Réseaux de nouvelle génération : la sécurité pour aujourd'hui et pour demain

Faire face aux menaces d'aujourd'hui sur des réseaux conçus pour répondre aux besoins d'hier, met les entreprises en danger.

L'informatique en entreprise est en pleine évolution : consumérisation croissante, mobilité, cloud computing ; ces tendances génèrent de nouvelles opportunités commerciales, mais également de nouveaux risques et menaces. Les départements informatiques doivent trouver le moyen de protéger les actifs de leurs entreprises tout en leur permettant de profiter de ces tendances, ce qui peut s'avérer plus compliqué que nécessaire lorsque le réseau n'est pas adapté. Ce livre blanc passe en revue les implications de la sécurisation d'un réseau bon marché face aux risques émergents et les compare à ce que peut apporter un réseau de nouvelle génération.

Le modèle de sécurisation des réseaux d'hier

Il y a peu, il était encore relativement simple de sécuriser un environnement informatique. Les données de base que sont la situation géographique des employés, les applications qu'ils utilisent et le type d'appareils sur lesquels ils les font tourner étaient des variables connues. Ces données étaient par ailleurs relativement statiques, ce qui signifie que les politiques de sécurité restaient applicables dans la plupart des circonstances. Les applications étaient exécutées sur des serveurs dédiés entreposés dans un centre de données ; le département informatique en contrôlait l'accès et en fixait les limites afin de faire respecter les politiques de sécurité. Les applications et les terminaux étaient sécurisés et l'accès au réseau était limité. Le réseau proprement dit avait pour fonction de connecter les utilisateurs aux ressources informatiques selon une architecture client/serveur et, dans l'ensemble, le trafic réseau était prévisible.

À l'heure actuelle, cependant, plusieurs tendances émergentes ont une incidence majeure sur la sécurité des réseaux et ce, sur deux plans différents. Premièrement, ces tendances modifient l'architecture du réseau. La périphérie de réseau s'est déplacée dès l'instant où une vaste palette d'appareils mobiles ont commencé à se connecter au réseau de l'entreprise (et pas nécessairement depuis les locaux de celle-ci, d'ailleurs). Les applications bougent également : elles sont virtualisées et peuvent passer d'un serveur, voire d'un centre de données, à l'autre. Parallèlement, les utilisateurs étendent le réseau de l'entreprise en ayant recours au cloud lorsqu'ils utilisent des applications de collaboration telles que Dropbox ou Google Docs. Le département informatique ne sait plus quels sont les appareils qui se connectent au réseau, ni où ils se trouvent. Les applications utilisées ne sont plus seulement celles qu'il fournit. Les données ne sont plus cantonnées au centre de données, mais peuvent résider à l'autre bout du pays, sur des smartphones ou des tablettes, voire hors de portée, dans le cloud.

La deuxième tendance qui affecte la sécurité du réseau est l'émergence de menaces de plus en plus complexes et sophistiquées. Les réseaux d'hier étaient frappés par des attaques très généralistes : les pirates envoyaient par exemple deux millions d'e-mails ciblant une vulnérabilité connue et comptaient sur le fait que statistiquement, un certain pourcentage des destinataires ouvriraient l'e-mail et succomberaient à l'attaque.

PUBLICATION PERSONNALISÉE DE
CSO Custom Solutions Group

SPONSORISÉ PAR
CISCO

Les économies réalisées lors de l'achat d'un réseau bon marché s'évaporent rapidement, car celui-ci ne dispose d'aucune fonction de sécurité intégrée. Par conséquent, le département informatique doit faire face aux menaces à l'aide de solutions à différents niveaux.

Ce modèle a complètement changé aujourd'hui : les hackers ne ciblent plus les foules, et n'utilisent plus nécessairement les vulnérabilités les plus connues. À l'inverse, ils procèdent à des attaques plus ciblées et plus complexes. Ils font appel à l'ingénierie sociale pour obtenir des informations sur la cible puis exploitent la confiance des utilisateurs en une application ou en un autre utilisateur pour installer un logiciel malicieux ou voler des données. Ces attaques très ciblées sont moins susceptibles d'être détectées que les attaques généralistes et risquent de rester inaperçues plus longtemps.

