RESOURCE CENTER

Qu'est-ce que le cadre de cybersécurité du NIST ? Le guide ultime

Get the full interactive view at
https://bitwarden.com/fr-fr/resources/nist-cybersecurity-framework/

bitwarden

Histoire du NIST

Le National Institute of Standards and Technology (NIST) fournit des conseils et des bonnes pratiques aux organisations, afin d'aider les entreprises, les organisations à but non lucratif et les autres institutions du secteur privé à améliorer la gestion des risques liés à la cybersécurité. Le NIST fait partie du ministère américain du commerce et constitue l'un des plus anciens laboratoires de sciences (physiques) du pays.

En 2013, le président a publié le décret 13636 qui stipule que

> **"La politique des États-Unis consiste à renforcer la sécurité et la résilience des infrastructures critiques du pays et à maintenir un cyberenvironnement qui encourage l'efficacité, l'innovation et la prospérité économique tout en promouvant la sûreté, la sécurité, la confidentialité des affaires, la vie privée et les libertés civiles".**

Ce décret a établi certaines exigences que le NIST a appliquées à son cadre de cybersécurité :

- Identifier les normes et les lignes directrices en matière de sécurité applicables aux différents secteurs des infrastructures critiques.
- Fournir une approche hiérarchisée, flexible, reproductible, basée sur la performance et rentable.
- Aider les propriétaires et les exploitants d'infrastructures critiques à identifier, évaluer et gérer les cyberrisques.
- Permettre l'innovation technique et tenir compte des différences organisationnelles.
- Fournir des orientations neutres sur le plan technologique et permettre aux secteurs des infrastructures critiques de bénéficier d'un marché concurrentiel pour les produits et les services.
- Inclure des orientations pour mesurer la performance de la mise en œuvre du cadre de cybersécurité.
- Identifier les domaines d'amélioration qui devraient faire l'objet d'une collaboration future avec des secteurs particuliers et des organismes de normalisation.

Pourquoi cette question est-elle devenue si importante ?

En d'autres termes, les menaces croissantes en matière de cybersécurité affectent quotidiennement les entreprises et autres organisations. En l'absence d'une source unique de vérité, il serait presque impossible pour les entreprises de développer un cadre complet et efficace pour les aider à mettre en œuvre des mesures efficaces pour atténuer les risques de sécurité. C'est pourquoi le cadre de cybersécurité du NIST est devenu si important pour les entreprises ; il encourage les solutions efficaces, innovantes et résilientes pour maintenir la sécurité.

Table des matières

Qu'est-ce que le cadre de cybersécurité du NIST ?

Le cadre de cybersécurité du NIST aide les organisations de tous types à mieux comprendre, gérer et réduire les risques liés à la cybersécurité. Le résultat final de ces conseils est une meilleure protection des réseaux et des données. Le cadre de cybersécurité du NIST est décomposé de manière à ce que toute entreprise ou organisation puisse le mettre en œuvre afin de mieux comprendre où consacrer son temps et ses ressources pour améliorer la protection de la cybersécurité. Il s'agit de permettre aux entreprises de protéger plus efficacement leurs données, les données de leurs clients, leurs réseaux et leurs employés.

Bien que le cadre de cybersécurité du NIST ait été élaboré par une organisation américaine, il a été créé dans l'optique d'une adoption mondiale. À cette fin, il a été traduit dans de nombreuses langues et adopté par des gouvernements, des entreprises et des organisations du monde entier.

Depuis la version 1.1 du cadre de cybersécurité du NIST, de nombreuses organisations et gouvernements l'ont adopté avec succès :

- Saudi Aramco
- Gouvernement des Bermudes
- Direction nationale israélienne du cyberespace
- Cimpress-FAIR
- Multi-États - Centre d'analyse et de partage de l'information
- Centre médical de l'Université du Kansas
- Université de Pittsburgh
- ISACA
- Forum intersectoriel japonais
- Université de Chicago
- Autorité du fleuve du Bas-Colombie
- Optic Cyber Solutions

La dernière version du cadre de cybersécurité du NIST (CSF) s'adresse à des publics, des secteurs d'activité et des organisations de tous types et de toutes tailles, qu'il s'agisse de petites écoles, d'organisations à but non lucratif ou de grandes entreprises. Le cadre a été conçu de manière à ce que toute organisation, quel que soit son niveau de sophistication en matière de cybersécurité, puisse bénéficier des informations qu'il présente.

