CONSTRUISEZ VOTRE HAVRE DE SÉCURITÉ

Une seule faille de sécurité suffit pour compromettre vos activités. Sécurisez l'ensemble de votre réseau avec Cisco Digital Network Architecture

www.cisco.fr/dna

Une gestion du réseau sans risque

Les DSI d'aujourd'hui se tournent de plus en plus vers les nouvelles technologies numériques pour permettre à leur entreprise de réussir dans un monde qui change vite.

En général, tout se passe bien... jusqu'à ce qu'un problème survienne.

En se lançant sans réfléchir dans le numérique, les entreprises s'exposent davantage à la cybercriminalité, aux nouvelles formes de programmes malveillants et à d'autres cybermenaces. Comment gérer la croissance exponentielle des menaces tout en profitant des opportunités créées par les nouvelles technologies numériques ? Pouvez-vous risquer de compromettre votre réseau en innovant ?

« C'est très simple : plus les vecteurs d'attaque restent indétectés, plus les hackers ont le temps d'exploiter nos systèmes et notre infrastructure, et de parvenir à leurs fins. Il nous revient de réduire leur marge de manœuvre. »

John N. Stewart, Vice-président
et responsable de la sécurité, Cisco

Chez Cisco, nous couvrons tous les risques liés à la sécurité de réseau.

Cisco Digital Network Architecture fournit une visibilité totale sur les menaces et vous protège entièrement contre les risques internes et externes rencontrés au niveau des connexions réseau filaires, sans fil et WAN. La solution Cisco DNA transforme votre réseau en détecteur de menaces pour identifier, isoler et éliminer les menaces dès leur entrée dans le réseau. Le réseau joue également le rôle d'exécuteur de fonctions de sécurité pour mieux se protéger et répondre plus vite aux attaques, garantissant une sécurité totale à tout moment sur l'ensemble du réseau.

Bloquez les attaques même quand vous ne les voyez pas

Alors que le nombre de connexions Internet augmente à chaque minute, votre réseau est continuellement en proie à des cyberattaques avancées. Chaque connexion réseau, qu'elle soit créée par des services cloud, la mobilité, l'Internet des objets (IoT) ou une autre activité, représente une porte d'entrée potentielle pour les hackers.

Grâce à Cisco® ISE (Identity Services Engine), qui surveille toutes les connexions à votre réseau, vous savez exactement quels périphériques, utilisateurs ou applications tentent d'accéder à votre réseau et pouvez appliquer des fonctions de Threat Intelligence pour les accès non autorisés. Avec notre technologie de segmentation du réseau, vous pouvez protéger chaque segment en appliquant des politiques de groupe spécifiques qui déterminent l'accès des utilisateurs en fonction de leur rôle et de leurs besoins professionnels. Cela vous permet de simplifier la gestion des accès tout en sachant exactement qui a accès aux données sur votre réseau et à quel moment.

« Cisco ISE empêche tous les accès non autorisés au réseau tout en permettant de gérer les accès opérationnels de manière ultraflexible, grâce à la centralisation de la gestion des politiques et à l'automatisation des procédures de configuration et de gestion du réseau. »

Mirko Berlier, Ingénieur Cisco et Architecte d'Expo 2015

Que faire si les menaces parviennent à entrer dans le réseau ? Cisco TrustSec® et Cisco ISE vous aident à réduire votre « surface d'exposition aux attaques ». Grâce à la segmentation du réseau et au moteur de politiques de sécurité centralisé, même si une attaque se produit, votre réseau vous en informe et isole les appareils infectés rapidement afin d'éviter la propagation de l'attaque.

Selon une étude récente publiée par Forrester, TrustSec permet aux départements informatiques d'implémenter des changements 98 % plus rapidement, de diminuer les coûts jusqu'à 80 % et de fournir un retour sur investissement de 140 %.

En savoir plus : Cisco ISE | Cisco Network as an Enforcer | Cisco TrustSec

Sécurisez les points d'accès à votre réseau

Toutefois, les attaques ne se produisent plus seulement au cœur du réseau. En raison du nombre accru de points d'accès aux réseaux locaux et aux sites distants, la périphérie du réseau devient le principal point d'entrée des accès non autorisés ou malveillants. Heureusement, la solution intégrée d'utilisation du réseau Cisco comme détecteur de menaces transforme votre réseau Cisco en véritable système de sécurité. Vous bénéficiez d'une visibilité étendue et approfondie sur votre réseau et tout ce qui s'y connecte avant, pendant et après une attaque.

Comment cela fonctionne-t-il ?

Cisco Umbrella pour les sites distants est une solution de sécurité cloud intégrée par défaut dans votre routeur Cisco ISR 4000. Rapidement mise en œuvre, elle est votre première ligne de défense contre les menaces dans les sites distants, sans coût supplémentaire.

Ensuite, avec Cisco IOS® Flexible NetFlow et nos fonctions avancées d'analyse de la sécurité, Cisco Stealthwatch® détecte automatiquement les comportements anormaux du réseau et des utilisateurs, facilitant l'identification des éléments suspects auxquels réagir.

Avec Cisco Stealthwatch, le diagnostic des problèmes de sécurité et de réseau est ramené de plusieurs jours, voire plusieurs mois, à seulement quelques minutes.

En savoir plus :

- Cisco Umbrella Branch
- Cisco IOS Flexible Netflow
- Cisco Stealthwatch
- Cisco Network as a Sensor

Réduction des délais de reprise

Votre réseau peut corriger les failles plus rapidement grâce à l'automatisation fournie par le contrôleur Cisco APIC-EM (Application Policy Infrastructure Controller Enterprise Module). Grâce à ce contrôleur, vous pouvez corriger les problèmes en temps réel pour l'ensemble de votre entreprise, au lieu de procéder au cas par cas pendant plusieurs semaines, voire plusieurs mois. Grâce à Cisco Advanced Malware Protection, qui observe, analyse et enregistre l'activité de chaque fichier entrant dans le réseau, vous savez exactement d'où provient chaque programme malveillant. Vous pouvez alors l'isoler et trouver une solution en quelques clics.

100%

des programmes malveillants, des exploits et des tentatives de contournement détectés

Pour la troisième année consécutive, Cisco sort leader des tests de NSS Labs sur les systèmes de détection des failles, en détectant 100 % des programmes malveillants, des exploits et des tentatives de contournement.

En savoir plus :

Cisco APIC-EM

Cisco Advanced Malware Protection

Exploitez pleinement le potentiel de votre réseau.

Réduisez les risques, améliorez l'efficacité de vos systèmes de sécurité et optimisez la mise en conformité avec Cisco Digital Network Architecture.

www.cisco.fr/dna