STORMSHIELD

CONFORMITÉ EN MATIÈRE DE CYBERSÉCURITÉ POUR LES ORGANISATIONS DU SECTEUR DE LA SANTÉ

Dans le domaine de la santé, où la disponibilité des services est essentielle, une cyberattaque peut littéralement être une question de vie ou de mort. De plus, les prestataires de soins de santé sont légalement contraints de protéger les données des patients. Alors que les systèmes de santé s'appuient de plus en plus sur les données mobiles, celles-ci ne doivent subir aucune intrusion.

> 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 de la santé 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 public 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 Netwo rk 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.

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 de la santé 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.

Liste de recommandations de l'ENISA

L'agence européenne ENISA a publié une liste de recommandations cyber dans le cadre de marchés publics hospitaliers, que ce soit pour des services, des produits ou des infrastructures. Un document à destination des responsables informatiques des centres hospitaliers.

Les produits Stormshield sont qualifiés et certifiés au plus haut niveau européen, un synonyme de confiance et de robustesse. Ils 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. En déployant une solution qualifiée et certifiée au plus haut niveau européen, vous bénéficiez d'un produit dont la robustesse a été éprouvée lors du processus de certification.

Vous voulez en savoir plus ? C'est parti !

> OBLIGATIONS DE CONFORMITÉ FACULTATIVES

Si elles le souhaitent, les organisations du secteur de la santé 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.

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

ROYAUME-UNI

Data Protection Act 2018

Similaire au RGPD, le Data Protection Act est une loi de protection des données spécifique au Royaume-Uni. Il stipule que les données personnelles doivent être couvertes par « un niveau approprié de protection » selon les risques encourus en cas de faille de sécurité. Cela inclut un niveau de sécurité empêchant toute manipulation non autorisée ou illégale, toute perte accidentelle, toute destruction ou tout endommagement des données.

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.

> RÉGLEMENTATIONS PROPRES À CHAQUE PAYS

FRANCE

Code de la santé publique en France- Article relatif aux hébergeurs de données de santé

L'article L1111-8 du Code de la santé publique vient définir les conditions d'activité des hébergeurs des données de santé à caractère personnel. L'hébergeur et son service d'archivage doivent ainsi mettre en œuvre la sécurisation efficiente des données de santé qui leur seraient confiés.

Les solutions Stormshield vous accompagnent dans la mise en conformité de votre établissement grâce à un ensemble complet de fonctionnalités telles que la sécurisation de vos données avec conformité garantie, même en cas de stockage des données confidentielles dans le Cloud – et ce quelle que soit leur localisation, avec la solution Stormshield Data Security.

Instruction interministérielle n°901/SGDSN

L'instruction interministérielle française n°901 relative à la protection des systèmes d'information sensibles s'applique notamment aux entités publiques ou privées soumises à la réglementation relative à la protection du potentiel scientifique et technique de la nation (PPST) qui mettent en œuvre des systèmes d'information sensibles. Les données traitées sur ces systèmes d'information sensibles, comme les brevets par exemple qui doivent être consignés dans des zones à régimes restrictifs, doivent également porter la mention « Diffusion restreinte ».

Pour prévenir la compromission d'informations sensibles et protéger l'image de l'entité, la solution Stormshield Data Security permet un chiffrement des données de bout-en-bout. Son implémentation cryptographique certifiée EAL3+, qualifiée par l'ANSSI et l'OTAN, est ainsi adaptée à la protection des données de type « Diffusion restreinte ».

Ordonnance n°2020-1407 du 18 novembre 2020 relative aux missions des agences régionales de santé

L'article 1 de cette ordonnance pose l'obligation de déclaration des incidents informatiques aux autorités compétentes de l'État et à l'Agence nationale de santé publique pour toutes les structures de santé, sanitaires et médico-sociales.

Les journaux d'événements proposés par les solutions Stormshield, au titre d'événements de sécurité, font partie des informations essentielles à transmettre aux autorités compétentes en cas d'incidents. L'évolution de la solution Stormshield Endpoint Security répond tout particulièrement à cette problématique lorsque l'attaque est sophistiquée et qu'elle tente de leurrer les moyens de protection. En plus de bloquer proactivement les comportements d'attaque les plus sophistiqués, Stormshield Endpoint Security Evolution fournit les éléments de contextualisation nécessaires à l'investigation poussée des incidents de sécurité.

> RÉGLEMENTATIONS PROPRES À CHAQUE PAYS

FRANCE

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.

Avec l'opus « Sécurité numérique des collectivités territoriales : l'essentiel de la réglementation », retrouvez un guide complémentaire à notre ebook. Un document synthétique, pratique et abordable à destination des élus et des cadres territoriaux chargés d'en garantir l'application et la conformité.

> RÉGLEMENTATIONS PROPRES À CHAQUE PAYS

ALLEMAGNE

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 du domaine de la santé 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. De plus, en 2016, la loi BSI-Kritisverordnung a été adoptée pour spécifier quels systèmes critiques sont couverts par les dispositions de la loi sur la sécurité informatique. Ce décret couvre également le secteur de la santé.

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.

