PHILIPS

Rapport

Philips et la cybersécurité

Nous nous engageons à répondre de manière proactive aux préoccupations de nos clients en matière de sécurité et de protection de la vie privée

Janvier 2018

Table des matières

« La cybersécurité est au cœur de la transition vers les soins connectés »

Jeroen Tas
Directeur de l'innovation et de la stratégie, Philips

1. La numérisation des soins de santé – opportunités et menaces

Face au défi du vieillissement de la population, les systèmes de santé actuels peinent à mettre au point des modèles de soins appropriés et abordables. Les soins de santé connectés – rendus possibles par des dispositifs, des applications et des plateformes de santé connectés – sont à l'origine d'un potentiel sans précédent pour transformer les soins de santé et permettre une meilleure santé et de meilleurs soins à moindre coût.

La prolifération de millions d'appareils numériques connectés permet aux utilisateurs et aux réseaux de partager, rechercher, naviguer, gérer, comparer et analyser un flux pratiquement illimité de données qui peuvent être utilisées pour améliorer les résultats des soins. Cet « écosystème » numérique a déjà aidé l'industrie à élargir le portefeuille d'appareils intelligents personnels et axés sur les soins de santé, à stimuler l'innovation et à accroître l'efficacité des services.

À titre d'exemple : l'analyse des dossiers médicaux électroniques et des informations de diagnostic recueillies par les équipements d'imagerie, les moniteurs et les appareils personnels portables renforce le pouvoir de décision des professionnels et permet aux personnes de jouer un rôle plus actif dans la gestion de leur santé personnelle.

Toutefois, l'augmentation exponentielle du volume et des types de données disponibles entraîne également une vulnérabilité accrue à la cybercriminalité – les données relatives aux soins de santé sont la première cible des cybercriminels et ont 10 fois plus de valeur que les seules données relatives aux cartes de crédit.

Les données personnelles contenues dans les dossiers de santé sont très précieuses, car elles peuvent être utilisées, par exemple, à des fins malveillantes, telles que la création de fausses identités ou la présentation de fausses demandes d'assurance.

Les menaces comprennent des attaques de sécurité malveillantes via des virus, des vers et des intrusions de pirates. Les auteurs vont des pirates individuels au crime organisé et même aux États-nations.

Les cyber-attaques telles que celle de WannaCry en mai 2017 montrent que même les organisations les plus grandes et les plus sophistiquées peuvent être vulnérables aux perturbations. Dans ce cas, certains hôpitaux ont même dû rediriger les patients vers d'autres cliniques.

> 100 000 000

de violations de dossiers en 2015

34 % des dossiers compromis sont liés aux soins de santé[1]

Plus de 75 %

de tous les sites Web légitimes contiennent **des vulnérabilités non corrigées**[2]

Deux milliards

de dossiers personnels ont été volés aux États-Unis en 2016, dont **100 millions** étaient des dossiers médicaux[3]

Cible n°1

Les soins de santé sont la cible principale

La récupération d'un dossier médical perdu ou volé peut coûter jusqu'à **363 $ par dossier**[4]

Le coût de la **cybercriminalité** devrait atteindre **2000 milliards de dollars** d'ici 2019[5]

En 2016, la cybercriminalité a coûté à l'économie mondiale plus de **450 milliards de $**[6]

Sources :

1. IBM X-Force Rapport sur les renseignements relatifs aux menaces 2016
2. Symantec
3. CNBC
4. IBM X-Force Rapport sur les renseignements relatifs aux menaces 2016
5. Recherche Juniper
6. CNBC

2. La position de Philips sur la cybersécurité

Philips propose des innovations qui aident les consommateurs et les professionnels de la santé à se connecter plus facilement et à prendre des décisions mieux informées. Certaines des possibilités les plus puissantes et les plus prometteuses en matière d'innovation dans le domaine des soins de santé concernent la recherche sur de grands groupes d'étude et de grands ensembles de données.

La position stratégique et concurrentielle de Philips repose en grande partie sur les **données, l'innovation numérique et la confiance des consommateurs**.

Philips traite un nombre croissant de données relatives à la santé, l'un des types de données personnelles les plus sensibles. **Nos clients demandent des niveaux d'assurance de plus en plus élevés concernant les mesures de sécurité et de protection de la vie privée que nous avons mises en place**. Plus que jamais, nos mesures de protection de la vie privée sont essentielles dans les décisions de faire des affaires avec des partenaires.

Conscient des préoccupations de ses clients et consommateurs, et du rôle essentiel que joue la sécurité dans les écosystèmes numériques interconnectés d'aujourd'hui, Philips s'est engagé à déployer des **plans de sécurité complets** qui garantissent la sécurité des produits, des données commerciales (informations d'entreprise) et personnelles (patients).

Nos plans de sécurité englobent notre **personnel, nos processus et nos technologies**, dans le but de garantir la **confidentialité, l'intégrité et la disponibilité** des données critiques et des systèmes qui les hébergent.

Le concept de **sécurité intégrée** (ou **Sécurité à dessein** au sein de l'UE) – de bout en bout, de la conception à l'assistance en passant par la production – est la clé du succès à long terme de nos produits, services et solutions.

Philips encourage l'adoption cohérente de stratégies pour faire face de manière proactive aux risques et aux menaces, notamment ce que l'on appelle souvent dans le domaine de la cybersécurité **« Les trois péchés capitaux »** :

- **Le risque lié aux mots de passe** : le risque lié à l'absence d'une gestion solide des identités et des autorisations, par exemple l'authentification multifactorielle.
- **Le risque lié au cryptage** : risque lié à l'absence d'un cryptage solide des données, de bout en bout – depuis la source où les données sont générées, sur le réseau et lorsqu'elles résident dans un centre de données – et/ou de solutions efficaces de prévention des pertes de données.
- **Le risque lié à la gestion des correctifs** : risque lié à l'absence d'une gestion efficace des correctifs, créant des vulnérabilités dans les systèmes d'exploitation existants, par exemple.

La sécurité – tout comme la sûreté et la qualité – est une condition préalable à la confiance en la marque Philips. **Les clients et les consommateurs doivent pouvoir compter sur la sécurité, la sûreté et la qualité de nos produits et services** et comprendre l'intérêt de partager leurs données – sinon les avantages pour la santé qui découlent de la connectivité et de l'analyse de grands ensembles de données risquent de ne jamais être réalisés. C'est pourquoi nous continuons à mettre en avant de manière proactive les avantages des technologies de santé connectées et à investir dans des systèmes sécurisés sur lesquels nos clients peuvent compter.

« La sécurité des produits et de l'information est une combinaison d'éducation, de stratégies et de procédures, de sécurité physique et de technologie ».

Michael McNeil
Responsable des services produits et sécurité à l'international, Philips

3. Transparence, conformité et plus encore

Philips met en œuvre la sécurité au sein d'une industrie des dispositifs médicaux fortement réglementée. Les organismes de réglementation tels que la Food and Drug Administration américaine exigent que les versions et les modifications du matériel et des logiciels soient soumises à des méthodes de vérification et de validation rigoureuses afin de garantir que **des normes élevées de sécurité, d'efficacité, de qualité et de performance** sont respectées dans tous les produits et services Philips concernés.

Philips veille au **respect** des normes et réglementations en matière de protection des données et de la vie privée.

Philips s'efforce d'être **ouvert et transparent dans le signalement et la correction des vulnérabilités** et a mis au point un solide processus de divulgation coordonnée des vulnérabilités (précédemment défini comme la divulgation responsable).

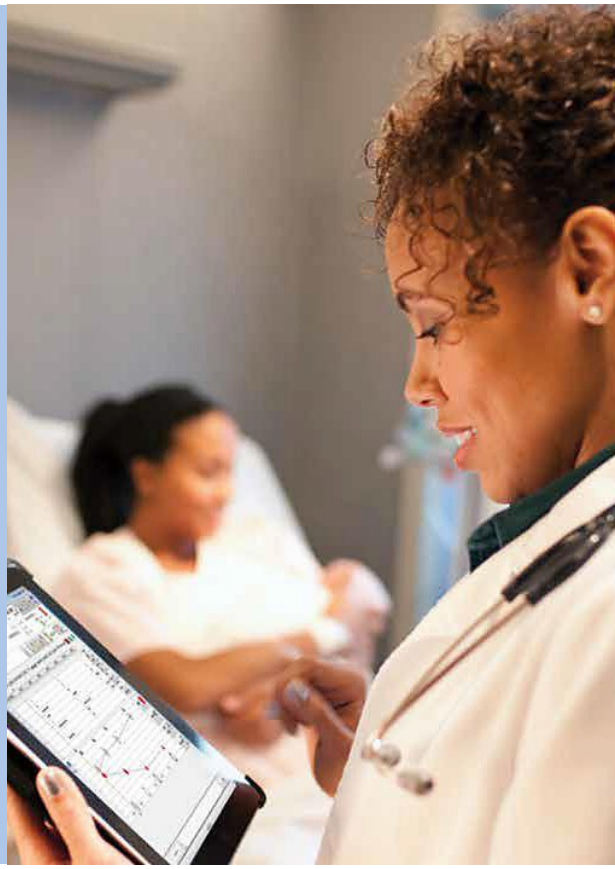
Notre stratégie consiste non seulement à rester au fait des nouvelles vulnérabilités en matière de sécurité et des menaces extérieures potentielles, mais aussi à **prendre nos responsabilités et à collaborer** avec les organismes de réglementation, les partenaires industriels et les prestataires de soins de santé, entre autres, pour combler les failles de sécurité et mettre en place des mesures de protection.