Sécuriser un réseau bon marché

Malheureusement, une autre évolution vient encore compliquer le travail de sécurisation des départements informatiques. Certains analystes et fournisseurs encouragent les entreprises à considérer le réseau comme un produit de base : n'importe lequel fait l'affaire et il suffit de choisir le moins cher à l'achat. Cependant, les économies réalisées lors de l'achat d'un réseau bon marché s'évaporent rapidement, car celui-ci ne dispose d'aucune fonction de sécurité intégrée, ce qui oblige le département informatique à faire face aux menaces à l'aide de solutions impliquant plusieurs produits et, par conséquent, à passer plus de temps à déployer, configurer et administrer le système. Le système de sécurité résultant est incapable de tenir le rythme face à l'émergence des nouvelles menaces, et encore moins de les anticiper. Ses différents composants n'étant pas unifiés, il peut se révéler difficile de faire appliquer les politiques de sécurité de manière cohérente au sein de l'environnement informatique. En matière de défense, plus le département informatique dispose d'informations sur le contexte, mieux il est équipé pour mettre un terme aux attaques réseau. Devoir corréler les données provenant de plusieurs systèmes différents pour obtenir ces informations est une perte de temps.

Un réseau bon marché sécurisé de cette manière est par conséquent un réseau instable, qui engendre un risque accru d'interruption, que ce soit en raison d'une brèche dans la sécurité ou d'une panne affectant l'un des multiples systèmes. Lorsque le réseau défaille, tout le reste fait de même, y compris le chiffre d'affaires.

Approche moderne de la sécurité du réseau

Fort heureusement, les réseaux bon marché et leurs implications en termes de sécurité ne constituent pas la seule possibilité. En matière de sécurisation des réseaux, les innovations sont apparues au même rythme que les tendances en informatique. Les réseaux de nouvelle génération tiennent compte des technologies de demain et intègrent des fonctions de sécurité qui les protègent activement contre les menaces les plus complexes et les plus ciblées. C'est cette protection qui permet aux départements informatiques d'avancer en toute confiance et de saisir les opportunités commerciales que représentent la mobilité et le cloud computing.

Les réseaux de nouvelle génération sont dotés d'une pleine conscience du contexte et offrent une visibilité et un contrôle inégalés, ce qui leur permet d'assurer la sécurité sur tout le réseau, du siège social aux filiales, pour les employés en interne comme pour les travailleurs à distance et ce, sur réseau câblé, sans fil ou VPN. Leur architecture globale permet de créer, de distribuer et de faire appliquer des règles de sécurité basées sur un langage contextuel, à base d'opérateurs de type « qui, quoi, où, quand et comment ». Les mesures prises pour faire respecter ces règles peuvent aller du cryptage des données au blocage de l'accès à certaines données ou certains appareils. Si, par exemple, un employé se connecte au réseau de l'entreprise à l'aide d'un smartphone, le réseau identifie à la fois l'appareil, l'utilisateur et les autorisations dont ils bénéficient. Non seulement le système gère les politiques applicables à l'appareil et à l'utilisateur, mais il les partage avec tous les points du réseau et met automatiquement et instantanément à jour les informations disponibles lorsqu'un nouvel appareil fait son apparition sur le réseau.

Avec des règles de sécurité globales, il est évidemment plus facile d'adopter une politique de type « bring your own device »[1], mais également de faire face aux problèmes de sécurité que peut poser le cloud computing. Avec un réseau de nouvelle génération, les entreprises peuvent désormais, sur simple activation d'un paramètre (et ce, même sur les réseaux distribués), rediriger le trafic Web intelligemment afin d'appliquer les politiques de contrôle et de sécurité granulaire.

[1] Dans le cadre des politiques de type « bring your own device », les employés sont autorisés à utiliser leurs propres appareils (smartphones, tablettes, etc.) pour accéder aux ressources de l'entreprise.

Avec la mise en place d'un réseau à dépenses d'investissement réduites, le département informatique risque de devoir dire « non » aux nouvelles technologies ou initiatives commerciales, tout simplement parce que le réseau est incapable de les prendre en charge.

Réseau bon marché contre réseau de nouvelle génération

Le réseau de nouvelle génération offre bien plus que des fonctions de sécurité intégrées. Il s'agit d'un réseau mis au point de manière stratégique, optimisé pour les besoins d'aujourd'hui, mais également conçu pour pouvoir faire face aux problèmes technologiques de demain et pour protéger l'investissement qu'il représente. En d'autres termes, un réseau de nouvelle génération est un réseau dynamique capable de gérer la mobilité, le cloud computing et l'évolution des menaces. Il s'agit également d'un mécanisme de fourniture de services permettant aux responsables de la sécurité (CSO) de répondre favorablement aux besoins qu'engendrent les efforts stratégiques des entreprises.

