LIVRE BLANC POUR LES ENTREPRISES

LA SÉCURITÉ COMMENCE AUX POINTS D'EXTRÉMITÉ

Pourquoi donner la priorité à la sécurisation des terminaux

RÉSUMÉ SYNTHÈSE

82 % des entreprises ont subi une cybermenace/cyberviolation de sécurité au cours des 12 derniers mois.[1] La fréquence, la gravité et le coût de la cybercriminalité augmentent sans cesse.

Le paradigme de sécurité « Défendre et protéger » - défense d'un périmètre réseau au moyen de pare-feux - est révolu. Détecter et réagir en amont est aujourd'hui devenu nécessaire.

Mais les budgets du SI ne suivent pas l'évolution de la cybersécurité. 77 % des dépenses sont encore consacrées à la défense et la protection.[2] 36 % seulement des responsables de la sécurité informatique estiment leur budget suffisant pour sécuriser efficacement leurs terminaux.[3]

Une protection renforcée des données est possible. Avec la bonne technologie - allant des solutions de détection et de réaction en matière de sécurité jusqu'aux équipements individuels -, la bonne stratégie et des ressources suffisantes, les organisations peuvent se protéger des cyberattaques.

Faute d'augmenter les investissements en cybersécurité et d'adapter les investissements aux besoins d'une défense vraiment efficace, les entreprises laissent leur porte ouverte aux menaces informatiques, augmentant le risque de dégâts financiers sévères pour l'organisation.

Introduction

La cybersécurité : un défi majeur pour les entreprises
60 % des responsables informatiques pensent que leurs défenses sont dépassées par la sophistication et le nombre des cyberattaques. 80 % des responsables sécurité considèrent que les Menaces persistantes avancées (Advanced Persistent Threats ou APT), les entreprises criminelles, les hackers activistes et le piratage d'État s'accentuent et représentent le principal défi de la sécurité informatique.[4]

Selon un rapport récent de la société NTT Security, les cyberattaques ont augmenté de 24 % dans le monde au cours du deuxième trimestre 2017, le secteur de l'industrie étant l'un des plus touchés et ciblés par les cybercriminels. [5]

Mais se focaliser sur les menaces extérieures, c'est un peu se tromper de cible et risquer d'allouer trop de ressources à la stratégie de prévention et de protection du périmètre.

Si les attaques externes – virus, logiciels malveillants, hameçonnage – prévalent, les attaques internes sont plus coûteuses.[6] Et une bonne part de ces attaques externes proviennent de vulnérabilités internes, d'employés négligents qui ne respectent pas les consignes de sécurité, de machines non protégées raccordées au réseau - ce que 81 % des personnes interrogées dans le cadre de l'enquête Ponemon considèrent comme la plus grande menace en matière de sécurité informatique.

Et avec le temps, cela ne fera qu'empirer. Le terminal est le nœud le plus faible de n'importe quel réseau et, avec l'accroissement du BYOD (« Bring Your Own Device »), du télétravail et de l'Internet des objets, les terminaux prolifèrent. Ce qui signifie que les points d'entrée des hackers se multiplient eux aussi.

Le temps du réseau d'ordinateurs de bureau reliés par Ethernet est bien loin. Les réseaux d'entreprise sont devenus amorphes et complexes : ce sont aujourd'hui une combinaison d'appareils personnels et professionnels, donnant librement accès aux données via des points d'accès Wi-Fi internes ou externes.

A partir de ce constat, il est nécessaire d'actualiser sa ligne de défense, et de l'adapter aux nouvelles menaces.

Dans ce livre blanc, nous allons examiner la nature et l'importance de la menace - pour mieux connaître notre ennemi - avant d'aborder la cybersécurité à l'époque des appareils multiples, des réseaux non sécurisés et du Cloud.

