L'ÉCONOMIE DE DÉFENSE

Modélisation des investissements pour faire face aux risques liés à la sécurité à l'époque de recrudescence des cyber-menaces

JUNIPER NETWORKS

L’économie de défense : Modélisation des investissements pour faire face aux risques liés à la sécurité à l’époque de recrudescence des cyber-menaces

La nouvelle étude parrainée par Juniper Networks et menée par RAND Corporation « The Defender’s Dilemma: Charting a Course Toward Cybersecurity » (Le dilemme du défenseur : tracer la voie vers la cybersécurité) introduit un modèle heuristique, unique en son genre, pour aider les entreprises à identifier les enjeux et facteurs économiques liés à la défense.

Les cyberattaques sont en passe de devenir l'une des plus grandes menaces auxquelles sont confrontées les entreprises, quel que soit leur secteur. Qu'il s'agisse du vol de propriété intellectuelle dû à l’espionnage industriel ou d’atteintes à la sécurité des données à grande échelle, les entreprises doivent redoubler d'efforts pour garder une longueur d'avance face aux menaces et gérer efficacement les risques. En réponse, les entreprises ont fortement mobilisé leur temps, leur énergie et leurs ressources pour lutter contre les menaces auxquelles elles font face.

Il y a une bonne raison à cela. L'année dernière, une étude de RAND Corporation (RAND), parrainée par Juniper Networks et intitulée « Markets for Cybercrime Tools and Stolen Data: Hackers’ Bazaar » (Marché des outils de la cybercriminalité et des données volées : le bazar du pirate), a révélé que les cybercriminels disposent de cyber-marchés noirs organisés, qui ont désormais atteint des niveaux de maturité économique sans précédent. Dans les faits, ces marchés permettent aux cybercriminels d’être mieux armés pour pénétrer les réseaux des entreprises et de générer des bénéfices bien plus conséquents. De plus, l'étude prédit que les moyens d'attaque dépasseraient bientôt ceux de la défense.

> Juniper est convaincu que si le calcul économique est clair pour les cybercriminels, on ne peut pas en dire autant pour les entreprises qui se retrouvent dans un environnement beaucoup plus agité, flou et chaotique.

Principales conclusions du rapport :

D'après Juniper, le nouveau modèle de RAND identifie cinq facteurs principaux qui influencent le coût lié à la cybersécurité pour les entreprises, comme décrit dans le présent résumé et dans le rapport complet de RAND. Chacun de ces facteurs a ou aura un impact significatif sur ce coût.

1. Il n’existe pas d’approche standard : les entreprises n’adoptent pas une stratégie économique optimale
2. Nombre d’outils ont une « demi-vie » et perdent de la valeur
3. L'impératif humain : investir dans la compétence permet de réduire les coûts sur le long terme
4. L'Internet des objets est à la croisée des chemins
5. L’élimination des failles logicielles réduit considérablement les coûts

Plusieurs spécialistes de la sécurité admettent depuis un certain temps que ces facteurs doivent être pris en compte dans le cadre d'un programme de sécurité. Cependant, l'étude de RAND est la première à modéliser de manière quantitative leur impact sur les coûts. Ce faisant, ce nouveau modèle contribue, en se basant sur des données concrètes, à aider à comprendre en quoi chaque facteur est important et comment il permet aux entreprises de gérer les risques de sécurité de manière plus stratégique et globale.

Le dilemme du défenseur

La nouvelle étude de RAND, qui se penche sur les réalités économiques pour les défenseurs, montre que les responsables de la sécurité des systèmes d'information (RSSI) ont l'impression de faire du surplace, augmentant les investissements dans la sécurité sans pour autant se sentir plus protégés. Plus inquiétant encore, ils pensent que les cybercriminels sont rapidement en train de prendre l'avantage sur les défenseurs et nombreux sont ceux qui sont indécis concernant le moment ou le montant à investir dans la sécurité.

Cette situation est en partie due au fait que plusieurs entreprises, voire même certains acteurs dans le domaine de la sécurité, ont du mal à qualifier la sécurité comme un facteur de risque pour l'entreprise. En cybersécurité, la gestion du risque est une notion souvent mal comprise et et se concentre sur les risques posés par les menaces et les vulnérabilités au lieu des risques pour le fonctionnement et sur les résultats de l'entreprise. Souvent, l'accent est essentiellement mis, y compris dans l'évaluation de programmes de sécurité, sur les capacités d'un outil ou programme particulier à stopper un certain nombre d'attaques, au lieu de se concentrer sur des critères plus pertinents pour l'entreprise.

Au lieu de mesurer le volume d'attaques bloquées, l'objectif d'un programme complet de sécurité devrait être de comprendre le retour sur investissement de la gestion du risque, c'est à dire la réduction du risque sur l'investissement. Cela implique de trouver de meilleures façons d'appréhender les facteurs qui influencent significativement le coût total des risques liés à la cyber-sécurité et la manière de les gérer plus efficacement.

