ENTREPRISES, ÉVALUEZ LA RENTABILITÉ DE VOS INVESTISSEMENTS EN CYBERSÉCURITÉ

Le monde de l'entreprise a toujours cherché à exploiter au maximum les ressources informatiques au coût le plus bas possible, mais en évaluer le retour sur investissement n'est pas aussi simple.

RÉSUMÉ ANALYTIQUE

En cas de faille de sécurité, chaque seconde compte et coûte de l'argent. Mais les entreprises sont peu nombreuses à pouvoir déterminer le retour sur investissement lié à leurs initiatives en matière de cybersécurité. Comment en déterminer la valeur ? Et si l'estimation des différents profits possibles pouvait permettre à votre entreprise de se concentrer sur des solutions de cybersécurité parfaitement adaptées, et optimiser ainsi son retour sur investissement ?

La solution de cybersécurité que vous mettez en œuvre impacte votre retour sur investissement :

Classique/ traditionnelle : généralement sur site et prise en charge par des équipes informatiques importantes au sein de grandes entreprises

Solution Cloud : gérée via une console d'administration et des outils basés dans le Cloud, sans matériel supplémentaire.

Externalisée : un fournisseur de services tiers (fournisseur de services gérés - MSP) s'occupe de tout.

Chacune présente ses propres avantages et impacts sur le budget. Mais pour des entreprises disposant de ressources limitées, ou qui préfèrent externaliser la gestion auprès d'un fournisseur tiers, la cybersécurité dans le Cloud constitue la meilleure solution, en termes de facilité de gestion et de rentabilité.

LORSQUE MOINS PERMET DE FAIRE PLUS

« Être plus performant tout en faisant appel à des ressources plus limitées ». Telle est la devise que les entreprises ont adoptée depuis quelques années, devise que les professionnels de l'informatique connaissent déjà fort bien. Le monde de l'entreprise a toujours cherché à exploiter au maximum les ressources informatiques au coût le plus bas possible. Or, le véritable enjeu des services informatiques consiste actuellement à s'adapter à l'évolution toujours plus complexe en s'appuyant sur des ressources moindres.

En matière de cybersécurité, les entreprises de toute taille peinent à suivre l'évolution constante des menaces tout en contrôlant une palette toujours plus large d'appareils, d'applications et d'utilisateurs finaux.

En 2013, selon PriceWaterhouseCooper, le recrutement de personnel spécialisé dans la cybersécurité a baissé. À cette période, les recherches de Kaspersky Lab ont révélé que 58 % des entreprises ont reconnu un manque de ressources pour assurer la sécurité informatique (soit en termes de personnel, de systèmes ou de connaissances). Au quatrième trimestre 2016, les entreprises évoquent un manque de cybercompétences et augmentent leur budget pour pallier à cette pénurie.

Mais ce n'est pas uniquement une question de compétences : aujourd'hui, 40 % des entreprises mentionnent la complexité accrue de l'infrastructure comme un facteur important d'augmentation des budgets de sécurité informatique. Il est intéressant de constater que personne ne semble véritablement savoir ce que représente le retour sur investissement lié à leurs initiatives en matière de cybersécurité : 62 % des grandes entreprises et 59 % des PME révèlent qu'elles continueront à réaliser des investissements, indépendamment de leur capacité à évaluer le rendement.

Comment les entreprises peuvent-elles alors déterminer la rentabilité liée aux investissements en matière de cybersécurité ? Et si l'évaluation des différents profits pouvait permettre à votre entreprise de se concentrer sur des solutions de cybersécurité parfaitement adaptées, et optimiser ainsi son retour sur investissement ?

FONDAMENTAUX DE LA CYBERSÉCURITÉ

La gestion de la cybersécurité représente un coût, et pour déterminer les retours sur investissement, il faut tenir compte de trois domaines clés étroitement liés autour desquels elle s'articule : les investissements, les dépenses d'exploitation et les ressources humaines. En clair, il s'agit de déterminer l'importance de l'investissement, les coûts liés à la gestion de la solution et le personnel chargé de superviser ces deux domaines.