[1] HPI Printer Security Research 2016 (Spiceworks)
[2] PAC Incident Response Management 2015: https://www.pac-online.com/download/19443/155514
[3] Ponemon 2016 State of the Endpoint Report
[4] IBM CISO Assessment 2014
[5] http://www.nttcomsecurity.com/fr/nouveautes-et-evenements/nid-00791/rapport-ntt-security-des-cyberattaques-plus-labor-es-et-plus-fr-quentes-au-deuxi-me-trimestre-2017/
[6] https://digitalguardian.com/blog/insiders-vs-outsiders-whats-greater-cybersecurity-threat-infographic

L'ampleur de la menace

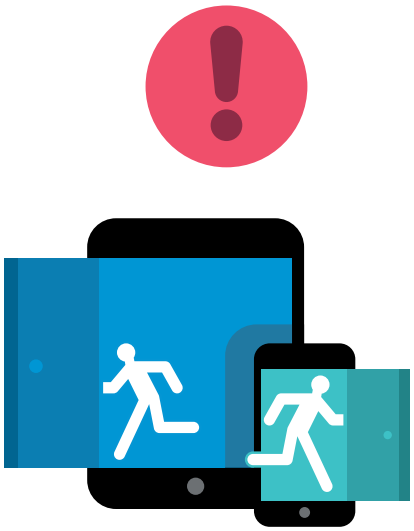
Un piratage d'informations coûte en moyenne aux entreprises 907 053 dollars pour la remise en état, auxquels s'ajoute une perte ultérieure de 13 % du chiffre d'affaires. Il faut en moyenne neuf semaines à une entreprise pour se relever d'une cyberattaque.[7]

Environ 85 % des sociétés interrogées dans le cadre du Rapport HP sur la Sécurité des imprimantes de 2015 déclarent avoir subi une menace ou une violation de sécurité au cours des 12 derniers mois. 80 % des professionnels de l'informatique interrogés pensent que cette menace augmentera au cours des trois prochaines années.[8]

Les pertes dues à la cybercriminalité se font durement ressentir. Pertes de valeur pour ce qui a été volé ou endommagé. Perte de chiffre d'affaires dû à une détérioration de l'image et à une perte de productivité. Ressources perdues en remise en état - temps de service support, déploiement de nouvelles politiques de sécurité, départ de collaborateurs et autres réactions en interne. Amendes et pénalités infligées par les autorités de contrôle, et baisse du cours de bourse.

La menace ne pourra que croître avec le nombre d'appareils connectés au réseau. En raison de l'Internet des Objets, le Gartner Group prévoit 11,4 milliards d'appareils connectés en 2018, contre 6,4 milliards en 2016. Alors que d'ici 2020, plus de 25 % des attaques identifiées sur les entreprises seront liées à l'IoT, moins de 10 % des budgets de sécurité lui sont consacrés.[9]

La menace de la cybercriminalité est grande, et elle ne fait que croître.