Pour commencer à y répondre, Juniper Networks a approché et parrainé des économistes et des experts en sécurité au sein de RAND afin d'analyser les principaux facteurs influençant le coût des risques liés à la cyber-sécurité pour les entreprises. Ces recherches examinent également les investissements possibles des entreprises pour gérer plus efficacement les risques que la menace croissante des cyberattaques fait peser sur leur réputation, leurs données et leurs réseaux.

RAND a déjà démontré sa capacité à fournir des analyses et idées objectives pour aider d'autres secteurs à appréhender des problèmes complexes, qu'il s'agisse de maîtriser les dépenses de santé ou de répondre à des enjeux de sécurité nationale et de budget de la défense. En analysant le problème urgent du coût de la cyber-sécurité pour les entreprises, l'organisation peut aider les professionnels et l'ensemble des acteurs de la cyber-sécurité à confirmer les problématiques auxquelles ils sont confrontés et à renforcer leurs argumentaires auprès des dirigeants sur la manière d'y faire face.

Un modèle heuristique des risques liés à la sécurité des entreprises

Le cœur des efforts de RAND a été de développer un modèle heuristique unique en son genre. Il fournit aux entreprises un outil d'apprentissage pour mieux comprendre les principaux facteurs influençant les coûts de la gestion des cyber risques et les différentes décisions d'investissement qui peuvent avoir une incidence sur ces coûts. En observant les interactions possibles entre ces facteurs, le modèle fournit un cadre de réflexion différent sur les choix en matière de cyber-sécurité.

Malgré l'existence de plusieurs modèles intéressants qui aident les entreprises à déterminer les risques spécifiques ou les informations les plus essentielles à protéger, tels que l'évaluation des menaces, ressources et vulnérabilités opérationnelles essentielles (« Operationally Critical Threat, Asset and Vulnerability Évaluation » ou OCTAVE) et l'analyse factorielle des risques liés aux informations (« Factor Analysis of Information Risk » ou FAIR), le modèle de RAND est le premier cadre qui représente le coût *global* de la gestion des risques liés à la cybersécurité. Il le fait en analysant la manière dont les choix effectués par les entreprises, combinés à l'introduction de nouvelles technologies et aux actions des cybercriminels, interagissent et influencent les coûts de la cyber-sécurité.

Le risque est défini par :

le coût pour les sociétés de se défendre
(outils, formation, gestion des périphériques personnels, isolement « air gap »)

+

le coût induit par une possible violation
(basé sur la valeur des informations menacées)

×

la probabilité d'une violation,
où 1,0 = 100 %
(en tenant compte de la surface d'attaque des logiciels et de l'efficacité des investissements de sécurité d'une entreprise)

Pour appréhender les risques dans leur globalité, le modèle de RAND analyse la manière dont les entreprises cherchent à minimiser le coût total de la cyber-sécurité. Cela inclut aussi bien les coûts directs qu'indirects de la prévention des cyberattaques, ainsi que les pertes potentielles résultant d'une attaque réussie, mesurés par la valeur des informations menacées et la probabilité d'une attaque aboutie.

> Le modèle de RAND est le premier système à cartographier le coût *global* de la gestion des cyber risques

Pour déterminer les dépenses pour l'entreprise, le modèle de RAND utilise 27 paramètres qui influencent les coûts sur une période de 10 ans. Chacun de ces paramètres peut être ajusté pour mesurer son impact sur les coûts.

Ils sont généralement répartis en trois catégories :

1. **Caractéristiques de l'entreprise :** taille de l'organisation, nombre de terminaux dans le réseau et valeur des informations menacées.
2. **Programme et investissements de sécurité :** le modèle permet aux entreprises de se pencher sur l'utilisation de quatre instruments différents, chacun ayant un coût mais réduisant aussi la probabilité d'une attaque réussie :
   - les coûts directs pour l'achat et l'utilisation d'outils de sécurité ;
   - les coûts directs et indirects des formations poussées sur les menaces destinées aux employés ;
   - les coûts indirects que représentent les pertes potentielles de productivité dues aux restrictions sur les périphériques intelligents et à l'isolement de type « air gap » des sous-réseaux particulièrement sensibles ;
   - les efforts des équipes de sécurité pour mettre en œuvre les programmes de sécurité.
3. **Évolution de l'écosystème :** l'impact des changements dans l'écosystème technologique sur le coût de la sécurité. Par exemple, comment l'introduction d'un nombre croissant de périphériques, due à l'Internet des objets, modifie la surface d'attaque ou comment le nombre de nouvelles vulnérabilités logicielles apparues dans une année donnée influence la probabilité d'une attaque réussie et les coûts qui en résultent.

Juniper estime que ce modèle fournit un point de départ systématique pour aider les RSSI à comprendre les différentes décisions qu'ils peuvent prendre pour protéger leur organisation et pour mieux mobiliser et obtenir l'appui de l'équipe de direction.