Afin d'harmoniser davantage nos efforts, **Philips participe activement aux principaux groupes industriels** qui s'intéressent à la sécurité ou à la protection de la vie privée. Nous nous efforçons de veiller à ce que les exigences de sécurité appropriées et nécessaires des clients soient incluses dans les normes, les lignes directrices et les initiatives de l'industrie.

Philips soutient les Recommandations pour un partenariat public-privé contre la cybercriminalité du **World Economic Forum**.

« La sécurité des patients dans l'environnement de soins connecté d'aujourd'hui est une tâche que nous prenons tous très au sérieux. Alors que nous faisons tous évoluer nos programmes de cybersécurité, la transparence, la responsabilité et la réactivité doivent être des priorités que nous continuons à maintenir ».

Michael McNeil
Responsable des services produits et sécurité à l'international, Philips



4. Sécurité des produits

Philips prend très au sérieux le risque croissant de menaces de cybersécurité[1] pour ses produits. Nous nous sommes engagés depuis longtemps dans l'effort continu d'amélioration de nos processus et systèmes afin de minimiser les risques pour les patients qui dépendent de nos solutions et services.

Nous sommes tout à fait conscients de la tendance croissante aux cyberattaques sophistiquées dans les industries et, de plus en plus, dans les soins de santé. L'intégration croissante des réseaux hospitaliers, des bases de données cliniques, des dispositifs médicaux et des systèmes de surveillance de la santé des personnes augmente également le potentiel de vulnérabilités en matière de cybersécurité.

Philips a été l'un des premiers à reconnaître qu'une cybersécurité efficace ne consiste plus à protéger la « boîte » ou le produit individuel, mais réside dans une approche systématique qui prend en compte où et comment les appareils sont utilisés. **Chez Philips, la « sécurité intégrée » est un état d'esprit de bout en bout : l'intégration des principes de sécurité commence avec la conception et le développement des produits, en passant par les tests et le déploiement. Elle est suivie de stratégies et de procédures robustes pour le contrôle, des mises à jour efficaces et, si nécessaire, la gestion des réponses aux incidents.**

Pour que nos produits et services résistent aux cyber-menaces, il faut un engagement indéfectible en faveur de l'évaluation des risques et une adhésion au développement de produits basés sur la sécurité. Cela exige un déploiement rapide des technologies de sécurité (telles que le cryptage et la gestion des correctifs) et une amélioration continue. C'est pourquoi nous avons chargé notre Product and Solutions Security Program (Programme de sécurité des produits et des solutions) de créer, d'implémenter et de mettre à jour des approches complètes et efficaces pour répondre aux exigences des clients.

Les principales initiatives de Philips en matière de sécurité des produits sont les suivantes :
Lancement d'une Lancement d'une Product Security Policy (Politique de sécurité des produits) Philips, avancée par l'industrie et accessible au public, consistant en des politiques, des procédures et des normes habilitant l'organisation à mettre en œuvre les meilleures pratiques de sécurité.

La politique décrit notre organisation stratégique et nos procédures pour :

- Maintenir un réseau mondial de professionnels de la sécurité et de la protection de la vie privée dans le cadre de la Product Security Policy (Politique de sécurité des produits) Philips
- Développer et déployer de meilleures pratiques pour nos produits et services
- Guider les activités d'évaluation des risques et de réaction aux incidents concernant les menaces et les vulnérabilités potentielles et identifiées en matière de sécurité et de vie privée
- Régir la sécurité intégrée dans les produits et services au cours de leur cycle de vie, notamment l'évaluation des risques et la réponse aux vulnérabilités identifiées dans les produits et services

Mise en œuvre de normes de sécurité qui respectent ou dépassent les exigences réglementaires actuelles et les meilleures pratiques du secteur, notamment :

- Les exigences en matière de sécurité et de confidentialité des produits et services sont non seulement alignées sur la norme ISO/CEI-800001 recommandée par la FDA, mais ont même servi de base à la norme 80001-2-2.
- Les exigences en matière de sécurité et de confidentialité des services sont alignées sur les normes reconnues telles que NIST 800-53 Rev 4, ITIL v3.1.24 et la série ISO/CEI-27000.
- Création d'informations destinées aux clients, telles que la déclaration de divulgation du fabricant pour la sécurité des dispositifs médicaux, norme du secteur (MDS[2]).
- Soutien aux orientations de la FDA sur la gestion de la cybersécurité des dispositifs médicaux avant la mise sur le marché, et à la gestion de la cybersécurité des dispositifs médicaux après la mise sur le marché par la FDA.

Le Security Center of Excellence (Centre d'excellence pour la sécurité) de Philips partage des informations avec les principaux chercheurs et installations de test en matière de cybersécurité dans le monde entier, et les aide ainsi à éliminer, réduire et atténuer rapidement les cybermenaces.

Surveillance et réponse aux menaces, vulnérabilités et incidents de sécurité :

- Philips surveille en permanence les nouvelles menaces, vulnérabilités et incidents de sécurité, y compris les vulnérabilités identifiées par les fournisseurs de systèmes d'exploitation et autres logiciels tiers, ainsi que par les clients et les chercheurs en sécurité.
- Les Product Security Incident Response Teams (équipes de réponse aux incidents de sécurité des produits) Philips évaluent les incidents de sécurité potentiels et les vulnérabilités découvertes et élaborent des plans de réponse si nécessaire.

Protection contre les logiciels malveillants et gestion des correctifs :

- Les produits qui prennent en charge la protection contre les logiciels malveillants disponibles dans le commerce sont livrés avec un logiciel de protection contre les logiciels malveillants préinstallé, ou avec une documentation client détaillant les paramètres de protection contre les logiciels malveillants spécifique au produit et approuvée par Philips.
- Les produits Philips peuvent utiliser des logiciels tiers, y compris des systèmes d'exploitation comme Microsoft Windows et Linux. Les évaluations de l'impact de ces correctifs par les équipes d'ingénierie des produits Philips commencent généralement dans les 48 heures suivant la prise de conscience par Philips d'une nouvelle vulnérabilité de sécurité ou de la disponibilité d'un correctif.

Une politique de divulgation responsable pour signaler et traiter les vulnérabilités identifiées :

- Nous avons conçu et mis en œuvre une politique de divulgation responsable de ce type, qui a été distinguée comme une pratique recommandée dans le secteur.
- Notre politique de divulgation responsable est accessible au public, avec des canaux de communication clairs pour les clients, les chercheurs et les autres parties prenantes de la communauté de la sécurité.
- Cette politique englobe la surveillance et la réponse aux communications entrantes, l'engagement de suivi, l'évaluation des notifications de vulnérabilité et le suivi du statut, et l'alignement sur les politiques de réponse aux incidents, de remédiation et de prévention.

Philips s'engage à continuer d'innover dans le cadre de mesures stratégiques et efficaces à long terme afin d'instiller davantage l'éthique de la sécurité des produits médicaux. Nous nous réjouissons de poursuivre cette conversation d'une importance capitale, afin de nous aider à atteindre notre objectif d'améliorer des milliards de vies dans le monde.

1. La cybersécurité est l'ensemble des technologies, processus et pratiques conçus pour protéger les réseaux, les ordinateurs, les programmes et les données contre les attaques, les dommages ou les accès non autorisés -http://whatis.techtarget.com/definition/cybersecurity

« Les données sont la nouvelle devise, et le piratage est un modèle économique. Les gains financiers du piratage informatique dépasseront bientôt ceux du commerce mondial de la drogue ».

Stef Hoffman
Responsable de la sécurité des informations, Philips

5. Sécurité des informations des entreprises

La croissance de Philips est alimentée par une technologie innovante à laquelle nos clients font confiance et sur laquelle ils comptent. La conception, le développement et la production de cette technologie sont soutenus par des systèmes informatiques internes sophistiqués.