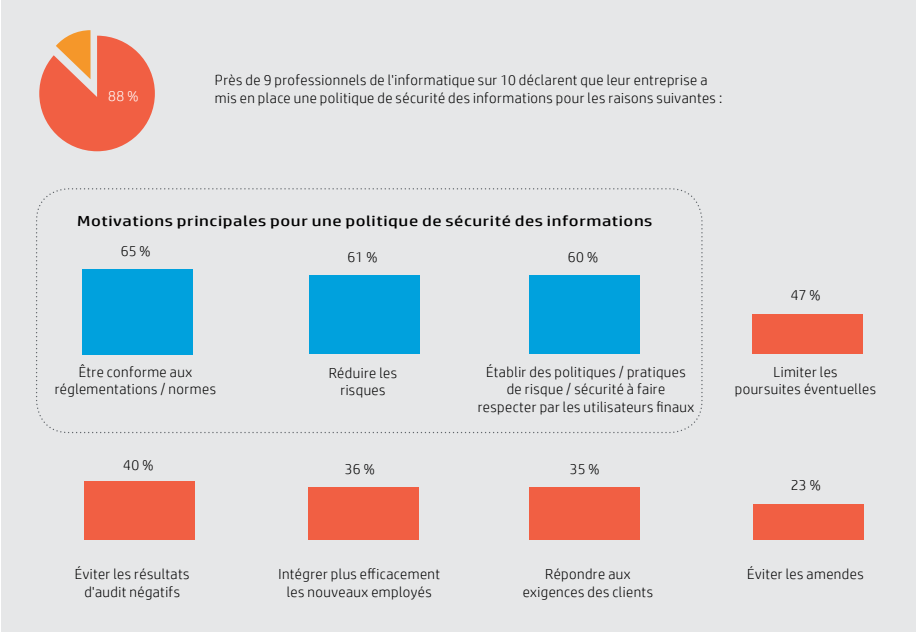
Les formes de menaces

Les entreprises subissent d'innombrables cyberattaques tous les jours. La plupart sont des attaques de faible intensité, virus ou logiciels malveillants. 99 % des organisations interrogées par Ponemon en 2016 avaient eu affaire à des logiciels malveillants au cours des 12 derniers mois. De telles attaques en provenance de l'extérieur sont relativement bénignes, et coûtent en moyenne aux organisations 4 639 dollars.[10]

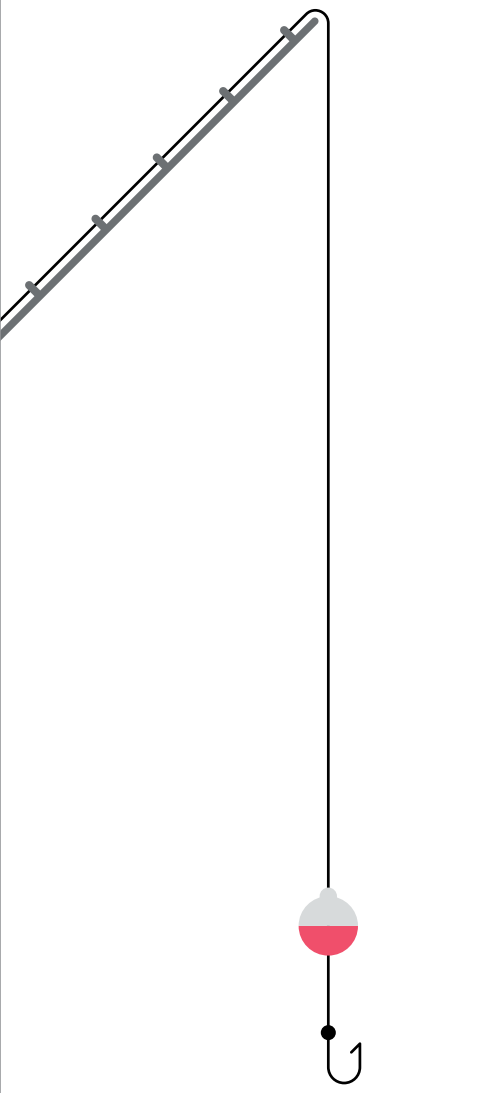
Mais les attaques plus graves deviennent de plus en plus fréquentes. 51 % des organisations interrogées en 2015 avaient subi des attaques de type DDoS (déni de service distribué), lesquelles peuvent être invalidantes - coûtant en moyenne 127 000 dollars. Ce qui est encore plus alarmant c'est que 35 % avaient subi une attaque interne malveillante d'un coût moyen de 145 000 dollars.[9]

La tendance qui se dégage est celui d'attaques mineures incessantes depuis l'extérieur, avec des attaques majeures rares, mais dont la probabilité est frappante, dues vraisemblablement à des négligences en interne, sinon à de la malveillance. 62 % des entreprises ont subi des attaques d'hameçonnage ou d'ingénierie sociale (élicitation), exploitant la faiblesse des employés, d'un coût moyen de 86 000 dollars.[11]

Une étude indépendante de Spiceworks – pour le compte de HP – révèle la répartition des attaques subies en 2014-2015 par 90 entreprises britanniques.[12]



[7] NTT Security Risk:Value Report 2016
[8] HP 2Printer Security Report 2015
[9] http://www.gartner.com/newsroom/id/3291817
[10] https://ssl.www8.hp.com/ww/en/secure/pdf/4aa6-8392enw.pdf
[11] https://digitalguardian.com/blog/insiders-vs-outsiders-whats-greater-cybersecurity-threat-infographic
[12] HPI Printer Security Research, Spiceworks 2016



Comment les violations se produisent-elles

Les médias décrivent la plupart du temps des pirates informatiques rusés et intelligents, parvenant à déjouer les défenses de réseaux sécurisés des entreprises, mais la réalité est en général plus prosaïque.