> Le modèle fournit un point de départ systématique pour aider les RSSI à comprendre les différentes décisions qu'ils peuvent prendre pour protéger leur organisation et pour mieux mobiliser et obtenir l'appui du reste de la direction.

Afin d'aider les entreprises à appliquer la plupart de ces paramètres à leur propre organisation, Juniper a développé une représentation interactive du modèle. Les utilisateurs peuvent modifier les principales variables, celles qui ont la plus grande influence sur les coûts, et ainsi commencer à identifier les meilleurs investissements en sécurité que les entreprises devraient envisager.

Les projections du modèle donnent plus des orientations générales que de diagnostiques précis, puisque les besoins et enjeux diffèrent selon les entreprises. Toutefois, cela constitue une base de discussion et un excellent point de départ pour les spécialistes de la sécurité cherchant à gagner un soutien en interne.

Pour les entreprises et les décideurs politiques qui veulent explorer l'intégralité du modèle de RAND, sa méthodologie complète est disponible en ligne.

FACTEURS ÉCONOMIQUES DE LA GESTION DES RISQUES DE LA CYBERSÉCURITÉ

Le modèle illustre les interactions entre les coûts dus aux cyberattaques et les dépenses qu'une entreprise consacre à sa sécurité.

LES COÛTS SONT DÉFINIS PAR LA SOMME DES :

pertes dues à une cyberattaque **+** coûts directs de formation des utilisateurs **+** coûts directs pour l'achat et l'utilisation d'outils de sécurité **+** coûts indirects dus aux restrictions sur les périphériques personnels ou intelligents **+** coûts indirects de l'isolement de type « air gap » des sous-réseaux sensibles

PERTES DUES À UNE CYBERATTAQUE

PROBABILITÉ D'UNE ATTAQUE

POUR UNE ENTREPRISE, LA PROBABILITÉ QU'UNE ATTAQUE ABOUTISSE DANS L'ANNÉE EST LE FACTEUR DES RÉSISTANCES RENCONTRÉES EN INTERNE ET EN EXTERNE.

×

IMPACT D'UNE ATTAQUE

LA GRAVITÉ POUR UNE ENTREPRISE D'UNE ATTAQUE RÉUSSIE EST DÉTERMINÉE PAR LA VALEUR DES INFORMATIONS EXFILTRÉES.

FACTEURS

RÉSISTANCE EXTERNE

- FORMATION DES EMPLOYÉS
- BYOD
- NOMBRE DE TERMINAUX
- CAPACITÉ DES TERMINAUX À RÉSISTER AUX INTRUSIONS

×

RÉSISTANCE INTERNE

- OUTILS

VALEUR A RISQUE

- ISOLEMENT DE TYPE « AIR GAP »

QUELQUES CHANGEMENTS DANS LE TEMPS :

- Croissance du nombre et des vulnérabilités des terminaux
- Évolution des pertes dues aux cyberattaques
- Arrivée de nouveaux outils de cybersécurité
- Baisse de l'efficacité de certains outils face aux contre-mesures

Les calculs ont été effectués pour l'année 0 (par exemple 2015) puis réitérées pour chacune des dix années suivantes.