Lors du calcul du coût total d'acquisition (TCO) du réseau, il est recommandé aux CSO de ne pas sous-estimer la valeur commerciale que peuvent apporter les opportunités stratégiques. Avec la mise en place d'un réseau à dépenses d'investissement réduites, le département informatique risque de devoir dire « non » aux nouvelles technologies ou initiatives commerciales, tout simplement parce que le réseau est incapable de les prendre en charge. Cela veut dire « non » aux politiques autorisant les employés à amener leurs propres appareils au travail, « non » à l'extension de la virtualisation aux applications professionnelles essentielles, « non » aux services liés au cloud, « non » au format rich media. Tous les avantages que ces technologies pourraient apporter en termes d'économies, de compétitivité, de productivité et d'agilité sont perdus et ce, pour quelques euros économisés sur le réseau. À l'inverse, ces mêmes avantages peuvent compenser le coût plus élevé d'un réseau professionnel de nouvelle génération.

Examinons plus en détail la différence entre un réseau à bas prix ou réseau suffisant, et un réseau de nouvelle génération, générateur d'activité :

- **Fonction du réseau :** un réseau à bas prix n'a qu'un objectif : relier l'utilisateur aux ressources informatiques. Un tel objectif était peut-être acceptable en 2005, quand les utilisateurs étaient assis à leur bureau, devant un ordinateur branché sur un port Ethernet. Mais un réseau d'entreprise de nouvelle génération est unifié : il se compose d'éléments câblés, sans fil et distants. Il prend en charge un grand nombre d'appareils différents ainsi que la gestion des accès au bâtiment et de l'énergie. Il est multifonctionnel et gère la connectivité entre machines, un élément qui peut s'avérer indispensable lors de l'installation de capteurs ou la création d'un système de sauvegarde du centre de données.
- **Sécurité :** avec un réseau à bas prix, la sécurité est un supplément. En d'autres termes, elle repose sur des produits ciblés qui ne communiquent pas très bien les uns avec les autres. Un réseau de nouvelle génération comprend des capacités de sécurité du site au cloud. « Intégration » signifie moins de frais administratifs et moins de failles de sécurité.
- **Intelligence applicative :** un réseau convenable ne reconnaît pas les applications ni les terminaux. Pour lui, les données ne sont que des données. Le réseau de nouvelle génération est conscient des applications et des terminaux. Il s'adapte à l'application distribuée et au périphérique d'extrémité sur lequel il apparaît.
- **Qualité de service :** les réseaux à bas prix d'aujourd'hui reposent sur des normes QoS très basiques, qui s'avèrent souvent insuffisantes pour la gestion du trafic vidéo ou des bureaux virtualisés. Le réseau de nouvelle génération est équipé de commandes optimisées pour les contenus multimédias pour assister l'intégration de la voix et de la vidéo.
- **Normes :** le réseau à bas prix repose sur des normes non tournées vers l'avenir. Le réseau de nouvelle génération prend non seulement en charge les normes d'aujourd'hui, mais dispose également d'innovations qui lui permettront de se conformer à celles de demain.
- **Garantie :** les réseaux à bas prix sont assortis d'une assistance de maintenance limitée et d'une déclaration de garantie. Les fournisseurs de réseaux de nouvelle génération offrent une garantie, mais également des services intelligents avec une gestion intégrée.
- **Coût d'acquisition :** malheureusement, les économies réalisées sur le prix d'achat sont souvent réduites à néant par l'augmentation des frais de fonctionnement qu'engendre le réseau : frais d'intégration plus élevés, interruptions de service, brèches graves dans la sécurité. Alors que les vendeurs de réseau à bas prix minimisent ces coûts, les fournisseurs de réseaux de nouvelle génération proposent un produit qui non seulement réduit les frais de fonctionnement, mais permet aux entreprises de bénéficier de services informatiques améliorés et de saisir les opportunités commerciales, ce qui augmente son retour sur investissement.

Tenter de sécuriser un réseau d'hier pour lui permettre de prendre en charge les technologies d'aujourd'hui est un combat perdu d'avance. Pour anticiper les risques et menaces qu'engendrent la consumérisation de l'informatique, la mobilité et le cloud computing, il faut absolument disposer d'un réseau de nouvelle génération.