Selon Laurie E. Locascio, directeur du NIST et sous-secrétaire au commerce pour les normes et la technologie :

> "Le CCA a été un outil essentiel pour de nombreuses organisations, les aidant à anticiper et à faire face aux menaces de cybersécurité... Le CCA 2.0, qui s'appuie sur les versions précédentes, ne se limite pas à un seul document. Il s'agit d'un ensemble de ressources qui peuvent être personnalisées et utilisées individuellement ou en combinaison au fil du temps, à mesure que les besoins d'une organisation en matière de cybersécurité changent et que ses capacités évoluent".

L'histoire du cadre de cybersécurité du NIST

La dernière évolution du cadre de cybersécurité du NIST ne se limite pas aux infrastructures critiques, mais englobe toutes les organisations (de toutes tailles), quel que soit leur secteur d'activité.

Lorsque le cadre de cybersécurité du NIST a été créé, l'objectif était d'assurer un engagement continu avec les parties prenantes du gouvernement, de l'industrie et du monde universitaire. Pour créer ce cadre, le NIST a organisé des activités de sensibilisation et des ateliers dans tout le pays, ainsi qu'une demande d'informations (RFI) et une demande de commentaires (RFC). Leur objectif initial était triple :

- Identifier les normes, les lignes directrices, les cadres et les meilleures pratiques en matière de cybersécurité.
- Spécifier les lacunes prioritaires.
- Élaborer des plans d'action pour combler ces lacunes.

La période de consultation pour la collecte d'informations s'est terminée le 8 avril 2013, et le NIST a reçu plus de 270 réponses à la demande d'informations. À partir de ces réponses, le NIST a élaboré l'ordre du jour de son premier atelier sur le cadre de cybersécurité, qui s'est tenu à Washington DC dans le but de susciter l'intérêt, d'accroître la sensibilisation et de donner un aperçu du processus de développement collaboratif. L'atelier a porté sur le décret, les objectifs de l'élaboration et la réaffirmation du processus d'élaboration du cadre.

Le deuxième atelier a eu lieu du 29 au 31 mai 2013 à l'Université Carnegie Mellon, avec un ordre du jour basé sur l'analyse de l'appel à manifestation d'intérêt initial. Les objectifs étaient de mieux définir et clarifier les informations reçues et d'encourager le débat sur plusieurs sujets liés à la sécurité. À l'issue de cet atelier, le NIST a analysé les informations recueillies et créé des résumés qui ont été partagés avec les industries et utilisés pour créer le projet initial du cadre de cybersécurité.

La première version du cadre de cybersécurité du NIST a été publiée le 2 juillet 2013.

Le NIST a organisé plusieurs ateliers à la suite de la publication, afin de discuter et d'affiner la version initiale. Le 12 février 2014, la version 1.0 du cadre de cybersécurité du NIST a été publiée.

Les fonctions essentielles du cadre de cybersécurité du NIST

Le cadre de cybersécurité du NIST se compose de plusieurs fonctions essentielles, qui donnent un aperçu général des meilleures

pratiques. Ces fonctions ne doivent pas être considérées comme des étapes procédurales, mais plutôt comme des moyens de faire face à la nature dynamique des risques liés à la cybersécurité.

Gouverner

Cette fonction fournit des résultats qui aident à déterminer ce qu'une organisation peut faire pour donner la priorité aux autres fonctions dans le contexte de sa mission et des attentes des parties prenantes.

Identifier

La fonction d'identification fait appel à la nécessité de développer une compréhension organisationnelle des risques de cybersécurité pour les systèmes, les actifs, les données et les capacités. Cet élément se concentre sur l'entreprise, afin qu'elle puisse prioriser ses efforts d'une manière qui soit cohérente avec sa stratégie de gestion des risques.