Face à la menace croissante de la cybersécurité, qui vise ces technologies et les données qu'elles hébergent, l'objectif de l'organisation de sécurité informatique Philips est de protéger les systèmes d'information des entreprises pour assurer :

- **La confiance de nos clients :** renforcer la marque Philips pour qu'elle soit synonyme de sûreté, de qualité et de sécurité
- **Notre capacité à croître :** prévenir la perte d'informations exclusives afin d'assurer la compétitivité à long terme de l'entreprise
- **Nos performances financières :** protéger les actifs des entreprises afin de prévenir les conséquences financières négatives, notamment la perte de clients, de revenus et de profits
- **Notre stabilité opérationnelle :** maintenir un fonctionnement continu en prévenant la dégradation ou la perturbation des infrastructures vitales
- **Notre respect de la réglementation :** veiller à ce que les systèmes d'information respectent ou dépassent toutes les exigences réglementaires

La sécurité informatique ne peut être résolue par la seule technologie. Pour assurer une sécurité informatique globale, il convient de se concentrer sur trois domaines : les personnes, les processus et la technologie (voir page suivante). L'Information Security organization (organisation de sécurité informatique) Philips met en place des contrôles dans ces trois domaines pour garantir les points suivants :

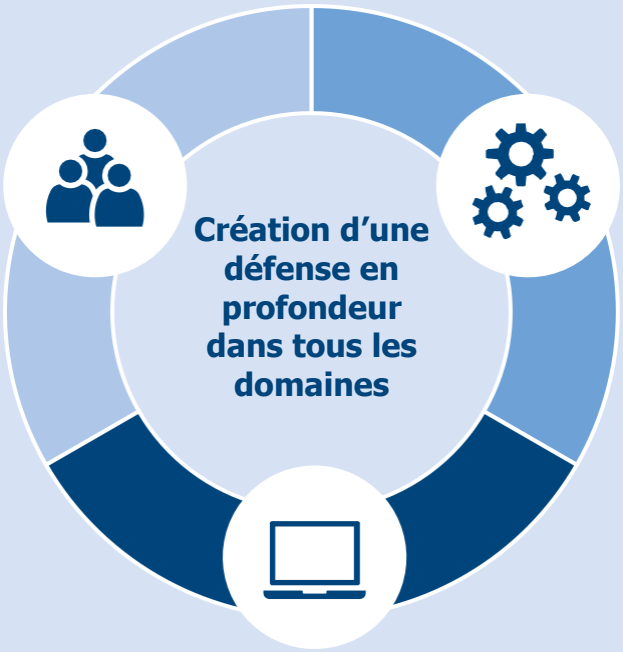
- **Confidentialité :** seules les personnes qui devraient y avoir accès peuvent récupérer les données
- **Intégrité :** les informations ne peuvent être modifiées sans que cela soit détecté
- **Disponibilité :** les informations peuvent être consultées en cas de besoin

Philips relève – et continuera de relever – les défis d'un paysage de menaces en évolution pour sécuriser les systèmes informatiques des entreprises et accroître la confiance de ses clients. L'organisation de sécurité informatique Philips continuera à concentrer ses investissements sur la rétention des meilleurs talents en matière de cybersécurité, à améliorer les outils et les capacités de cybersécurité et à intégrer les meilleures pratiques de sécurité dans tout ce qu'elle réalise.

La sécurité informatique se concentre sur les personnes, les processus et la technologie

Les personnes

Se concentre sur les aspects comportementaux des employés et sur l'amélioration de leur aptitude à la sécurité, développant ainsi une culture de la sécurité



Les processus

Se concentre sur nos processus opérationnels et veille à ce que le risque de sécurité soit évalué et que des mesures d'atténuation appropriées soient intégrées dans le processus afin de réduire ce risque

La technologie

Se concentre sur la compréhension et la surveillance de notre paysage technologique et sur l'apport d'améliorations technologiques pour renforcer notre posture de risque en matière de sécurité

6. Confidentialité

Chez Philips, nous nous sommes engagés depuis longtemps à respecter la vie privée de nos clients, des consommateurs et des autres personnes avec lesquelles nous traitons, notamment les patients. La transparence quant à la manière dont nous traitons les données personnelles contribue à instaurer la confiance. Alors que nous évoluons en une entreprise numérique, il est de plus en plus important de respecter nos normes de protection de la vie privée pour réaliser cet engagement.

L'accent étant mis sur les technologies de la santé, la confidentialité et la sécurité des données sont devenues stratégiquement vitales, car les données relatives à la santé comptent parmi les types de données personnelles les plus sensibles. Notre position concurrentielle dépend fortement de l'utilisation de ces données et la confiance du public est primordiale. **Notre engagement en faveur de la protection de la vie privée va au-delà de la conformité réglementaire**, et nous intégrons des contrôles de protection de la vie privée et des données tout au long du cycle de vie de toutes les données.

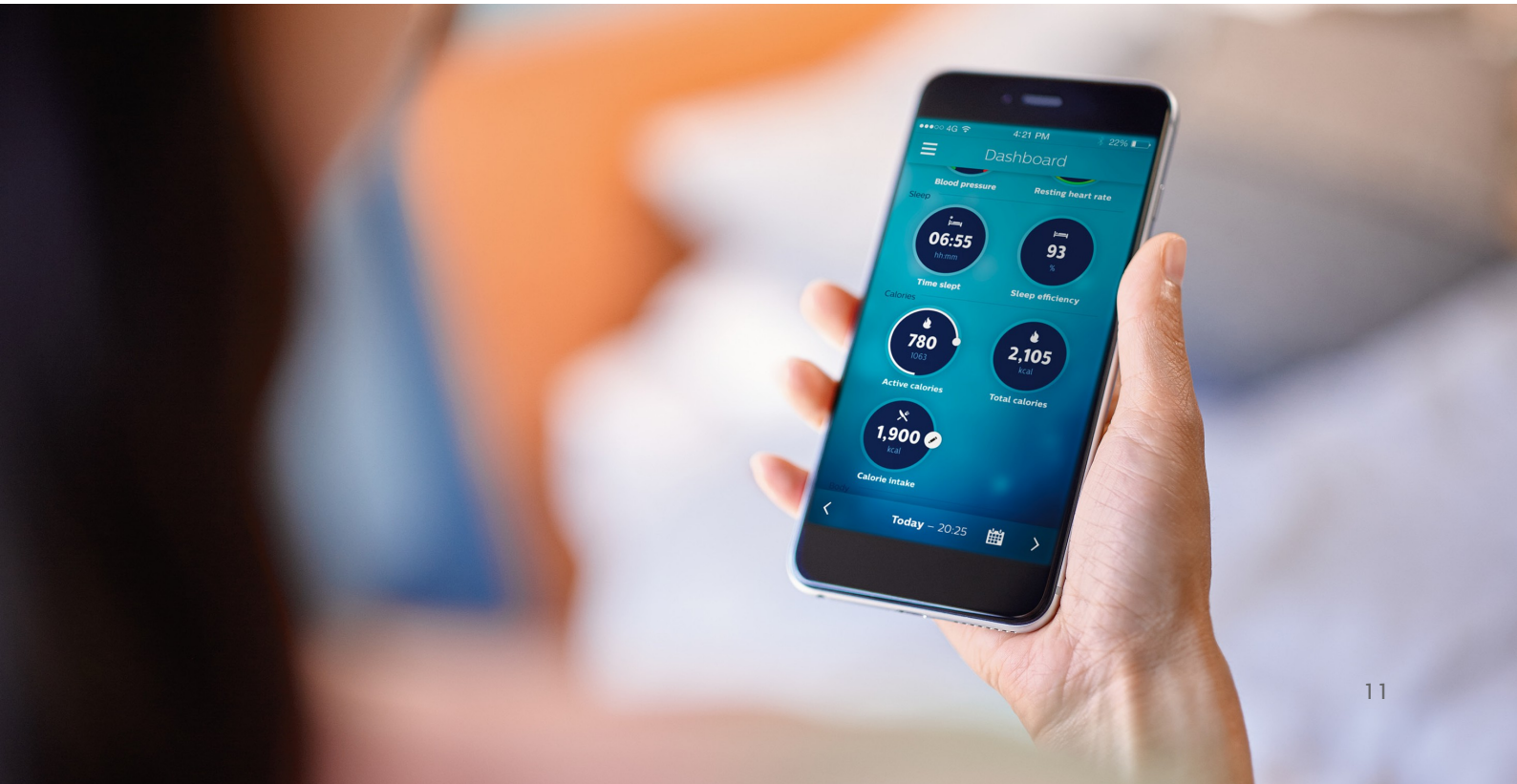
Le respect de la vie privée et la protection des données font partie intégrante de nos **principes généraux d'entreprise** en vertu desquels nous nous soumettons à un certain nombre d'engagements, notamment :

- Mettre en œuvre des Binding Corporate Rules (BCRs – règles d'entreprise contraignantes) (BCRs) qui constituent une base de référence pour la protection de la vie privée au sein de Philips dans le monde entier et permettent le transfert international de données entre les sociétés du groupe Philips.
- Mettre en œuvre un programme de protection de la vie privée et d'une structure de gouvernance qui intègre la protection de la vie privée et des données dans l'entreprise.
- Restreindre la collecte de données et, le cas échéant, obtenir du consentement des personnes.
- Informer les personnes de la manière dont les données collectées seront utilisées et leur permettre d'exercer leurs droits.
- Prendre les mesures appropriées pour maintenir l'exactitude et la pertinence des données.
- Protéger les données à caractère personnel grâce à des mesures de sécurité appropriées.