Année 0 — Année 10

JUNIPER NETWORKS

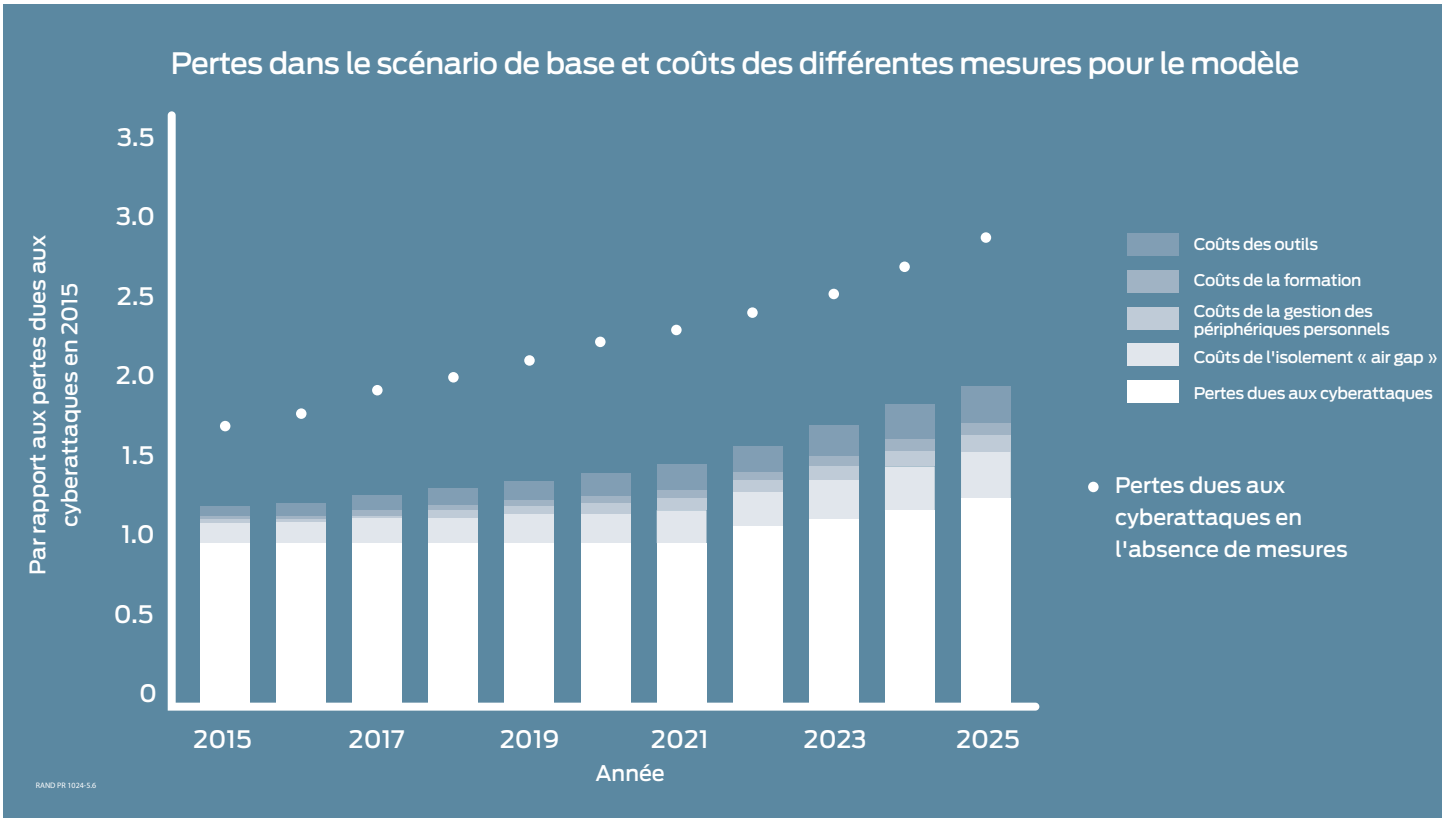
Ce que le modèle nous apprend sur l'évolution future de la sécurité

Ce qui importe encore plus que le fonctionnement du modèle, ce sont les conclusions auxquelles il aboutit. Le rapport de RAND fournit un cas d'usage basique du modèle, qui prend en compte les dépenses globales des entreprises et leur évolution sur 10 ans.

Le modèle de RAND laisse à penser que le coût de la gestion des cyber risques est appelé à augmenter de 38 % sur les 10 prochaines années, et ceci dans tous les secteurs.

> Le coût de la gestion des risques liés à la cybersécurité est appelé à augmenter de 38 % sur les 10 prochaines années, et ceci dans tous les secteurs.

Il est intéressant de noter que l'augmentation des coûts n'est pas entièrement due à l'augmentation des pertes liées aux cyberattaques. Elle découle principalement de l'augmentation des investissements dans des programmes de sécurité, notamment pour les entreprises qui souhaitent maîtriser les pertes potentielles (par exemple, l'investissement dans les outils de formation, les restrictions sur les périphériques personnels ou les périphériques intelligents, et l'isolement « air gap » du réseau). Cependant, ces investissements sont finalement rentables car, en leur absence, les pertes seraient beaucoup plus importantes et augmenteraient plus rapidement. Dans le graphique ci-dessous, la ligne en pointillés montre l'ampleur des pertes en l'absence d'investissement dans la protection de réseaux.



Principaux facteurs de coût pour les RSSI

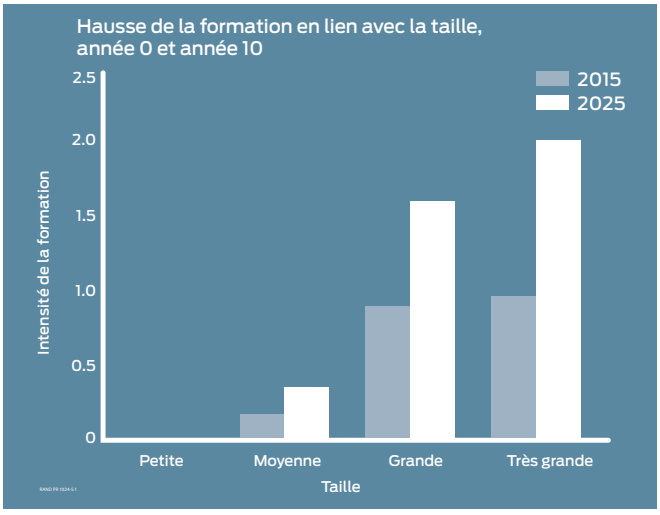
Le modèle de RAND fournit également de précieuses indications pour les entreprises. Juniper voit cinq principaux facteurs de coûts, confirmés par le modèle de RAND, qui doivent être pris en considération lorsque les entreprises développent leurs systèmes de sécurité. Alors que ces facteurs sont connus par les professionnels de la sécurité mais considérés comme anecdotiques, leur fort impact dans le modèle économique de RAND confirme leur importance.