Protéger

Cette fonction permet à l'organisation de sécuriser ses actifs et de prévenir ou de réduire la probabilité et l'impact d'un événement lié à la cybersécurité.

Détecter

Cette fonction permet de découvrir et d'analyser en temps utile les anomalies, les indicateurs de compromission et les autres événements indésirables qui indiquent qu'un événement de cybersécurité s'est produit ou va se produire.

Répondre

Cette fonction permet de contenir les effets d'un incident de cybersécurité, en couvrant la gestion des incidents, l'analyse, l'atténuation, l'établissement de rapports et la communication.

Récupérer

Cette fonction se concentre sur le rétablissement rapide des activités normales de l'entreprise, afin de réduire les effets d'un incident de cybersécurité et de permettre la communication nécessaire (et appropriée) pendant le rétablissement.

L'objectif ultime de ces fonctions est d'offrir une vision stratégique de haut niveau de la manière dont une organisation se prépare, réagit et se rétablit en cas d'événements liés à la cybersécurité.

Mise en œuvre du cadre de cybersécurité du NIST

Après avoir bien compris ce que fait le cadre de cybersécurité du NIST et comment il a évolué, vous vous demandez probablement comment le mettre en œuvre au mieux.

Le NIST recommande une approche en 7 étapes pour la mise en œuvre, qui se présente comme suit :

1. **Établir des priorités et délimiter le champ d'application** – Établissez des priorités parmi les objectifs et les actifs de votre organisation qui doivent être protégés.

2. **Orienter** – Familiarisez-vous, vous et votre équipe, avec les processus, les systèmes et les composants qui entrent dans le champ d'application, ainsi qu'avec les principales règles de conformité auxquelles ils doivent se conformer.

3. **Créer un profil actuel** – Indiquer quels résultats de contrôle du cadre sont déjà atteints au sein de votre organisation, puis dresser une liste de ce qui doit encore être intégré.

4. **Procéder à une évaluation des risques** – Analyser votre environnement opérationnel pour déterminer la probabilité d'événements liés à la cybersécurité, ainsi que l'impact qu'ils pourraient avoir.

5. **Créez un profil cible** - Concentrez-vous sur l'évaluation des catégories et sous-catégories du cadre de cybersécurité pour vous aider à décrire les résultats que vous souhaitez obtenir en matière de cybersécurité.

6. **Déterminer, analyser et hiérarchiser les lac** unes - Déterminez les lacunes de votre organisation en matière de cybersécurité. À partir de cette analyse, vous pouvez ensuite élaborer un plan hiérarchisé pour répondre à ces besoins.

7. **Mettre en œuvre votre plan d'action** - Passez à l'action et mettez en œuvre le plan que vous avez créé pour résoudre tous les problèmes découverts au cours des étapes précédentes.

Il convient de garder à l'esprit que le cadre n'est pas inflexible. En fait, le cadre offre suffisamment de flexibilité pour s'intégrer à vos processus de sécurité existants. Vous devriez voir comment cela fonctionne dans les sept étapes énumérées ci-dessus.

Avantages de l'adoption du cadre de cybersécurité du NIST

Grâce à la manière dont le NIST présente les sept étapes de la mise en œuvre du cadre, les organisations obtiennent un aperçu complet des risques auxquels elles sont exposées, de la manière de planifier en fonction de ces risques, d'améliorer la communication à l'échelle de l'organisation et de renforcer la conformité. L'éducation concernant les faiblesses d'une organisation et la manière de les atténuer est l'un des avantages cruciaux du cadre NIST.

> Selon la Commission fédérale du commerce, le cadre du NIST "aide les entreprises de toutes tailles à mieux comprendre, gérer et réduire leurs risques en matière de cybersécurité et à protéger leurs réseaux et leurs données".

Le NIST comprend que chaque organisation est différente et propose même 3 conseils pour sécuriser vos mots de passe (ce qui devrait être considéré comme universel).