En tant qu'entreprise mondiale, Philips doit tenir compte de toutes les lois nationales sur la protection de la vie privée et des données. Nos BCRs et notre programme de protection de la vie privée visent à garantir le respect de la vie privée au sein de Philips dans le monde entier, y compris là où les lois sur la protection de la vie privée sont absentes.

Philips s'engage à respecter des normes de sécurité élevées et à gérer les données de manière responsable en appliquant les principes de la **« confidentialité par conception »**. Cette approche vise à intégrer des contrôles de protection de la vie privée et des données tout au long du cycle de vie des données, depuis le stade de la conception jusqu'au déploiement, à la collecte, à l'utilisation et à l'élimination finale des données.

Pour faire progresser les soins de santé rendus possibles par les big data, nous devons favoriser la confiance et en expliquer la valeur aux personnes. Nous devons garantir le droit fondamental à la vie privée et, grâce à notre engagement en faveur de normes de sécurité élevées et d'une gestion responsable des données, nous pouvons réduire la peur et le doute et offrir une valeur encore plus grande aux consommateurs grâce à une innovation permanente.



7. Structures et mécanismes en place

- Les Binding Corporate Rules (**BCRs – Règles d'entreprise contraignantes**) sont des règles internes relatives au traitement des données à caractère personnel au sein de Philips, qui sont également connues sous le nom de Privacy Rules (Règles de confidentialité) de Philips. Les Privacy Rules (Règles de confidentialité) de Philips sont largement basées sur les exigences de l'UE en matière de protection des données et les principes de confidentialité de l'OCDE, et prescrivent un robuste cadre de protection des données au sein de notre organisation. Les Privacy Rules (Règles de confidentialité) de Philips fixent des exigences globales en matière de protection des données qui s'appliquent à Philips dans le monde entier et permettent la circulation internationale des données personnelles au sein de Philips.

- Les **fournisseurs** qui traitent des données personnelles au nom de Philips doivent accepter de se conformer à des exigences strictes, comme le reflètent nos BCRs.

- Nous disposons de centres d'excellence dédiés à la protection de la vie privée, à la sécurité des produits et à la sécurité de l'information. Le Global Privacy Office (**Bureau international de la protection de la vie privée**) **de Philips** aide et soutient le personnel de Philips quant au respect des obligations en matière de protection de la vie privée et établit le cadre mondial pour le respect de la vie privée et la gestion des risques.

- Le Product Security & Services Office (**Bureau de sécurité des produits et services**) **de Philips** régit l'intégration de la sécurité dans les produits et services tout au long de leur cycle de vie. Cela comprend les évaluations des risques de sécurité des produits, les évaluations de vulnérabilité et de pénétration indépendantes des projets, les formations spécialisées en sécurité des produits et les activités de réponse aux vulnérabilités identifiées dans les produits et services existants qui sont pris en charge.

- Nous adoptons une approche globale, de bout en bout, de la sécurité des produits et de l'information. Nous avons mis en place des processus et un cadre pour garantir que chaque étape du cycle de vie du développement des produits est réalisée avec un niveau élevé de confidentialité et d'intégrité. Dans le cadre de notre Secure Product Development Life Cycle **(Cycle de vie sécurisé de développement de produits)**, nous surveillons en permanence les vulnérabilités et validons les correctifs, activités qui sont soutenues par notre Security Center of Excellence – Centre d'excellence pour la sécurité.

- Nous avons mis en place un **programme de formation pour tous les employés** concernant la protection des informations et des données personnelles et les étapes à suivre pour se conformer aux Privacy Rules (Règles de confidentialité) de Philips et aux lois applicables. Les employés qui manipulent des données sensibles reçoivent une formation supplémentaire basée sur leur rôle afin de garantir une manipulation correcte des données. Nous avons également des programmes de formation spécialisée en matière de sécurité pour nos équipes de développement.

- En ce qui concerne nos **plateformes numériques HealthSuite**, nous sous-traitons l'hébergement de certains services techniques à des fournisseurs tiers de niveau 1 (tels qu'Amazon, salesforce.com). Ces fournisseurs doivent se faire certifier chaque année par des auditeurs indépendants selon la norme ISO/CEI 27001 et d'autres normes de sécurité et de confidentialité pertinentes (telles que HIPAA/HITECH, SSAE No. 16, NIST SP800-53) le cas échéant.

8. Pour de plus amples informations

Informations sur la sécurité des produits Philips ›

Page Web de la politique de confidentialité de Philips ›

Annexe :

Déclaration sur la sécurité des produits

Déclaration sur la sécurité des produits

Ce document résume la position de Philips sur la sécurisation de nos produits, services, applications et systèmes et décrit nos processus pour fournir des produits avec une **sécurité intégrée**.

Contexte

Chez Philips, nous reconnaissons que la sécurité des soins de santé, de la santé personnelle et des produits et services de consommation à domicile de Philips constitue une partie importante de votre planification de la sécurité. Nous nous engageons à vous aider à maintenir la confidentialité, l'intégrité et la disponibilité des données personnelles, des données commerciales et des produits matériels et logiciels Philips qui créent et gèrent ces données.

Les menaces pesant sur la sécurité des appareils et des informations personnelles et médicales continuent de s'accroître. Ces menaces comprennent des attaques de sécurité malveillantes via des virus, des vers et des intrusions de pirates. Les gouvernements du monde entier ont promulgué des lois pour criminaliser nombre de ces cyberattaques et pour protéger les informations de santé identifiables individuellement (par exemple, US-HIPAA, Canada-PIPEDA, législation générale sur la vie privée en vertu de la directive européenne 95/46/CE, Japon-PIPA, et autres).

Pour respecter notre engagement en matière de sécurité, nous, chez Philips, avons mis en place un programme mondial visant à :

- Développer, déployer et prendre en charge des fonctions de sécurité avancées pour nos produits et services.
- Gérer les événements de sécurité sur le terrain. Philips participe à des collaborations entre l'industrie et le gouvernement afin de garantir que les innovations de produits et les informations cliniques sont produites et disponibles au plus haut niveau de qualité, de disponibilité et de confidentialité.

Nous mettons en œuvre la sécurité dans le cadre d'une industrie des dispositifs médicaux fortement réglementée et du climat mondial. Les réglementations gouvernementales (par exemple, celles de la Food and Drug Administration américaine) exigent que les modifications apportées au matériel et aux logiciels soient soumises à une vérification et une validation rigoureuses afin de garantir le respect de normes élevées de sécurité et de performance dans tous les dispositifs médicaux Philips[1]. De même, Philips s'efforce de garantir le même niveau élevé pour les produits de santé personnels, les innovations domestiques et les services.

Organisation

Philips opère dans le cadre d'une politique globale de sécurité des produits régissant la conception pour la sécurité dans la création de produits et de services, ainsi que l'évaluation des risques et les activités de réponse aux incidents pour les vulnérabilités identifiées dans les produits existants. Le responsable de la sécurité des produits à l'international supervise la gouvernance et la conformité de cette politique, en rendant compte directement au responsable de l'excellence des produits et de l'innovation de Philips. Sous la direction du programme mondial de sécurité des produits, Philips a mis en place et développé des capacités comprenant la surveillance mondiale, la remontée des cas, une réaction rapide et une visibilité totale de la gestion des problèmes de sécurité.

Table des matières

L'écosystème connecté/interconnecté

La prolifération de millions d'appareils numériques connectés permet aux utilisateurs et aux réseaux de partager, rechercher, naviguer, gérer, comparer et analyser un flux de données pratiquement illimité. Cet « écosystème » numérique a aidé l'industrie à élargir le portefeuille d'appareils intelligents personnels et axés sur les soins de santé, à stimuler l'innovation et à accroître l'efficacité des services. Il également considérablement augmenté le potentiel d'exposition aux vulnérabilités et aux cyberattaques.

Les produits et services interconnectés, interopérables et télécommandés sont en plein essor dans notre secteur. Certaines zones qui se présentent comme particulièrement vulnérables sont :

- Les réseaux de fournisseurs
- Les dispositifs de santé personnels
- Les services à distance
- Le stockage de données sensibles
- Les données sensibles en mouvement

La protection des réseaux de clients et des données personnelles/patientes privées au sein de l'écosystème est de la plus haute importance. Pour relever ce défi, les équipementiers tels que Philips doivent adopter une vision stratégique et intégrée de la sécurité des produits et établir un programme complet de cybersécurité basé sur les risques.

