de normes du bureau fédéral allemand pour la sécurité de l'information (BSI, Bundesamt für Sicherheit in der Informationstechnik) conçues pour répondre aux exigences relatives au niveau adéquat de sécurité des données/informations. En février de chaque année, l'IT-Grundschutz-Kompendium est publié et explique les dangers et exigences de sécurité pour une thématique liée à la sécurité de l'information.

Normes du bureau fédéral pour la sécurité de l'information (BSI)

Les normes BSI constituent, en Allemagne, un élément de base de la méthodologie IT-Grundschutz. Les normes BSI actuelles sont les suivantes :

- 200-1 (exigences générales pour un système de gestion de la sécurité de l'information)
- 200-2 (exigences de base pour le développement d'un système performant de gestion de la sécurité de l'information)
- 200-3 (toutes les étapes liées aux risques pour la mise en place d'une protection informatique basique)

Loi sur la sécurité informatique (IT-Sicherheitsgesetz) et loi BSI (BSI-Gesetz)

Conformément à la loi sur la sécurité informatique allemande, les opérateurs d'installations/infrastructures critiques dans le secteur du transport doivent atteindre un niveau minimum de sécurité informatique et signaler toute perturbation informatique majeure au BSI. En ce qui concerne ce niveau minimum, la section 8a de la loi BSI a été promulguée par la loi sur la sécurité informatique, qui décrit le niveau minimum en des termes abstraits. En 2016, la loi BSI-Kritisverordnung a également été adoptée pour spécifier quels systèmes critiques sont couverts par les dispositions de la loi sur la sécurité informatique. Cette réglementation couvre également le secteur du transport.

Les produits Stormshield de confiance et certifiés permettent de déployer des solutions de sécurité qui améliorent le niveau de protection des systèmes informatiques. À titre d'exemple, Stormshield Network Security assure la segmentation des réseaux, la sécurisation des accès distants, l'authentification des utilisateurs et la gestion des vulnérabilités. Déployé en complément d'un antivirus (le cas échéant), Stormshield Endpoint Security (SES) propose une protection en profondeur des postes de travail contre les attaques sophistiquées. SES peut également améliorer la protection des systèmes d'exploitation obsolètes, détecter et gérer les incidents, et assurer une protection contre les attaques par rebond. Stormshield Data Security aide à prévenir les fuites de données grâce au chiffrement des informations sensibles.

> RÉGLEMENTATIONS PROPRES À CHAQUE PAYS

ITALIE

Décret 18 maggio 2018, n. 65 (mise en place en Italie de la directive (UE) 2016/1148 - NIS)

La loi établit des mesures pour une sécurité au niveau national, avec notamment la mise en place d'un CSIRT (également appelé CERT), en définissant les obligations des « opérateurs de marchés critiques » du s.c. et des prestataires numériques au niveau des procédures liées aux failles de sécurité, de la coopération internationale sur les problèmes de sécurité et de l'adoption d'une stratégie nationale de cybersécurité.

Les produits Stormshield de confiance et certifiés permettent aux Opérateurs de Services Essentiels (OSE) de déployer des solutions de sécurité qui améliorent le niveau de protection des Systèmes d'Information Essentiels (SIE). À titre d'exemple, Stormshield Network Security assure la segmentation des réseaux, la sécurisation des accès distants, l'authentification des utilisateurs et la gestion des vulnérabilités. Déployé en complément d'un antivirus (le cas échéant), Stormshield Endpoint Security (SES) propose une protection en profondeur des postes de travail contre les attaques sophistiquées. SES peut également améliorer la protection des systèmes d'exploitation obsolètes, détecter et gérer les incidents, et assurer une protection contre les attaques par rebond.