1. Il n'existe pas d'approche standard : les entreprises n'adoptent pas une stratégie économique optimale

L'étude de RAND laisse à penser que, dans leurs investissements, de nombreuses entreprises ne suivent sans doute pas une stratégie économique optimale. Le niveau optimal d'outils de sécurité, de formation pour les employés, de restrictions sur les périphériques personnels et l'identification des réseaux à isoler d'Internet varient considérablement d'une entreprise à l'autre.

Petites et moyennes entreprises

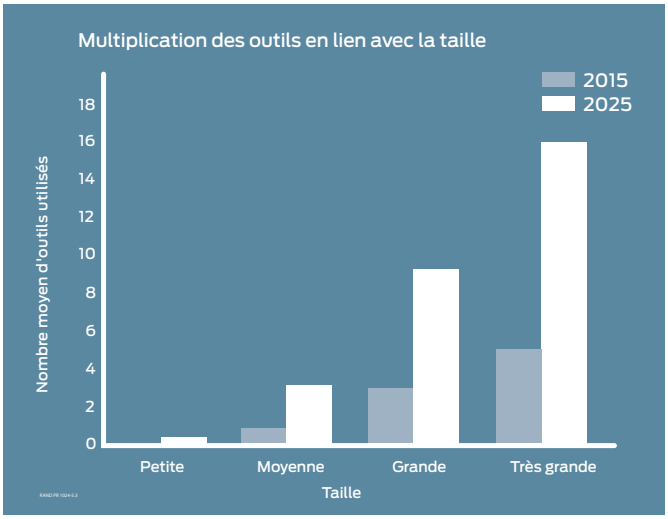
Les petites et moyennes entreprises (PME) sont celles qui bénéficient le plus des outils et processus basiques, sans devoir surinvestir dans des formations complexes sur la sécurité ou dans des technologies de sécurité plus avancées. Parce que les PME ont une surface d'attaque beaucoup plus petit et sont moins susceptibles de faire face à des attaques sophistiquées, surinvestir dans la sécurité serait disproportionné par rapport à la probabilité d'un piratage et aux pertes potentielles qu'elles subiraient en conséquence. Au contraire, des outils et des politiques basiques aident à protéger au mieux les PME en sécurisant leur réseau et en y limitant l'utilisation de périphériques personnels.



Grandes sociétés et cibles à forte valeur

Inversement, les grandes sociétés ou celles disposant d'informations hautement sensibles, comme les entreprises du secteur de l'armement ou celles pour qui la propriété intellectuelle est déterminante, ont besoin d'investir dans une gamme complète d'outils et de politiques. Elles sont beaucoup plus susceptibles d'être la cible d'attaques sophistiquées, de devoir faire face à un volume plus élevé d'attaques quotidiennes, ou d'être confrontées à tout type d'intrusion. En l'absence d'investissements importants, les pertes suites à un incident serait énormes.

En outre, les grandes entreprises sont susceptibles de bénéficier d'économies d'échelle dans leurs investissements en matière de sécurité. Par exemple, une formation avancée sur la sécurité devient plus rentable par personne quand le nombre d'employés augmente.



En supposant l'existence d'outils standards et de formations basiques de sensibilisation à la sécurité.

2. Nombre d'outils ont une « demi-vie » et perdent de la valeur

Le s contre-mesures utilisées par les cybercriminels pour contourner les défenses constituent l'un des plus grands défis auxquels doivent faire face les entreprises. Les cybercriminels développent continuellement des contre-mesures aux nouvelles technologies de sécurité, ce qui limite l'efficacité relative de ces outils et oblige les entreprises à les remplacer.

C'est le cas, par exemple, des systèmes de détection comme les sandboxes ou les antivirus. Bien que très utiles au départ et indispensables dans la stratégie de sécurité des grandes entreprises, ces types de défenses sont sujets aux contre-mesures. Par conséquent, ils doivent être continuellement réévalués et de nouvelles solutions doivent être mises en place pour que les défenses restent efficaces contre les attaques. C'est bien le fait que chaque mesure engendre une contre-mesure (une « dynamique contradictoire ») qui constitue la cause profonde de l'escalade en matière de cybersécurité.

Cette escalade finit par augmenter, pour les entreprises, le budget nécessaire en technologies de sécurité pour maintenir le même niveau de protection. Elle augmente également les coûts d'exploitation des entreprises, qui se retrouvent souvent avec un ensemble de plus en plus hétéroclite de technologies à gérer par les équipes de sécurité.

Le modèle de RAND prévoit que, sur la durée, *l'efficacité de ces technologies sujettes aux contre-mesures baissent de 65 % sur 10 ans*. En conséquence, le montant total que les entreprises devraient dépenser en outils de sécurité par rapport au coût total de la sécurité pour l'organisation augmente de 16,2 % entre la première et la dernière année du modèle. Hors contexte, ce chiffre peut sembler faible mais il reste important dans la mesure où les outils de sécurité représentent un coût majeur pour les entreprises.