SPONSORISÉ PAR

CISCO

L'architecture réseau sans frontières

Cisco a mis en place un cadre pour le réseau de nouvelle génération, nommé « Architecture Borderless Network ». Celui-ci définit comment la vision à long terme de Cisco est planifiée pour fournir de nouveaux services réseau, et assister les exigences des entreprises et des utilisateurs. Ces services permettent aux entreprises de mieux répondre à leurs besoins, à ceux des utilisateurs et à ceux de leur département informatique. Les services de réseau intelligents sont essentiels lorsqu'il s'agit de réduire le TCO et de donner au département informatique les outils qui lui permettront d'aider l'entreprise à proposer de nouvelles compétences.

Cisco a pour objectif de mettre en place des systèmes qui permettent aux départements informatiques de passer moins de temps à intégrer des fonctionnalités de base à leur réseau ; pour ce faire, la société fournit un ensemble de services qui permettent au réseau de mieux répondre aux besoins des entreprises et des utilisateurs.

L'un des éléments clés du succès des réseaux sans frontière de Cisco est l'infrastructure Cisco SecureX, un système de sécurité qui va des terminaux au cloud et prévoit des politiques et des moyens de surveillance à tous les coins du réseau, ainsi que des outils de gestion centralisée permettant de planifier le réseau, de le configurer, d'y distribuer les politiques et de le dépanner.

L'infrastructure Cisco SecureX

Cisco SecureX associe la puissance du réseau Cisco à des mesures de sécurité contextuelles qui protègent les entreprises d'aujourd'hui, quelle que soit la manière, le lieu ou le moment où leurs employés font usage de leur réseau. L'infrastructure Cisco SecureX repose sur trois principes fondamentaux :

- **Politiques contextuelles :** l'infrastructure utilise un langage descriptif simplifié permettant d'établir des politiques de sécurité tenant compte de cinq paramètres : l'identité de l'utilisateur, l'application utilisée, l'appareil utilisé pour l'accès, l'emplacement géographique et les informations temporelles. Ces politiques de sécurité permettent aux entreprises de mettre en place une sécurité efficace et de la faire respecter plus aisément sans perdre en productivité.
- **Application contextuelle de la sécurité :** l'infrastructure emploie des informations globales et d'autres fournies par le réseau pour prendre les meilleures décisions et pour assurer une sécurité à la fois homogène et omniprésente. Les possibilités de déploiement (services de sécurité intégrés, appareils autonomes ou services de sécurité passant par le cloud) offrent un maximum de souplesse tout en protégeant au mieux les utilisateurs et en réduisant la charge réseau.
- **Grâce à son intelligence réseau et globale,** l'infrastructure offre une vue détaillée de l'activité du réseau ainsi que des menaces afin de protéger rapidement et efficacement les utilisateurs et de faire appliquer les politiques de sécurité :
  - > L'intelligence locale de l'infrastructure du réseau Cisco tient compte du contexte (identité, appareil, emplacement et comportement) pour appliquer les politiques relatives aux accès et à l'intégrité des données.
  - > L'intelligence globale fournie par Cisco (Cisco Security Intelligence Operations, aussi appelée SIO) dresse une vue d'ensemble, complète et à jour, des menaces du moment, de leur contexte et de leur comportement, afin d'assurer à tous une protection maximale en temps réel.

L'infrastructure Cisco SecureX permet aux entreprises d'adopter la mobilité et le cloud tout en protégeant leurs actifs les plus précieux. Elle offre une visibilité et un contrôle granulaires de l'ensemble du réseau de l'entreprise, à l'utilisateur et à l'appareil près. Pour les départements chargés de la sécurité informatique des entreprises, cela contribue à une meilleure protection contre les menaces, la sécurité étant assurée de bout en bout, en permanence et assortie d'une intelligence globale. Les départements informatiques sont quant à eux plus efficaces, grâce à des politiques simplifiées, des options de sécurité intégrées et une application automatisée des règles de sécurité.

Conclusion

Tenter de sécuriser un réseau d'hier pour lui permettre de prendre en charge les technologies d'aujourd'hui est un combat perdu d'avance. Pour anticiper les risques et menaces qu'engendrent la consumérisation de l'informatique, la mobilité et le cloud computing, il faut absolument disposer d'un réseau de nouvelle génération. Conçu dès le départ avec des fonctions de sécurité intégrées, le réseau de nouvelle génération permet de répondre plus aisément aux besoins de l'entreprise tout en assurant la sécurité des applications stratégiques d'aujourd'hui.

Pour en savoir plus, consultez la page www.cisco.com/go/security