D.P.C.M. 17 febbraio 2017 (orientation sur la sécurité et la cybersécurité nationales italiennes relatives à la technologie de l'information - décret Gentiloni)

La Directive définit l'organisation institutionnelle en charge de la sécurité et la cybersécurité informatiques nationales, en établissant les obligations et responsabilités de chaque entité (CISR, CISR Tecnico, rôle et directives du DIS, Nucleo per la Sicurezza Cibernetica et ses obligations). La Directive établit également les mesures des « opérateurs de marchés critiques » ainsi que les prestataires du secteur de la communication.

D.P.C.M. 27 gennaio 2014 (cadre stratégique national italien pour l'espace cybernétique - QSN)

Le cadre stratégique national pour l'espace cybernétique vise à garantir l'efficacité et l'interopérabilité des ressources dédiées à la défense commune, et la prise en charge de l'intégration complète du cyberdomaine dans le processus de planification de la défense de l'OTAN et dans la doctrine militaire, afin d'assurer le déploiement de fonctionnalités puissantes contre les cyberattaques.

Stormshield Network Security a obtenu la certification « Restreint UE ». Par conséquent, ces produits peuvent être déployés dans des environnements sensibles pour permettre une diffusion sécurisée des informations classées. Cela contribue à l'interopérabilité internationale avec les institutions de l'Union européenne.

> RÉGLEMENTATIONS PROPRES À CHAQUE PAYS

ESPAGNE

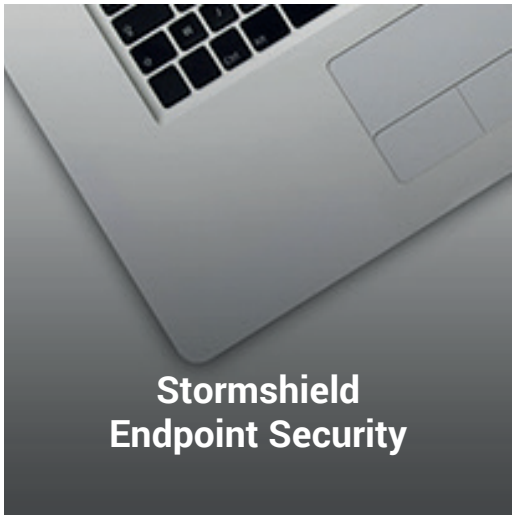
Loi espagnole de protection des infrastructures critiques (Ley PIC)

La loi de protection des infrastructures critiques (Ley PIC 8/2011) est complétée par le décret royal 704/2011. Les deux principaux objectifs de cette norme sont les suivants : répertorier toutes les infrastructures qui fournissent des services essentiels à notre société et concevoir un plan qui comprend des mesures de prévention et de protection efficace contre les menaces possibles dont sont victimes ces infrastructures, tant en matière de sécurité physique que de sécurité des informations et technologies de communication.

Les produits Stormshield de confiance et certifiés permettent à l'infrastructure critique de déployer des solutions de sécurité qui améliorent le niveau de protection des systèmes d'information essentiels. À titre d'exemple, Stormshield Network Security assure la segmentation des réseaux, la sécurisation des accès distants, l'authentification des utilisateurs et la gestion des vulnérabilités. Déployé en complément d'un antivirus (le cas échéant), Stormshield Endpoint Security (SES) propose une protection en profondeur des postes de travail contre les attaques sophistiquées. SES peut également améliorer la protection des systèmes d'exploitation obsolètes, détecter et gérer les incidents, et assurer une protection contre les attaques par rebond.

> POUR CHAQUE PROBLÈME, IL EXISTE UNE SOLUTION STORMSHIELD.

Les produits et solutions Stormshield pour le secteur du transport



> LA CONFORMITÉ NE FAIT PAS TOUT

Le grand nombre de réglementations et normes est devenu un véritable casse-tête pour toutes les organisations. Bien que ce guide fournisse des indications sur les réglementations applicables à chaque industrie, rappelez-vous que la conformité ne fait pas tout. N'oubliez pas que chaque organisation doit cartographier et gérer les risques pour garantir sa propre sécurité.

Crédits photos : ShutterStock© aressy.com