Où les entreprises devraient-elles donc concentrer leurs investissements ? RAND a également constaté que certains outils de sécurité sont moins sujets aux contre-mesures. Dans cette catégorie, on trouve les technologies et les systèmes de sécurité orientés sur l'amélioration de la gestion de la sécurité et des correctifs, l'automatisation et l'amélioration de la mise en œuvre effective des politiques de sécurité sur l'ensemble du réseau de l'entreprise. Ce ne sont pas là les types d'outils que les cybercriminels essayeront de contourner.

La plupart des entreprises auront donc besoin, pour protéger leurs systèmes, d'un ensemble d'outils des deux catégories. Cependant, le plus important d'après Juniper est que les entreprises comprennent l'existence de cette dynamique et la prennent en compte lors de l'évaluation de nouveaux investissements.

Vulnérables aux contre-mesures

- Détection des anomalies
- Détection de signature
- Utilisation de sandboxes pour les logiciels malveillants
- Contre-attaques actives
- Sensibilisation au phishing

Moins vulnérables aux contre-mesures

- Automatisation et mise en œuvre effective de la politique de pare-feu
- Authentification multi-facteurs
- Gestion automatisée des correctifs et surveillance des versions de correctifs
- Isolement des sous-réseaux
- Contrôle d'accès aux réseaux

3. L'impératif humain : investir dans la compétence permet de réduire les coûts sur le long terme

L'investissement dans la formation et la constitution d'une équipe de sécurité vigilante sont parmi les facteurs qui, d'après le modèle de RAND, pourraient réduire considérablement les coûts liés à la sécurité. Une équipe de sécurité compétente et bien dotée en personnel est tout aussi importante sinon plus que les investissements dans de nouveaux outils. Mêmes les meilleurs outils se révèleront inefficaces s'ils ne sont pas correctement gérés, ce que prend en compte le modèle.

Selon le modèle de RAND, *les entreprises faisant preuve d'une vigilance élevée, c'est à dire celles où le personnel informatique et de sécurité est le plus efficace pour gérer les programmes de sécurité, sont en mesure de réduire les coûts de cybersécurité de 19 % la première année et de 28 % au cours de la dixième année du modèle,* par rapport aux entreprise très peu vigilantes.

Juniper estime que malgré la pénurie réelle d'experts en sécurité ces économies potentielles sont trop importantes pour être ignorées.

Les entreprises doivent redoubler d'efforts pour investir dans la formation et pour renforcer leurs équipes de sécurité. S'il s'avère impossible de recruter du personnel, la sous-traitance de la gestion de fonctions spécifiques de sécurité à des experts externes est une autre approche possible. Le rapport de RAND suggère qu'optimiser les services externalisés peut offrir des avantages :

> *De nombreux défenseurs choisissent d'externaliser certaines fonctions défensives importantes à des spécialistes qui peuvent fournir un service particulier à un plus large éventail de clients. Par exemple, de nombreuses grandes sociétés n'effectuent pas elles-mêmes les tests de pénétration de leur réseau parce que cette discipline est tellement spécialisée qu'il est difficile de recruter et de maintenir le personnel à son potentiel le plus élevé.*[1]

2015

Niveau de vigilance	Différence du coût des attaques
Très faible	+13 %
Faible	+10 %
Moyenne	Neutre
Élevé	Neutre
Très élevé	-6 %

2025

Niveau de vigilance	Différence du coût des attaques
Très faible	+18 %
Faible	+13 %
Moyenne	Neutre
Élevé	-6 %
Très élevé	-10 %

[1] « The Defender's Dilemma: Charting a Course Toward Cybersecurity », RAND Corporation, 2015, Martin Libicki, Lillian Ablon et Timothy Webb.

4. L'Internet des objets est à la croisée des chemins

On parle beaucoup de l'Internet des objets, parfois même un peu trop. Mais une chose est sûre : dans un avenir proche, les entreprises auront sur leurs réseaux plus de périphériques que jamais. Selon RAND, l'Internet des objets aura un impact sur le montant global des coûts liés à la sécurité. Cependant, il est difficile de savoir si cela sera positif ou négatif. D'après Juniper, les entreprises sont ainsi à la croisée des chemins.

Si elles parviennent à gérer correctement les questions de sécurité qu'implique l'Internet des objets en mettant en œuvre de manière intelligente et sophistiquée des technologies de sécurité et une gestion des périphériques, elles pourraient réaliser à long terme des économies, le nombre de périphériques dans leur réseau dépassant celui des terminaux traditionnels. D'un autre côté, si l'Internet des objets connaît une évolution comparable à celle des ordinateurs à leur début, quand ils souffraient d'une myriade de problèmes de sécurité, les entreprises devront faire face à une flambée des coûts liés à la sécurité.