Loi fédérale allemande sur la protection des données (BDSG)

Si des données médicales sont traitées, des mesures appropriées et spécifiques doivent par conséquent être prises pour protéger les intérêts du sujet des données conformément à la section 22 (2) de la loi BDSG. Cette section spécifie les mesures techniques et organisationnelles à prendre lors du traitement de données médicales.

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 constitue une mesure technique appropriée pour garantir le niveau de sécurité adapté selon le risque.

> RÉGLEMENTATIONS PROPRES À CHAQUE PAYS

ALLEMAGNE

Loi sur la santé et l'électronique, et livre V du Code social en Allemagne

La loi sur la santé et l'électronique concerne la communication et les applications électroniques dans le secteur de la santé. Elle comprend une feuille de route concrète pour l'établissement d'une infrastructure télématique sécurisée et l'introduction d'applications médicales. La loi sur la santé et l'électronique est un acte modificatif qui vient amender le livre V du Code social.

Les produits Stormshield aident les organisations à se conformer à cette directive en améliorant la cyber-résistance de leur infrastructure. Stormshield Network Security garantit une protection de pointe avec des fonctionnalités de gestion des menaces unifiées. De plus, Stormshield Endpoint Security accroît le niveau de sécurité de l'antivirus traditionnel en bloquant les menaces sophistiquées. Enfin, Stormshield Data Security aide à se conformer aux exigences de protection des données.

> 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 protéger contre les attaques sophistiquées.

D.P.C.M. 178 del 2015 (dossier médical électronique en Italie - FSE, Fascicolo Sanitario Elettronico)

Le dossier médical électronique est un registre de renseignements médicaux et socio-sanitaires relatifs aux activités cliniques des patients.
Il a pour principal objectif de faciliter l'aide aux patients, en améliorant la synergie des activités d'assistance et des soins de santé. Le respect du droit (également en matière de sécurité) repose sur le RGPD et la garantie relative au FSE.

Les produits Stormshield aident les organisations du secteur de la santé 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 constitue une mesure technique appropriée pour garantir le niveau de sécurité adapté selon le risque.

> RÉGLEMENTATIONS PROPRES À CHAQUE PAYS

ESPAGNE

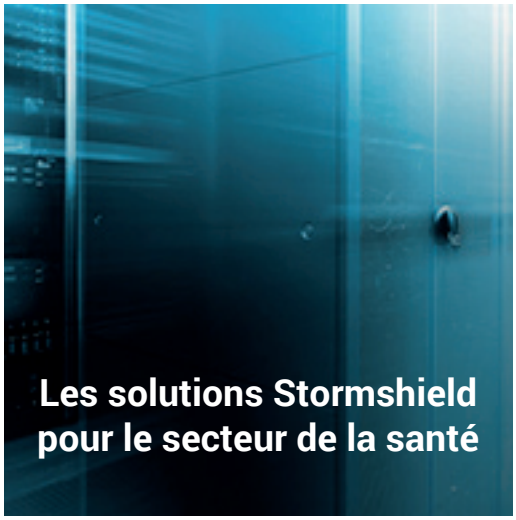
Plan de sécurité national espagnol, Décret royal 3/2010 du 8 janvier

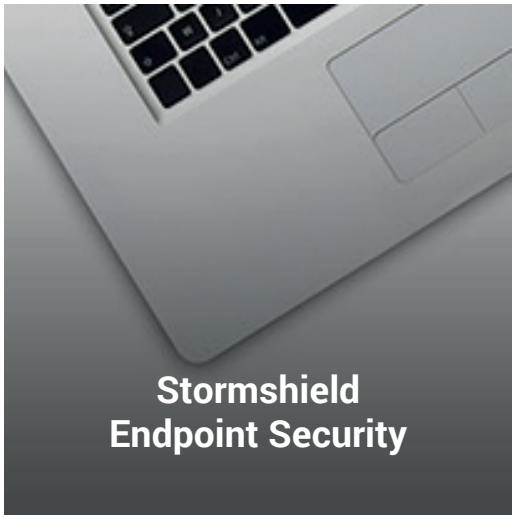
Si un hôpital est considéré comme une entité légale publique (associée à ou tributaire de l'administration gouvernementale générale, des communautés autonomes ou des entités locales), le plan suivant doit s'appliquer dans son intégralité pour les activités non régies par le droit privé.

Les produits Stormshield aident les organisations à se conformer à ce plan en améliorant la cyber-résistance de leur infrastructure. Stormshield Network Security garantit une protection de pointe avec des fonctionnalités de gestion des menaces unifiées. Notre gamme SNS est d'ailleurs la seule gamme européenne qualifiée « Productos Cualificados » et l'unique gamme de pare-feux qualifiée « Productos Aprobados » par le Centre National de Cryptologie espagnol (CCN). De plus, Stormshield Endpoint Security accroît le niveau de sécurité de l'antivirus traditionnel en bloquant les menaces sophistiquées. Enfin, Stormshield Data Security fournit des fonctionnalités de chiffrement des données, qui constitue une mesure technique appropriée pour garantir le niveau de sécurité adapté selon le risque.

> POUR CHAQUE PROBLÈME, IL EXISTE UNE SOLUTION STORMSHIELD.

Les produits et solutions Stormshield pour le secteur de la santé





> 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.