COMMENÇONS PAR LES INVESTISSEMENTS :

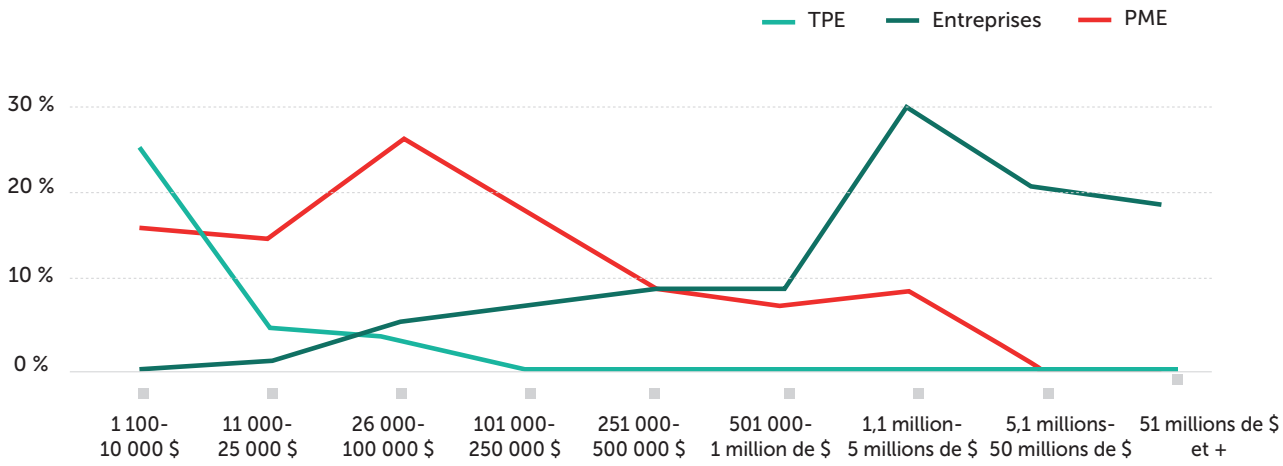
Si vous êtes responsable de la sécurité des systèmes d'information ou de la cybersécurité, vous serez ravi d'apprendre que les budgets sont en augmentation, avec l'approbation de la direction : 38 % des grandes entreprises et 33 % des PME indiquent que leur direction leur demande d'accroître les investissements en matière de cybersécurité.

Le revers de la médaille est que, bien entendu, les attentes en termes de solutions sont plus grandes. Seul bémol : les investissements plus importants en matière de cybersécurité peuvent être source de complexité. En effet davantage de matériels, d'appareils et d'applications doivent être intégrés, gérés et surveillés. En réalité, 25 % d'augmentation des fonctionnalités génèrent une augmentation de la complexité des tâches de 100 %. Pour 55 % des PME, le volume grandissant d'appareils qu'elles doivent sécuriser représente une difficulté majeure.

Qui va gérer tout cela ?

Ce qui nous amène aux dépenses d'exploitation et aux ressources humaines, toutes deux liées aux compétences...

Budget de sécurité informatique



Pourcentage des entreprises avec leur budget de sécurité informatique par tranche.

LE FACTEUR HUMAIN : ÉVALUATION DU COÛT LIÉ À UNE PÉNURIE DE CYBERCOMPÉTENCES

En dépit du fait que plus de la moitié (54 %) des PME sont convaincues que leur sécurité informatique sera compromise à un moment donné, en sachant que la préparation joue un rôle essentiel dans la prévention et la détection, 40 % révèlent qu'elles ne disposent pas de suffisamment de connaissances ou d'informations sur les menaces auxquelles elles sont confrontées.

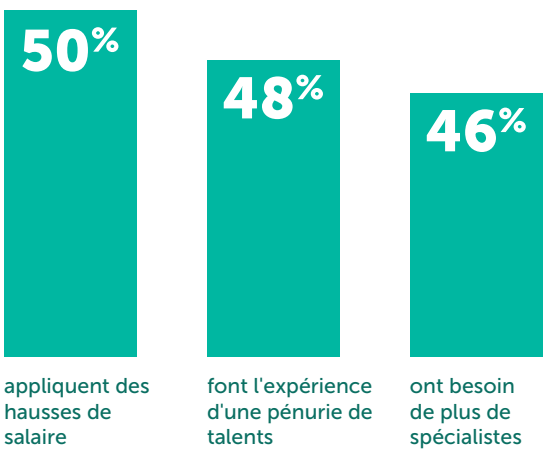
Si l'on considère qu'une équipe informatique de 16 personnes dans une PME ne dispose en moyenne que de 2 experts en cybersécurité, on comprend aisément la raison pour laquelle les ressources humaines jouent un rôle au moins tout aussi important dans la planification de la cybersécurité que la technologie ou l'infrastructure. Rien d'étonnant à ce que plus d'un tiers des entreprises du monde entier considèrent l'amélioration de l'expertise spécialisée en matière de sécurité comme l'un des trois principaux moteurs de l'investissement dans la sécurité informatique, la moitié reconnaissant une pénurie de talents.