Internet des objets (IdO)

Le paradigme de l'« Internet des objets » (IdO) envisage l'interconnexion et la coopération généralisées des objets intelligents sur l'infrastructure Internet actuelle et future[2]. Cette révolution dans l'échange de données permet aux gens de vivre plus sainement en utilisant des dispositifs connectés tels que des tablettes, des vêtements et des appareils portatifs pour contrôler leur propre santé de manière très personnalisée. Par exemple, Philips, en collaboration avec des partenaires de l'industrie, a développé notre plateforme numérique HealthSuite, qui permet aux appareils et applications IdO de fonctionner en conjonction avec des ensembles approfondis de données. La plateforme numérique HealthSuite offre à la fois une infrastructure native sur le cloud et les services de base nécessaires pour développer et faire fonctionner une nouvelle génération de dispositifs et d'applications de santé connectés et sécurisés.

L'analyse des dossiers médicaux électroniques et des informations de diagnostic recueillies par les équipements d'imagerie, les moniteurs et les appareils personnels portables renforce le pouvoir de décision des professionnels et permet aux patients de jouer un rôle plus actif dans la gestion de leur santé personnelle. Ces innovations transforment non seulement les soins aux malades chroniques, mais aussi à ceux qui sont et veulent rester en bonne santé.

Les applications, services et matériels mobiles de prochaine génération qui fonctionnent dans cet environnement en évolution rapide seront soumis à une analyse de risque rigoureuse ainsi qu'à des tests de pénétration de la sécurité. Les nouveaux dispositifs seront protégés par un cadre de défense sécurisé qui identifiera les utilisateurs, autorisera le consentement et suivra l'activité des utilisateurs pour garantir la confidentialité des données.

Principaux éléments du programme de sécurité des produits Philips

Dans un écosystème de soins de santé connecté et interopérable, le potentiel d'exposition aux vulnérabilités et aux attaques est important. Cette réalité incite Philips à consacrer des ressources importantes pour atténuer ces menaces. Des années de travail en tant que leader industriel dans le domaine des capacités de sécurité et de l'innovation des produits suggèrent qu'il existe cinq éléments essentiels à un programme de sécurité réussi.

1. Gouvernance
2. Test
3. Divulgation coordonnée des vulnérabilités
4. Nomenclature des logiciels
5. Feuille de route des échéances

Gouvernance	• **Alignement organisationnel** • **Leadership réfléchi (partage, apprentissage)** • **Faire appliquer les principaux facteurs de risque pour la sécurité des produits** • Politique et qualité **« Joindre le geste à la parole »**, évaluation des risques, développement sécurisé, analyse des codes, suivi, formation, réponse aux événements
Test	• **Test de pénétration** – Pirates informatiques éthiques • **Intégré dans l'évaluation des risques, le Cycle de vie de développement sécurisé (SDLC), l'embarquement et la maintenance** • Cas d'utilisation standardisés et outils pour des résultats communs et comparables
Divulgation coordonnée des vulnérabilités	• **Intégré dans la politique** et les processus de traitement des plaintes des clients Tirer parti de processus efficaces de gestion des réponses aux incidents
Nomenclature des logiciels	• **Suivi continu de la nomenclature des logiciels (SBOM)** pour les nouvelles vulnérabilités et les mises à jour des logiciels de sécurité • **Formation** et pratiques intégrées dans le continuum SDLC (pré-commercialisation, post-commercialisation)
Feuille de route des échéances	• **Historique des produits et gestion du cycle de vie de la SBOM** • **Innovation continue – Évaluation et suivi** du programme

Gouvernance

La coordination de la direction exécutive au sein de Philips garantit l'adhésion nécessaire pour aller de l'avant avec succès. Cette équipe interne assure une surveillance continue, en élaborant des stratégies et une structure pour assurer une mise en œuvre réussie des attributs essentiels du programme de sécurité des produits, notamment les politiques, les évaluations des risques, les tests de sécurité, les communications, les exigences des parties prenantes, la gestion des incidents, les mesures et une feuille de route de maturité pour l'amélioration continue.

L'équipe coordonne les efforts des acteurs externes de l'écosystème de la cybersécurité (clients, fournisseurs, régulateurs, organismes de normalisation, groupes industriels et chercheurs, entre autres) par un dialogue permanent. Cet effort est extrêmement productif pour établir des relations clés et promouvoir les meilleures pratiques de l'industrie en matière de sûreté et de sécurité des dispositifs personnels et médicaux. Par exemple, Philips est l'un des deux fabricants d'appareils médicaux membres du groupe de travail sur la cybersécurité du ministère américain de la santé et des services sociaux (HHS).

La gouvernance d'une stratégie globale de gestion des risques est au cœur du programme et de la mission de Philips la mission de la Sécurité des produits Philips. Cette stratégie régit un processus holistique de gestion des risques visant à prévenir, atténuer et/ou remédier aux risques pour la sécurité des produits avant et après leur mise sur le marché, en mettant notamment l'accent sur trois domaines de risque fondamentaux mais à fort impact, communs à l'industrie, risques que nous appelons les « trois péchés capitaux » :

1. Le risque lié aux mots de passe
– le risque lié à l'absence d'une gestion robuste des mots de passe

2. Le risque lié au cryptage
– le risque lié à l'absence d'un cryptage éprouvé des données et/ou de solutions efficaces de prévention des pertes de données

3. Le risque lié à la gestion des correctifs
– le risque lié à l'absence d'une gestion efficace des correctifs

Philips souligne que l'adoption cohérente de stratégies visant à traiter de manière proactive les risques des « trois péchés capitaux » et d'autres domaines clés de risques évalués est essentielle pour assurer la sécurité des produits et des services et réduire les expositions potentielles aux violations de données, aux vulnérabilités des tiers et aux sanctions des institutions réglementaires et des clients.

Test

Première dans l'industrie des dispositifs médicaux, Philips a créé un Security Center of Excellence (SCoE – Centre d'excellence pour la sécurité) pour développer des produits « cyber-résilients ». Au SCoE, une équipe dévouée de pirates éthiques, ou « ninjas de la sécurité », effectue en permanence des tests de vulnérabilité et de pénétration pour identifier de manière proactive les faiblesses des produits. Complétant et renforçant les tests de sécurité des produits effectués par les équipes d'ingénierie et de développement des produits Philips, les processus et résultats des tests SCoE sont définis dans des scénarios de cas d'utilisation standardisés pour une approche de réponse commune. Ces derniers sont ensuite exploités dans l'ensemble de notre entreprise mondiale Philips et intégrés dans l'évaluation des risques, le cycle de vie de développement sécurisé (SDLC) et les procédures de maintenance.

Les tests de sécurité des produits et services de Philips couvrent une grande variété de tâches de cybersécurité, notamment :

- Tests de vulnérabilité de la sécurité et de pénétration
- Évaluations des risques de sécurité
- Analyse du code source de la sécurité
- Engagements de tiers fournisseurs
- Tests techniques de sécurité des produits du Ministère américain de la Défense (US DoD)
- Formation à la sécurité adaptée à des rôles uniques, notamment l'architecture, le développement et les tests de produits
- Validation des outils
- Évaluation des outils
- Surveillance des menaces
- Mesures pour le développement de produits

Divulgation coordonnée des vulnérabilités

Le développement d'un programme coordonné de divulgation des vulnérabilités a commencé par la création d'une politique de divulgation coordonnée des vulnérabilités (initialement intitulée Divulgation responsable) pour rassurer les clients sur le fait que des efforts appropriés seront faits pour réparer toute vulnérabilité et prévenir les dommages futurs.

De même, il est important de traiter tous les incidents de sécurité avec un sentiment d'urgence et de sensibilité. Un processus formel de gestion des réponses aux incidents a été mis en place, qui comprend la documentation de toutes les communications, l'ouverture d'un programme de mesures correctives, l'élaboration d'une solution et la rédaction d'un rapport d'incident.

Les vulnérabilités confirmées font l'objet d'un rapport direct aux agences gouvernementales telles que le DHS américain (programme ICS-CERT) et sont ensuite communiquées au public par la presse. Les lignes directrices de la FDA américaine sur la gestion de la cybersécurité des dispositifs médicaux avant et après la mise sur le marché (28/12/16) fournissent des orientations sur les principes clés qui sont applicables dans la pratique et en coopération avec d'autres entités et processus gouvernementaux. La transparence est la clé.

Philips a été le premier grand fabricant d'appareils médicaux à concevoir et à mettre en œuvre une politique coordonnée de divulgation des vulnérabilités et reste aujourd'hui un leader industriel mondialement reconnu, dont la politique s'appuie sur des processus pleinement développés et ayant atteint leur maturité opérationnelle. Lorsque les médias attirent l'attention du public sur des incidents de sécurité, Philips est souvent montré du doigt comme un fabricant prêt à s'attaquer à des problèmes difficiles.