Dans ce scénario-là, le modèle de RAND indique que l'introduction de l'Internet des objets augmentera les pertes subies par les entreprises à cause des cyberattaques de 30 % sur 10 ans.

Si la plupart des entreprises ne ressentiront pas l'impact réel de l'Internet des objets avant plusieurs années, Juniper estime qu'elles devraient commencer dès maintenant à réfléchir attentivement à l'intégration de ces périphériques dans leurs réseaux et programmes de sécurité. Les entreprises devront veiller à ce que la performance de leur infrastructure de sécurité soit capable de gérer l'augmentation de la bande passante liée à ces nouveaux types de connexions et périphériques.

De plus, les entreprises devront déterminer les contrôles de sécurité qui doivent être mis en place pour régir ces nouveaux périphériques introduits dans l'environnement de l'entreprise. De la même façon que sont actuellement gérés les périphériques personnels, les entreprises doivent s'assurer dès aujourd'hui qu'elles disposent des outils nécessaires pour rapidement établir et gérer les objets qui, dans un avenir proche, se connecteront à leurs réseaux. Cela implique la définition et la mise en œuvre d'une gestion appropriée des droits afin d'éviter que ces nouveaux périphériques n'augmentent pas la surface d'attaque. La définition de politiques claires en interne quant à l'utilisation des objets connectés en entreprise est également de mise.

5. L'élimination des failles logicielles réduit considérablement les coûts

Le nombre de vulnérabilités exploitables dans les logiciels et les applications qu'ils utilisent est un élément qui, d'après RAND, a une influence massive sur les coûts. Les entreprises doivent souvent investir dans des mesures défensives parce que des systèmes ou logiciels fondamentaux ne sont pas sécurisés. Malheureusement, les RSSI n'ont que peu d'influence sur cet indicateur en particulier et ce sont les éditeurs de logiciels qui doivent produire des codes plus sécurisés.

Le modèle de RAND a constaté que si la fréquence des vulnérabilités des logiciels était divisée de moitié, le coût global pour les entreprises de la cybersécurité diminuerait de 25 %.

Cependant, on peut douter que les logiciels soient à l'avenir moins vulnérables. Si les architectures réseaux et logiciels ne changeaient pas, les défenseurs finiraient par prendre le dessus - mais l'innovation est la pierre angulaire du secteur des technologies de l'information.

L'étude de RAND suggère que le nombre de nouvelles vulnérabilités pourrait augmenter avec la multiplication des objets connectés et avec la complexité croissante des écosystèmes de logiciels construits sur des versions précédentes de code.

L'amélioration continue de la qualité des logiciels est rassurante. Par exemple, des outils gratuits sont maintenant à la disposition des développeurs pour les aider à identifier les vulnérabilités avant de livrer leurs produits. Plus les éditeurs de logiciels utilisent ces outils, plus le nombre de vulnérabilités découvertes dans leurs produits devrait baisser.

D'après Juniper, il incombe également aux entreprises d'examiner les logiciels qu'elles utilisent et d'exiger des éditeurs de logiciels de meilleurs tests de sécurité et de meilleurs correctifs. Si les entreprises cessent d'utiliser un certain programme à cause de ses failles de sécurité, les éditeurs seront plus enclins à offrir des produits de meilleure qualité et présentant moins de vulnérabilités.

La voie à suivre pour les entreprises et l'ensemble du secteur

Que peuvent donc faire les entreprises pour mieux gérer leurs investissements contre les cyber risques à une époque où la menace ne cesse d'augmenter ?

Gérer le portefeuille de sécurité comme une entreprise

Les entreprises doivent trouver une meilleure façon de gérer leur sécurité comme elles le font pour d'autres aspects de leur business : en quantifiant les risques et les bénéfices des différents choix. Juniper voit dans le modèle de RAND plusieurs pistes de mesures concrètes que les entreprises devraient prendre en considération lorsqu'elles évaluent leur stratégie et leurs dépenses en matière de sécurité.

Au bout du compte, les RSSI doivent s'efforcer d'avoir de meilleurs paramètres pour déterminer la réduction du risque sur investissement. En bref, les entreprises doivent régulièrement évaluer le cycle de vie et l'efficacité de leurs programmes - de la même manière qu'on gérerait un portefeuille d'actions de l'entreprise. C'est là que la représentation interactive de Juniper et l'intégralité du modèle de RAND et sa méthodologie complète sont utiles pour déterminer les outils les plus efficaces permettant de répondre aux besoins spécifiques de chaque entreprise.

Évaluer les outils de sécurité en gardant à l'esprit les contre-mesures

Comme le montre RAND, « les choix organisationnels peuvent, et devraient, être influencés par le risque de contre-mesures à tout investissement réalisé, notamment dans les défenses systémiques... Les entreprises devraient songer à installer le type de mesures qui est le moins susceptible d'attirer de contre-mesures ».