Le plus inquiétant dans tout cela ?
Une étude révèle une distinction claire entre la disponibilité des talents et le coût lié à la restauration après une faille de sécurité : les entreprises qui peinent à recruter les meilleurs talents dans la sécurité dépensent en moyenne trois fois plus pour se remettre d'une faille de sécurité. Le montant important des frais de restauration est dû aux salaires du personnel supplémentaire (14 000 $ en moyenne pour les PME).

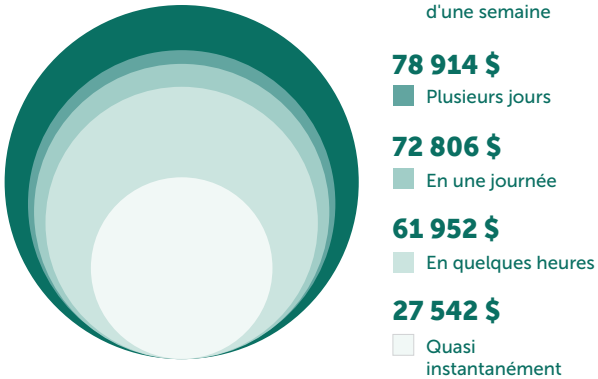
L'adage selon lequel « le temps c'est de l'argent » peut tout à fait s'appliquer à la cybersécurité. En cas de faille de sécurité, chaque seconde compte et coûte de l'argent. Une faille détectée quasi instantanément coûte en moyenne 28 000 $ aux PME, pouvant atteindre 105 000 $ si elle n'est pas détectée pendant plus d'une semaine. En termes de données, une moyenne de 417 dossiers sont compromis, même avec une détection instantanée. Ce chiffre passe à plus de 70 000 si la faille n'est pas détectée pendant plus d'une semaine.

En résumé : les ressources humaines sont aussi importantes que les ressources technologiques pour lutter contre les cybermenaces. Ce qui compte, c'est de trouver le juste équilibre pour votre entreprise.

Le facteur humain



Le temps c'est de l'argent



LA SOLUTION DE CYBERSÉCURITÉ QUE VOUS METTEZ EN ŒUVRE IMPACTERA VOTRE ROI

La cybersécurité pour les entreprises se décline en trois versions :

Classique/ traditionnelle
Généralement sur site et prise en charge par des équipes informatiques importantes au sein des grandes entreprises

Solution Cloud
Gérée via une console d'administration et des outils basés dans le Cloud, sans matériel supplémentaire.

Externalisée
Un fournisseur de services tiers (fournisseur de services gérés - MSP) s'occupe de tout.

Chacune présente ses propres avantages et impacts sur le budget.

SÉCURITÉ TRADITIONNELLE SUR SITE :

L'approche traditionnelle correspond au programme de cybersécurité « maison ». Des équipes de décideurs technologiques, financiers et commerciaux internes à l'entreprise choisissent la ou les solutions les plus adaptées aux besoins de l'entreprise, y compris les ressources matérielles permettant de les prendre en charge, et gèrent le tout en interne elles-mêmes. Cette version a l'avantage de permettre un contrôle maximum de la sécurité. En revanche, vous devez disposer des compétences et des ressources internes pour exploiter cet avantage.
Les entreprises qui choisissent de faire appel à différents fournisseurs pour différents composants de leur sécurité sont également confrontées au double problème que représentent la complexité et l'intégration, des domaines qui imposent des contraintes supplémentaires sur les ressources internes.
Les entreprises qui utilisent des approches traditionnelles en matière de cybersécurité sont en mesure de réduire les coûts en optant pour des solutions qui proposent des consoles d'administration centralisées, des fonctionnalités de gestion et d'automatisation des systèmes avancées ainsi que la possibilité de sécuriser et de contrôler des appareils hétérogènes.
Vous réduirez le temps que les administrateurs consacrent aux tâches quotidiennes mais à terme, vous devrez malgré tout disposer des compétences requises pour assurer le bon fonctionnement de l'infrastructure.