« Philips a été le seul fabricant de moniteurs pour bébés à être félicité pour avoir répondu aux **alertes de vulnérabilité** ».
— Forbes

« Nous applaudissons l'engagement de Philips à corriger cette vulnérabilité et leur protocole établi pour traiter les vulnérabilités des **produits à venir** ».
— ARS Technica

« Philips a été **« la plus réactive »** de toutes les entreprises pour remédier à cette lacune ».
— Wall Street Journal

En relation : voir la section « **Suivi et réponse aux incidents et aux vulnérabilités** »

Nomenclature des logiciels (SBOM)

Les entreprises (dont Philips) qui dépendent de l'intégration de logiciels tiers s'exposent à des risques cachés en programmant un code qui n'est pas le leur. Pour préparer la législation en cours sur ce sujet au niveau mondial, la création d'une nomenclature des logiciels (SBOM) pour chaque produit est essentielle. Elle identifie et décrit les composants des logiciels libres et tiers et permet aux organisations de réagir rapidement aux éventuelles vulnérabilités/violations de la sécurité.

Philips prend la tête de l'industrie pour intégrer une SBOM dans le cycle de vie de développement sécurisé (SDLC) de chaque produit Philips. Nous allons mettre en place des processus et des procédures pour garantir l'intégrité de tous les logiciels, micrologiciels ou produits développés pour nos clients.

En relation : voir la section "Programme de gouvernance et de conformité Open Source Philips (gouvernance de la SBOM)"

Feuille de route des échéances

L'intégration de la sécurité des produits dans le développement de nouveaux produits et le déploiement cohérent des processus de sécurité des produits dans l'ensemble du portefeuille ouvrent la voie à un avenir gérable. Le but et l'intention d'une feuille de route de maturité sont de mesurer et d'améliorer les processus et les capacités organisationnelles de Philips. In fine, notre désir est d'atteindre de meilleurs niveaux de maturité en matière de sécurité des produits avec le lancement de nouveaux produits, les opérations de service en cours et la gestion du cycle de vie après la mise sur le marché.

Dans le cadre de cet effort, Philips se concentre sur une stratégie de sécurité globale de gestion du cycle de vie des produits. Elle commence par une évaluation et une surveillance des produits de base ou anciens installés afin de détecter l'obsolescence du système d'exploitation, les incompatibilités et les vulnérabilités du matériel et des micrologiciels, puis permet une maintenance/mise à jour et une planification du cycle de vie continues et opportunes.

La sécurité des produits Philips en action

Évaluation de la sécurité des produits / conception des produits

Philips procède de manière proactive à des évaluations internes de la sécurité des produits afin d'identifier les éventuelles faiblesses en matière de sécurité. Fortes de ces informations, nos équipes d'ingénieurs définissent souvent les changements de configuration et les efforts de ré-ingénierie qui permettront de renforcer le système contre les menaces extérieures. Ces mêmes informations déterminent également les exigences de conception de la sécurité des nouveaux produits, intégrés dans les processus de cycle de vie de développement sécurisé de Philips pour tous les produits et services. La Politique de sécurité des produits Philips exige des objectifs de **sécurité intégrée** dans le cadre de tous les efforts de création de nouveaux produits.

Suivi et réponse aux incidents et aux vulnérabilités

Les groupes d'ingénierie des produits au sein de Philips surveillent en permanence les nouvelles vulnérabilités de sécurité, y compris celles identifiées par des fournisseurs tiers de logiciels et de systèmes d'exploitation et celles signalées par les entreprises de santé. Un réseau mondial de responsables de la sécurité des produits et leurs équipes collectent et gèrent les informations et traitent les vulnérabilités identifiées qui peuvent affecter les produits et solutions Philips.

Lorsque des événements à risque, des attaques de cybersécurité ou des incidents sont détectés ou signalés, les Product Security Incident Response Teams (équipes de réponse aux incidents de sécurité des produits) Philips évaluent chaque incident réel ou potentiel à l'aide d'une évaluation explicite de la menace/vulnérabilité/risque. Puis elles coordonnent une réponse unifiée avec les équipes de Philips, communiquent le statut et assurent un suivi pour enquêter sur les événements de sécurité et y remédier conformément à notre cadre de la Product Security Policy (Politique de sécurité des produits).

Cycle de vie de développement sécurisé de produits Philips (SDLC) – Sécurité à dessein

Les tendances de l'industrie ont montré que les cyber-attaques se déplacent vers la couche application des produits et constituent une menace importante pour les clients et les informations des patients sur l'Internet des objets (IdO). Selon les données recueillies par l'Internet Storm Center, plus de 70 % des attaques sur les réseaux visent la couche applicative. Pour renforcer la résilience de ses produits et services, Philips renforce son processus de réalisation de produits avec des capacités, des composants et des techniques, notamment des pratiques conformes aux normes ISO telles que la norme ISO 27034. Il s'agit d'un moyen pratique et éprouvé d'intégrer la sécurité et la confidentialité dans le processus de développement de logiciels.

Grâce à cette méthodologie, les exigences et les contrôles sont abordés à chaque phase du cycle de vie de développement sécurisé, notamment l'utilisation de l'évaluation des risques pour la sécurité des produits (PSRA), les processus d'évaluation de la confidentialité (PIA), l'analyse du code statique, l'analyse de la nomenclature des logiciels tiers (SBOM), les tests de pénétration éthiques et la formation continue sur la sécurité des produits dans toute l'organisation Philips. Si les outils et les processus sont essentiels pour le SDLC de Philips, la sécurité à dessein est un état d'esprit qui nécessite une approche de bout en bout qui commence par l'architecture et la conception de haut niveau et se poursuit par le codage, les tests et l'assistance post-commercialisation.

Programme de gouvernance et de conformité Open Source Philips (gouvernance de la SBOM)

La plupart des logiciels construits aujourd'hui intègrent des composants open source et d'autres composants commerciaux disponibles sur le marché. Ces composants tiers peuvent introduire des vulnérabilités dans un produit dont le fabricant n'a pas connaissance. Une « nomenclature des logiciels » (SBOM) documente soigneusement les outils utilisés pour construire une application et identifie exactement quels composants tiers sont inclus. Cela aide les organismes de sécurité à réagir rapidement et précisément aux risques potentiels.

De nombreux fabricants ne disposent pas d'une liste de nomenclatures précise pour chacun de leurs produits. Sans liste précise, ils n'ont pas une bonne compréhension des vulnérabilités associées aux composants du produit. Sans information sur les produits SBOM, et face à un problème de vulnérabilité, il n'existe pas de moyen facile d'identifier le code affecté et d'introduire une solution. Une réponse souple est donc extrêmement difficile.

La législation américaine en cours d'élaboration vise à assurer la sécurité des logiciels des produits. La Cyber Supply Chain Management and Transparency Act (loi sur la gestion et la transparence de la chaîne d'approvisionnement électronique) exige que les agences gouvernementales obtiennent des nomenclatures logicielles pour tout nouveau produit qu'elles achètent. Il faudra également obtenir des SBOM pour « tout logiciel, micrologiciel, ou produit contenant un composant binaire tiers ou open source[1] ».

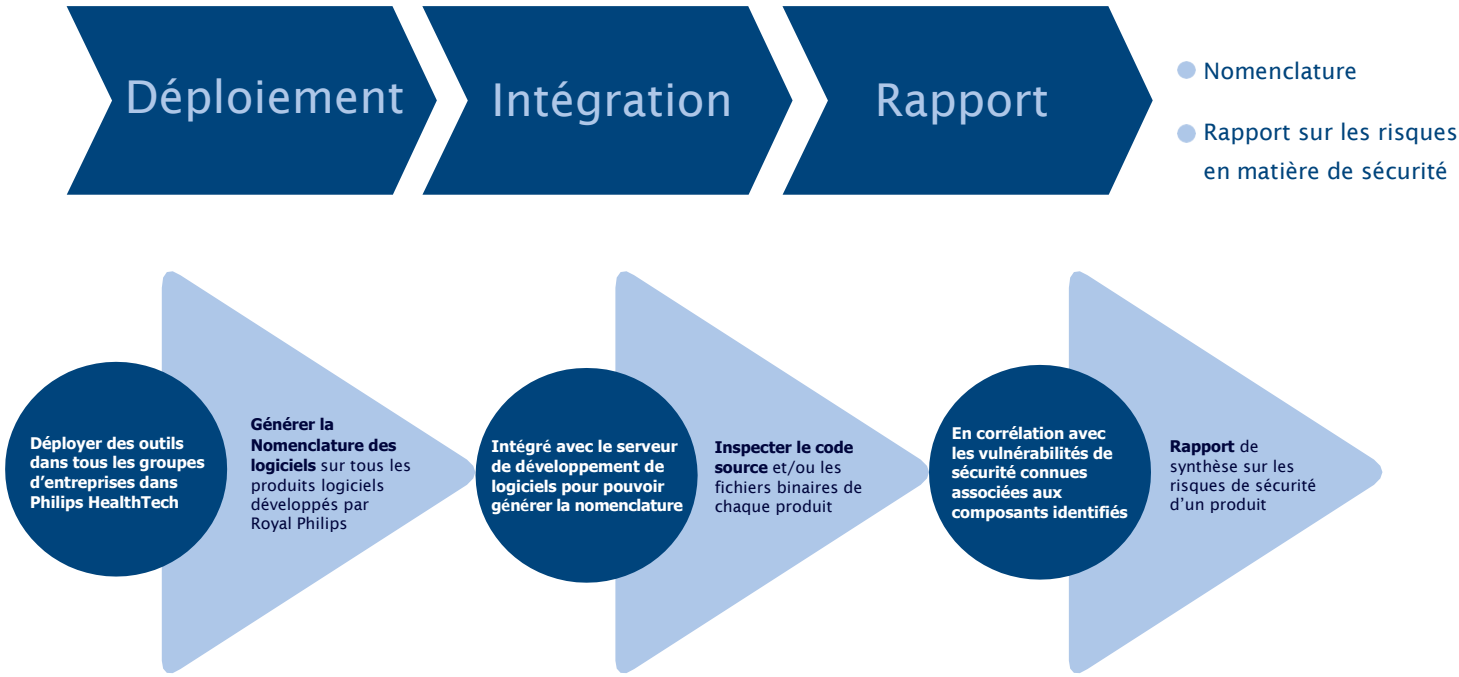
En conséquence de cette législation en instance, des exigences sont adoptées pour la gouvernance et la divulgation des vulnérabilités ou défauts de sécurité des logiciels libres et tiers, comme celles adoptées par l'administration américaine des anciens combattants et définies dans le document 800-53 (NIST 800-53) du National Institute of Standards and Technology des États-Unis.