Défis et considérations liés à l'adoption du cadre

Le cadre de cybersécurité du NIST peut être complexe. Il est important de bien comprendre les fonctions essentielles avant de passer aux sept étapes énumérées ci-dessus. Pour garantir un succès durable, il est essentiel d'encourager une culture de la cybersécurité au sein de votre organisation, faute de quoi vous vous heurterez à une résistance à ce qui pourrait être un changement radical des processus et des systèmes.

D'autres défis sont à relever :

- Contraintes de ressources - il se peut que vous ne disposiez pas actuellement du personnel capable de mettre en œuvre ces changements.
- Vous devrez très probablement passer du temps à personnaliser le cadre de cybersécurité pour qu'il corresponde mieux à votre organisation.
- Les menaces évoluent sans cesse, ce qui signifie que vos pratiques de sécurité doivent suivre le mouvement.
- Vous devrez intégrer le cadre de cybersécurité à vos processus existants.
- Il peut être difficile d'encourager l'engagement des parties prenantes, ce qui est directement lié à la promotion d'une culture de la cybersécurité capable de répondre à ces exigences.

Profils et niveaux du cadre de cybersécurité du NIST

Il existe quatre niveaux de mise en œuvre du NIST, à savoir

- **Niveau 1 Partiel** - Entreprises ayant des procédures de sécurité à la demande ou nulles.
- **Niveau 2 Informées des risques** - Entreprises qui sont conscientes des menaces auxquelles elles sont confrontées et qui ont mis en place certaines politiques, mais qui ne disposent pas d'une stratégie coordonnée.
- **Niveau 3 reproductible** - Entreprises dont les meilleures pratiques en matière de gestion des risques et de cybersécurité ont été approuvées par la direction. Ces entreprises se mesurent souvent à leurs concurrents et travaillent même avec d'autres organisations pour s'assurer que leurs pratiques sont alignées.
- **Niveau 4 Adaptation** - Entreprises dans des secteurs fortement réglementés (tels que les banques et les soins de santé) qui contribuent régulièrement à la sensibilisation aux risques.

Selon le NIST, le profil du cadre de cybersécurité "est l'alignement des fonctions, des catégories et des sous-catégories sur les exigences de l'entreprise, la tolérance au risque et les ressources de l'organisation". Ces profils aident les organisations à établir une feuille de route pour réduire les risques liés à la cybersécurité.

Le NIST propose un modèle de profil organisationnel personnalisable pour le cadre de cybersécurité, ainsi qu'une liste de profils communautaires pouvant être utilisés.

Mise à jour et évolution du cadre NIST

N'oubliez pas que le cadre de cybersécurité du NIST est conçu comme un document évolutif qui dépend de mises à jour régulières reflétant l'évolution constante du paysage de la cybersécurité et des menaces émergentes. C'est pourquoi il est essentiel que les organisations se tiennent au courant des dernières menaces, afin que le cadre de cybersécurité puisse évoluer pour répondre aux besoins actuels et s'améliorer continuellement.

Pour vous assurer que votre organisation est en mesure d'évoluer avec le cadre de cybersécurité du NIST, vous pouvez envisager de construire la meilleure pile technologique de cybersécurité pour votre entreprise, afin de vous assurer que vous êtes en mesure de tirer parti de la meilleure technologie capable d'évoluer avec le cadre de cybersécurité.

Tirer parti de Bitwarden pour renforcer la cybersécurité

Il va sans dire que la sécurité est devenue l'un des domaines les plus importants pour les organisations. Sans de solides pratiques de gestion des risques en matière de cybersécurité, les entreprises pourraient être victimes d'un grand nombre de menaces dans la nature. Avec l'aide du cadre de cybersécurité du NIST et une planification et une communication soignées, la sécurité de votre organisation pourrait s'améliorer considérablement. Abordez le cadre de cybersécurité du NIST de manière approfondie, suivez les sept étapes et soyez toujours prêt à le mettre à jour et à le faire évoluer afin que votre organisation soit mieux protégée contre les risques liés à la cybersécurité.

Prêt à démarrer dès aujourd'hui ? Envisagez d'adopter une solution de gestion des mots de passe pour que votre organisation parte du bon pied. Consultez les plans Bitwarden Business, contactez le service commercial et comparez les prix des plans.