COÛTS HABITUELS ($)*	COÛTS ANNUELS ($)
Coûts approximatifs pour une entreprise disposant de deux bureaux et de 100 terminaux au total	
Bureaux connectés à un réseau	
Ressources pour l'administration de la sécurité informatique : 4 000 $ par mois	**48 000**
Matériel : au moins 3 000 $	**coût unique**
Logiciel de cybersécurité : 4 614 € (environ 4 800 $) pour une licence d'un an	**4 800**
Acquisition de compétences en interne : 1 500 $ par an	**1 500**
COÛTS ANNUELS TOTAUX	**54 300**
COÛT UNIQUE TOTAL	**3 000**

**Coûts approximatifs communiqués à titre indicatif uniquement. Les coûts relatifs à des situations spécifiques peuvent être différents.*

SÉCURITÉ DANS LE CLOUD :

Avec près des deux tiers des PME utilisant déjà en moyenne trois solutions Cloud, il n'est pas surprenant de constater que la sécurité dans le Cloud est l'une des options enregistrant la croissance la plus rapide. Le faible coût d'accès, la facilité de gestion et la flexibilité des options de licences sont parfaitement adaptés aux PME qui souhaitent évoluer à la demande, quelle que soit l'orientation.

Côté budget, l'intérêt d'une sécurité basée dans le Cloud réside dans la rapidité avec laquelle elle peut être déployée. Elle offre, en outre, une plus grande facilité de gestion sans investissement matériel supplémentaire. Dans la mesure où l'ensemble de l'infrastructure requise est hébergée par le fournisseur dans le Cloud, les clients ne sont pas tenus d'acheter ou de gérer un serveur (ou d'en obtenir la licence) pour leur centre d'administration. Les plus petites entreprises peuvent ainsi s'appuyer sur des solutions de sécurité à la pointe de la technologie sans avoir à recruter de personnel compétent supplémentaire ou acquérir du matériel haut de gamme pour les gérer. Pour les PME qui peinent à développer leur expertise pour se protéger contre des menaces de plus en plus sophistiquées, c'est une solution gagnant-gagnant.

Cela s'explique avant tout par le fait que la console d'administration basée dans le Cloud permet de gérer plusieurs terminaux, appareils mobiles et serveurs de fichiers à distance, depuis n'importe quel endroit. Les solutions sont généralement prêtes à être exécutées et très intuitives. Autrement dit, les administrateurs informatiques ne disposant pas de compétences spécialisées en matière de sécurité peuvent facilement utiliser des fonctionnalités de sécurité très performantes. Les politiques de sécurité par défaut développées par des analystes compétents en cybersécurité permettent de bénéficier en interne d'informations prêtes à l'emploi et de bonnes pratiques sans qu'il soit nécessaire de recruter des gens ou de former des collaborateurs pour utiliser la nouvelle console d'administration dans le Cloud. Toutes les solutions sont intuitives et prêtes à être exécutées.

Comme tout est centralisé, les administrateurs des solutions de sécurité basées dans le Cloud peuvent contrôler le statut de sécurité de 1 000 postes du réseau d'entreprise depuis l'appareil en ligne de leur choix et à partir de n'importe quel endroit. Le suivi des rapports et des licences peut s'effectuer en toute simplicité depuis une interface simple d'utilisation et intuitive. Vous bénéficiez d'une sécurité optimale tout en tirant pleinement parti de votre personnel actuel.

COÛTS HABITUELS ($)*	COÛTS ANNUELS ($)
Coûts approximatifs pour une entreprise disposant de deux bureaux et de 100 terminaux au total	
Aucune nécessité de connecter des bureaux à un réseau	
Ressources d'administration : 2 000 $ par mois	24 000
Frais de licence : 200 € (environ 208 $) par mois	2 500
Compétences de base requises en interne : 700 $ par an	700
COÛTS ANNUELS TOTAUX	**27 200**
COÛT UNIQUE TOTAL	**0**

**Coûts approximatifs communiqués à titre indicatif uniquement. Les coûts relatifs à des situations spécifiques peuvent être différents.*

EXTERNALISATION AUPRÈS D'UN FOURNISSEUR DE SERVICES GÉRÉS

Cette option permet d'étendre la sécurité basée dans le Cloud. Plutôt que de confier l'exécution des contrôles dans le Cloud à une personne en interne, l'entreprise peut externaliser cette gestion auprès d'un tiers spécialisé qui n'est pas tenu d'être sur site. Vous bénéficiez de tous les avantages d'une solution de sécurité leader tout en préservant vos budgets. Rien d'étonnant à ce que 40 % des PME et 26 % des TPE révèlent que les MSP pourraient répondre à leurs besoins en matière de sécurité. Près d'un quart des PME prévoient d'adopter cette approche de la sécurité au cours des 12 prochains mois.