NIST 800-53 est une publication américaine qui recommande des contrôles de sécurité pour les systèmes informatiques et les organisations fédérales, et documente les contrôles de sécurité pour tous les systèmes informatiques fédéraux américains, à l'exception de ceux conçus pour la sécurité nationale[2].

Philips est en avance sur ces exigences grâce à notre programme de gouvernance SBOM qui comprend les trois phases suivantes :

- **Déploiement** – Générer la « Nomenclature des logiciels » sur tous les produits logiciels développés par Philips. Ceci est réalisé en déployant les outils SBOM dans tous les groupes d'entreprises.
- **Intégration** – Intégrer l'outillage et les processus SBOM dans le processus de développement/construction de logiciels. Inspecter le code source et/ou les binaires de chaque produit.
- **Rapport** – Créer un résumé des risques de sécurité pour chaque produit. Ensuite, il est nécessaire de corréler ce résumé avec les vulnérabilités de sécurité connues associées aux composants identifiés.

Approche de la gouvernance et de la conformité des logiciels Open Source



L'identification et la description des composants de logiciels libres et tiers au sein d'un portefeuille de produits permettent de réagir rapidement aux éventuelles vulnérabilités/violations de la sécurité. Les sept éléments clés suivants sont associés à un programme SBOM réussi :

1. Exigences relatives au document SBOM
2. Intégrer SBOM dans le processus de cycle de vie du développement logiciel, y compris la mise à jour et la maintenance
3. Identifier les vulnérabilités de la SBOM et les problèmes de licence et intégrer les résultats dans les évaluations des risques de sécurité, et prendre des mesures correctives en fonction des risques évalués
4. Inclure la SBOM dans toute la documentation pertinente sur le produit
5. Surveiller en permanence le SBOM pour détecter les nouvelles vulnérabilités et les mises à jour des logiciels de sécurité
6. Mettre à jour la SBOM dans les documents relatifs aux produits et les évaluations des risques de sécurité
7. Ajuster l'exigence globale de la SBOM en fonction des changements de la réglementation gouvernementale

Le processus SBOM de Philips Le processus SBOM de la Sécurité des produits Philips sera intégré sera intégré dans le cycle de vie de développement du système pour chacun de nos produits, conformément à la Product Security Policy (Politique de sécurité des produits) Philips. Les nouveaux systèmes répondront à ces attentes et seront préparés aux futures mises à niveau. Les anciens systèmes présentant des problèmes de sécurité seront mis à niveau, atténués ou remplacés.

Systèmes d'exploitation et gestion des correctifs

Certains produits Philips utilisent des systèmes d'exploitation (OS) d'ordinateurs commerciaux tiers comme Microsoft Windows. Nous surveillons en permanence les annonces de sécurité des fournisseurs et du secteur/des médias et effectuons des évaluations des risques sur les dispositifs médicaux actuels qui sont affectés par des vulnérabilités récemment découvertes.

Microsoft publie régulièrement des informations sur les correctifs de sécurité (hotfixes) pour MS Windows. Les évaluations de l'impact de ces correctifs par les équipes d'ingénierie des produits Philips commencent généralement dans les 48 heures suivant la prise de conscience par Philips d'une nouvelle vulnérabilité de sécurité ou de la disponibilité d'un correctif. Après évaluation, une indication de la réaction de Philips pour les produits concernés est mise à la disposition des utilisateurs, généralement dans un délai de 5 à 12 jours ouvrables pour la plupart des produits.

Selon la nature de la menace et le produit concerné, un « correctif » validé ou une mise à jour du logiciel peut être publié. Si la réponse recommandée nécessite une modification du logiciel système d'un dispositif médical, une mise à jour du logiciel peut être publiée. Les informations concernant la disponibilité et l'applicabilité de ces mises à jour sont également disponibles via les canaux de service standard de Philips et, pour certains produits, via notre site Web.

Afin de vous fournir ces informations importantes en temps utile et de manière pratique, le site Web de la Sécurité des produits Philips propose un accès à des informations dynamiques sur les vulnérabilités spécifiques aux produits. Ces informations sont présentées sous forme de tableaux simples, spécifiques à chaque produit, énumérant les vulnérabilités connues des logiciels et leur état actuel, les mesures recommandées aux clients et les commentaires généraux. Visitez le site Web de la Sécurité des produits Philips pour accéder à ces informations. Si vous avez des questions concernant les tableaux de vulnérabilité, la gestion des correctifs ou d'autres intérêts liés à la sécurité des produits, contactez Philips par e-mail à l'adresse productsecurity@philips.com ou contactez directement votre ingénieur du service extérieur Philips.

Protection contre les logiciels malveillants

Pour déployer et maintenir un fonctionnement efficace de votre équipement, les produits Philips sont livrés pour fonctionner en conformité avec les spécifications spécifiques du système et de la sécurité. Ces spécifications de produit peuvent inclure la configuration du dispositif, le réseau, le système d'exploitation et/ou les exigences logicielles pour la protection contre les logiciels malveillants. Pour plus d'informations, veuillez vous référer à la documentation ou au mode d'emploi de votre produit.

Site Web de Philips sur la sécurité des produits

Philips propose diverses ressources d'information sur son site Web consacré à la sécurité des produits, notamment des bulletins de sécurité, des FAQ, des informations sur la vulnérabilité, des liens vers des ressources sectorielles, des livres blancs sur la sécurité des produits et d'autres informations sur la sécurité des produits.

Formulaires MDS^2 pour les dispositifs médicaux

Pour aider nos clients américains à respecter leurs obligations au titre de l'HIPAA dans le cadre du règlement sur la sécurité de 2005, Philips a pris l'initiative de publier des informations sur la sécurité des produits[3]. Philips a pris de nombreuses mesures pour renforcer la sécurité de ses appareils médicaux en réponse aux demandes de ses clients. Lorsqu'ils sont utilisés correctement, les dispositifs de sécurité des produits de soins de santé Philips permettent aux utilisateurs de remplir plus facilement leurs obligations de garantir la confidentialité, l'intégrité et la disponibilité des informations de santé des patients. Compte tenu de l'importance accrue accordée à la sécurité des dispositifs médicaux et à la conformité avec la règle de sécurité de l'HIPAA aux États-Unis, la Healthcare Information and Management Systems Society (HIMSS) a créé une norme « Déclaration de divulgation du fabricant pour la sécurité des dispositifs médicaux » (MDS^2). La MDS^2 est destinée à fournir aux prestataires de soins de santé des informations importantes qui peuvent les aider à évaluer et à gérer les vulnérabilités et les risques associés aux informations électroniques de santé protégées (ePHI) créées, transmises ou conservées par les dispositifs médicaux.