D'après Juniper, les entreprises doivent donc privilégier les investissements dans des outils qui automatisent les tâches de sécurité par une gestion centralisée et une mise en œuvre distribuée, en particulier pour la sécurisation des réseaux. L'automatisation est un aspect sur lequel Juniper se concentre. Plusieurs raisons doivent encourager les entreprises à investir dans des outils d'automatisation :

- les outils avec automatisation intégrée sont moins sujets aux contre-mesures, ce qui les aide à garder leur efficacité au fil du temps et à maintenir leur valeur ;
- l'automatisation peut, pour les entreprises, réduire d'autres coûts liés à la sécurité en soulageant des équipes informatiques déjà très sollicitées ;
- l'automatisation permet au personnel de sécurité de passer moins de temps à configurer et à tester les systèmes, pour se concentrer davantage sur des tâches essentielles comme parer aux attaques les plus sophistiquées et renforcer leur stratégie de défense ;
- enfin, un système centralisé peut augmenter le bénéfice tiré d'autres investissements dans la sécurité en rendant ceux-ci plus faciles à gérer et à exécuter. Une gestion automatisée et centralisée de la détection des menaces permet d'avoir des sources d'informations claires sur les menaces et des réponses sur l'ensemble du réseau.

Vous trouverez de plus amples informations sur le travail et les investissements de Juniper dans l'automatisation en cliquant ici.

Le secteur doit se mobiliser

Les RSSI ne doivent pas être les seuls à œuvrer pour le progrès de la sécurité. Juniper considère qu'il est impératif que l'ensemble des acteurs dans le domaine de la sécurité ainsi que les gouvernements prennent des mesures fortes pour changer la dynamique actuelle et faire pencher la balance en faveur de la défense.

Former la génération suivante

La clé pour devancer les cybercriminels est de former la prochaine génération de développeurs pour qu'ils sécurisent mieux les innovations qu'ils créent. Le rapport de RAND va aussi dans ce sens, indiquant que « ... la programmation sécurisée ne fait pas partie de la plupart des diplômes en informatique. Ce sont les étudiants d'aujourd'hui qui développeront et créeront les périphériques de demain ».

Si la prochaine génération peut être formée à créer des logiciels intrinsèquement plus sûrs, le risque de piratage pourrait être considérablement réduit, ce qui diminuerait le coût global de la sécurité pour les entreprises.

Former les étudiants à la sécurité susciterait des vocations et les aiderait à être plus efficaces dans leur travail. En lançant le mouvement maintenant, le secteur de la sécurité pourra enfin pallier à une pénurie de main d'œuvre. De plus, en apprenant l'éthique, les futurs cybercriminels pourraient faire bon usage de leurs compétences au lieu de rejoindre le marché noir de la cyber-sécurité.

Développer la technologie en gardant à l'esprit les contre-mesures

Ceux qui, comme Juniper, innovent dans la sécurité, doivent continuer à créer des technologies conçues pour résister aux contre-mesures des cybercriminels et à améliorer la visibilité et le contrôle sur le réseau. Jamais le jeu du chat et de la souris entre cybercriminels et défenseurs ne prendra fin, mais un effort plus concerté pourrait donner un avantage aux nouvelles technologies face aux cybercriminels.

Nous ne prétendons pas que ce rapport ou ce modèle soit la touche finale à la compréhension des cyber-risques. Il devrait être le point de départ d'un débat nécessaire au sein du secteur sur la façon dont il appréhende le risque. Nous espérons que notre collaboration avec RAND permettra d'avancer et d'initier de nouveaux débats.

Vous trouverez le rapport complet de la RAND Corporation, ainsi que le rapport de l'année dernière et des documents supplémentaires de Juniper, en cliquant ici.

À propos du rapport

« The Defender's Dilemma: Charting a Course Toward Cybersecurity » a été rédigé par Martin Libicki, Lillian Ablon et Timothy Webb, experts en sécurité de la RAND Corporation. Il s'appuie sur des entretiens approfondis de responsables de la sécurité, menés entre octobre 2013 et août 2014, autour des menaces actuelles et émergentes. Cette étude se fonde sur le premier rapport d'une série, en deux parties, réalisée par RAND et parrainée par Juniper. Celui-ci, intitulé « Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar », examinait les facteurs économiques influençant les cybercriminels et le marché noir souterrain très sophistiqué qu'ils ont créés pour soutenir leurs efforts.

Siège social et direction des ventes

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Tél. : +1 408 745 2000 ou 888 JUNIPER (888 586 4737)
Fax : +1 408 745 2100
www.juniper.net

Direction pour l'Asie-Pacifique et l'Europe, et le Moyen-Orient

Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, Pays-Bas
Tél. : +31 0 207 125 700
Fax : +31 0 207 125 701

Juniper Networks (NYSE : JNPR) propose des solutions innovantes de routage, de commutation et de sécurité. Les innovations logicielles, silicium et systèmes de Juniper Networks transforment l'expérience des réseaux et le modèle économique associé. Pour en savoir plus, rendez-vous sur Juniper Networks (www.juniper.net) ou rapprochez-vous de Juniper via Twitter et Facebook.