L'externalisation de la sécurité auprès d'un MSP permet aux entreprises de toute taille de bénéficier d'un accès aux meilleurs talents dans ce domaine sans avoir à investir ou acquérir une expertise pour la gérer elles-mêmes. Les PME peuvent mettre en œuvre des solutions professionnelles sans se préoccuper du budget. En outre, grâce à l'expertise interne du MSP, vous pouvez réaliser des économies sur la sécurité et sur la veille sur les menaces les plus récentes. À l'instar des solutions basées dans le Cloud, l'option MSP offre une grande flexibilité : dans la mesure où l'éditeur du logiciel est en charge de l'infrastructure, le MSP peut très facilement s'adapter à votre saisonnalité ou à d'autres besoins, comme l'acquisition de nouvelles options par exemple. Vous vous déchargez ainsi des tâches liées notamment à la gestion des licences.

COÛTS HABITUELS ($)*	COÛTS ANNUELS ($)
Coûts approximatifs pour une entreprise disposant de deux bureaux et de 100 terminaux au total	
Aucune nécessité de connecter des bureaux à un réseau mais ils doivent se situer à une distance raisonnable d'un partenaire MSP.	
Ressources informatiques : 3 000 $ par mois	**36 000**
Aucune compétence requise en interne	**0**
COÛTS ANNUELS TOTAUX	**36 000**
COÛT UNIQUE TOTAL	**0**

**Coûts approximatifs communiqués à titre indicatif uniquement. Les coûts relatifs à des situations spécifiques peuvent être différents.*

CHOISIR LA SOLUTION LA MIEUX ADAPTÉE

La complexité compromet la sécurité, l'efficacité et la croissance. Elle est à l'origine d'erreurs et limite votre capacité à gérer le changement. Les professionnels de l'informatique sont tout à fait conscients de ces problématiques. Mais quelle solution adopter pour atténuer ces problèmes sans pour autant ajouter des restrictions aux utilisateurs finaux ou surcharger des ressources déjà bien sollicitées ?

En explorant des options de cybersécurité que vous n'avez pas encore envisagées, (solution dans le Cloud ou fournisseur MSP), vous pouvez améliorer le retour sur investissement de votre sécurité. Offrez davantage de temps à vos administrateurs informatiques et réduisez la nécessité de disposer d'une expertise interne ou de nouveaux matériels grâce à une sécurité dans le Cloud ou externalisée. Ou bien, optez pour une solution traditionnelle sur site qui vous permet de bénéficier de contrôles centralisés et de fonctionnalités de gestion des systèmes avancées afin d'exploiter pleinement vos ressources humaines internes et celles de votre l'infrastructure.

La meilleure solution a toujours consisté à se préparer avant qu'un problème ne survienne. Si vous ne trouvez pas de talents supplémentaires ou ne pouvez pas vous permettre de les recruter, mieux vaut optimiser les capacités du personnel actuel en simplifiant leur travail. Kaspersky Lab peut vous accompagner, quel que soit votre choix.

ÊTES-VOUS PRÊT À CHOISIR VOTRE ARME EN MATIÈRE DE SÉCURITÉ INFORMATIQUE ?

Si vous pouvez déterminer l'approche de cybersécurité la plus adaptée à votre entreprise, c'est le moment de mettre la théorie en pratique...

Êtes-vous une entreprise disposant d'une cybersécurité sur site ? Téléchargez votre évaluation gratuite de **Kaspersky Endpoint Security for Business** et découvrez comment des fonctionnalités de gestion des systèmes puissantes et avancées, de chiffrement et de contrôles intuitifs peuvent protéger votre entreprise contre les menaces les plus sophistiquées.

Vous vous orientez sur la facilité d'utilisation que représente le Cloud ? Inscrivez-vous pour tester gratuitement **Kaspersky Endpoint Security Cloud** et découvrez comment réduire les coûts et les ressources en gérant plusieurs terminaux, appareils et serveurs de fichiers à distance, où que vous soyez.

Vous souhaitez externaliser la gestion auprès d'un fournisseur tiers spécialisé ? **Consultez la page destinée aux fournisseurs de services gérés de Kaspersky Lab.**

Site Entreprises Kaspersky Lab

Blog B2B de Kaspersky Lab