Les formulaires MDS^2 de Philips sont à la disposition des clients sur notre site Web de Sécurité des produits à l'adresse suivante : www.philips.com/productsecurity

Rôle du client dans le partenariat pour la sécurité des produits

Nous reconnaissons que la sécurité des produits Philips doit être un élément important de votre stratégie de sécurité approfondie. Toutefois, la protection ne peut être réalisée que si vous mettez en œuvre une stratégie globale à plusieurs niveaux (comprenant des politiques, des processus et des technologies) pour protéger les informations et les systèmes contre les menaces internes et externes. Conformément aux normes du secteur, cette stratégie doit porter sur la sécurité physique, la sécurité opérationnelle, la sécurité des procédures, la gestion des risques, les politiques de sécurité et les plans d'urgence. La mise en œuvre pratique des éléments techniques de sécurité varie selon les sites et peut faire appel à un certain nombre de technologies, de configurations et de solutions logicielles. Comme pour tout système informatique, la protection peut comprendre des pare-feu, une segmentation du réseau et/ou d'autres dispositifs de sécurité entre le système médical et le réseau de votre établissement. Ces défenses de périmètre et de réseau sont des éléments essentiels dans le cadre d'une stratégie globale de sécurité des dispositifs médicaux. Toute connexion d'un dispositif à un réseau interne ou externe doit être effectuée avec une gestion des risques appropriée pour l'efficacité du produit et la sécurité des données et des systèmes.

Politiques relatives aux logiciels tiers et aux correctifs

Philips vend des appareils et systèmes médicaux et personnels très complexes. Seules les modifications autorisées par Philips doivent être apportées à ces systèmes, soit par le personnel de Philips, soit conformément aux instructions explicites publiées par Philips. Avec l'augmentation actuelle des menaces à la sécurité, les groupes d'ingénierie de produits de Philips travaillent à la qualification de logiciels et de solutions de tiers liés à la sécurité pour certains équipements. En outre, nous continuons à considérer la sécurité des patients et des opérateurs comme notre principale préoccupation, et nous sommes tenus de suivre des procédures réglementaires et d'assurance qualité pour vérifier et valider les modifications apportées à nos dispositifs médicaux. Comme pour les autres appareils médicaux, tout produit Philips « uniquement logiciel » doit être utilisé uniquement sur des ordinateurs et des réseaux correctement sécurisés, conformément à la documentation, aux contrats de service et aux instructions d'utilisation de votre produit Philips. Nous suggérons fortement à votre personnel de sécurité de surveiller les vulnérabilités du système et des applications et de maintenir le système d'exploitation et les autres logiciels installés sur votre système à jour et corrigés.

Philips vend une large gamme d'appareils, des produits de consommation courante aux systèmes de surveillance à domicile, en passant par les systèmes d'acquisition et de visualisation d'images, les PACS axés sur les TI, les systèmes vitaux opérationnels 24 heures sur 24 et 7 jours sur 7 et les moniteurs de surveillance des patients en temps réel. La nature diversifiée de notre portefeuille de produits nous a amenés à soutenir un large éventail de solutions, notamment l'installation et la maintenance de logiciels tiers sur nos systèmes. Veuillez contacter Philips pour obtenir des informations plus spécifiques sur votre produit[4].

Cas général

La plupart des équipements Philips ne permettent pas l'installation de logiciels tiers de quelque nature que ce soit par le client (par exemple, scanners antivirus, outils de productivité de bureau, correctifs système, pare-feu sur plateforme, etc.), sauf si Philips en a fait une exigence de spécification de fonctionnement ou si un consentement écrit préalable a été obtenu. Les modifications non autorisées apportées aux produits Philips peuvent annuler votre garantie et modifier le statut réglementaire de l'appareil. Aucun service résultant d'une modification non autorisée n'est couvert par nos contrats de service. De telles modifications non autorisées peuvent affecter les performances ou la sécurité de votre appareil de manière imprévisible. Philips n'est pas responsable des équipements qui ont fait l'objet de modifications non autorisées.

Lorsque Philips autorise l'utilisation de logiciels, de correctifs système ou de mises à niveau de tiers, l'installation autorisée est généralement effectuée par (1) Philips au moment de la fabrication ou de l'installation ou (2) un ingénieur de service qualifié Philips après l'installation.

Exceptions

Philips peut, dans certaines circonstances, autoriser l'installation ou l'activation de logiciels tiers directement par un ingénieur de service qualifié de Philips, mais toujours conformément aux instructions explicites et publiées de Philips et uniquement pour le système et la version couverts par l'autorisation écrite de Philips.

Avant d'envisager l'installation ou l'activation d'un logiciel tiers sur un produit Philips, vous devez contacter votre représentant de service Philips local afin de déterminer si votre produit particulier est qualifié pour ce logiciel spécifique et, le cas échéant, quelles restrictions peuvent s'appliquer.

Il est important de comprendre que toute modification non autorisée d'un appareil ou d'un système médical Philips (par exemple, modification du pare-feu du produit, correctifs logiciels, logiciels de sécurité, utilitaires, jeux, fichiers musicaux, autres logiciels, etc.) peut nuire aux performances ou à la sécurité du système de manière imprévisible, privant ainsi votre personnel et leurs patients des protections offertes par Philips, des exigences réglementaires et de qualité. Ces installations ou modifications peuvent avoir des effets secondaires préjudiciables :

1. Ouverture ou élargissement des voies qui pourraient compromettre l'accès ou le contrôle
2. Introduction de virus, de logiciels espions, de chevaux de Troie, d'accès par porte dérobée ou d'autres agents à distance
3. Installation de mises à jour non autorisées qui pourraient entraîner des vulnérabilités du produit et du système

Si vous soupçonnez ou avez connaissance de modifications non autorisées apportées à votre produit ou solution Philips, vous devez immédiatement le signaler au service clientèle Philips ou à votre ingénieur du service extérieur qui vous aidera à déterminer la mesure appropriée.

Service à distance de Philips

Philips a créé un réseau mondial de services à distance (RSN) basé sur le Web pour connecter un grand nombre de vos systèmes Philips à ses ressources de services avancés. Cette conception de pointe fournit à votre équipement un point d'accès unique aux équipements Philips sur site grâce aux technologies de réseau privé virtuel. Cette approche de tunnel sécurisé a été développée pour fournir une solution de service à distance de premier ordre qui sécurise la connexion grâce à un contrôle d'autorisation et d'authentification explicite avec cryptage de toutes les informations de la session de service.

Les innovations de produits et les solutions Philips dans un monde en mutation

Conformément à la nécessité d'accroître la sécurité de nos produits, Philips continue d'examiner et de reconcevoir les produits existants afin de répondre au mieux aux exigences de nos clients soucieux de la sécurité. Nous sommes profondément engagés dans la création des produits de demain basés sur des principes de sécurité fondamentaux.

Nous continuerons à travailler en étroite collaboration avec les fournisseurs, les organisations informatiques et les consommateurs afin de fournir des solutions flexibles aux problèmes d'aujourd'hui, même si nous créons de nouveaux produits à « Sécurité intégrée ». Les questions concernant nos efforts pour améliorer la sécurité de nos produits peuvent être adressées à votre service extérieur ou à votre représentant commercial ou à productsecurity@philips.com. Si votre préoccupation s'étend à la manière dont Philips gère les données personnelles (c'est-à-dire la vie privée), vous pouvez envoyer vos questions par e-mail à healthcare.privacy@philips.com.

Nous vous remercions de votre intérêt constant pour les nombreuses solutions innovantes fournies par Philips.

1 Recommandation de la FDA américaine pour le secteur : Cybersécurité pour les dispositifs médicaux en réseau contenant des logiciels prêts à l'emploi (OTS). http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.html

2 La vie privée sur Internet des objets : Menaces et défis, https://arxiv.org/abs/1505.07683

3 Pour obtenir des copies de la déclaration de divulgation du fabricant pour la sécurité des dispositifs médicaux (sous la forme standard HIMSS MDS2) pour les produits Philips, visitez http://www.healthcare.philips.com/main/support/productsecurity/mds2.wpd

4 Coordonnées de l'assistance Philips :
Soins de santé Philips :
- Amérique du Nord – +1 800 669 1328 (ou +1 321 253 5693)
- Asie – +85 2 2821 5888
- Europe, Moyen-Orient, Afrique – +49 7031 463 2254
- Amérique latine – +55 11 2125 0744
- Canada – +1 800 291 6743

Contacts mondiaux (soins de santé, santé personnelle, produits de consommation)
- http://www.philips.com/c-cs/global-country-selector.html
- Sélectionnez le pays, choisissez « Service client » et sélectionnez « Contactez-nous ».

5 Application de la gestion des risques aux réseaux informatiques intégrant des dispositifs médicaux, http://www.iso.org

6 U.S. Department of Veterans Affairs Medical Device Isolation Architecture Guide, v2.0, disponible sur le site Web du HIMSS http://www.himss.org/ASP/topics_FocusDynamic.asp?faid=101

7 Groupe de travail sur la sécurité des dispositifs médicaux de la Healthcare Information and Management Systems Society (HIMSS) http://www.himss.org/ Voir les rubriques et Tools > Medical Device Security

8 U.S. FDA Postmarket Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff (déc. 2016), http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm482022.pdf

9 L'IHE est une initiative conjointe de la Healthcare Information and Management Systems Society (HIMSS) et de la Radiological Society of North America (RSNA) http://www.ihe.net/

www.philips.com/productsecurity

www.philips.com