Les virus peuvent profiter de réseaux compromis, mais les logiciels malveillants s'appuient le plus souvent sur les erreurs humaines. Les attaques de type phishing en dépendent entièrement. Les attaques à grande échelle, par déni de service et vols de données, sont aussi causées bien souvent par la négligence d'utilisateurs.

Le piratage de Dropbox serait dû à un employé de l'entreprise qui utilisait son mot de passe LinkedIn pour accéder aux systèmes internes de l'entreprise. Plus récemment, une attaque informatique massive s'est déclarée en Europe en juin 2017, touchant dans un premier temps l'Ukraine avant de se répandre dans plusieurs pays européens.[14]

Même une aide involontaire suffit aux pirates. L'ignorance, ou le non-respect, des protocoles de sécurité est tout aussi pernicieux. L'utilisation de leur propre équipement au travail et l'usage de logiciels du cloud du commerce par les employés est une menace croissante : les deux introduisent des éléments non sécurisés dans un réseau par ailleurs sûr, échappant au contrôle de la direction informatique, et causant une vulnérabilité non prise en compte.

La plupart du temps, les pirates n'ont pas besoin d'algorithmes perfectionnés ou de technologies de pointe, il leur suffit que l'un de nous soit peu vigilants.

Le pare-feu prend l'eau

Jusqu'à récemment, les remparts de sécurité étaient constitués par des logiciels anti-virus et des pare-feux, afin de créer un périmètre sécurisé. Dans l'environnement de travail actuel, cette stratégie n'est tout bonnement plus suffisante.

81 % des personnes interrogées par Ponemon déclarent que les appareils mobiles de leur réseau ont été la cible de logiciels malveillants. L'utilisation d'applications cloud commerciales par les employés – citée par 72 % des personnes interrogées –, le BYOD (69 %) et les employés travaillant de leur domicile ou autres sites extérieurs à l'entreprise (62 %) sont d'autres facteurs augmentant les risques de sécurité.[15]

Dit simplement, un pare-feu se justifiait quand vous-même, en tant qu'administrateur, détenait le contrôle des appareils connectés. Mais dans une époque où les employés viennent au travail avec leurs propres appareils - souvent plusieurs - et où un nombre croissant de collaborateurs se connectent à distance, protéger le périmètre n'est tout simplement plus possible. Chaque appareil non vérifié est un point d'extrémité vulnérable que les pirates peuvent exploiter.

[13] http://datanews.levif.be/ict/actualite/le-piratage-chez-dropbox-a-touche-69-millions-d-utilisateurs/article-normal-545251.html

[14] https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0

[15] Ponemon 2016 State of the Endpoint Report

Le point de vue de HP : aller plus loin que la simple sécurité du réseau

Commentaires de Michael Howard, Directeur international des pratiques de sécurité chez HP, sur la sécurité des terminaux

Une préoccupation clé et actuelle est que les entreprises ont du mal à sécuriser chaque terminal par manque de prise de conscience et de connaissance de certains appareils et des risques qu'ils comportent. Elles se sentent à l'abri derrière un pare-feu, bien que celui-ci ne soit plus une protection suffisante en cas d'attaque. Les équipes de sécurité doivent connaître chaque terminal de l'infrastructure et vérifier qu'il dispose de couches de protection multiples contre des attaques de plus en plus sophistiquées.

Il est essentiel que les équipes de sécurité informatique connaissent chaque recoin de leur infrastructure informatique d'entreprise et construisent une couche protectrice supplémentaire au-dessus du périmètre réseau standard. Les pare-feu à eux seuls ne peuvent résister à des attaques sophistiquées, et une politique de défense avec des couches de protections multiples à chaque terminal est un must pour garantir que votre entreprise est en règle et éviter de fortes amendes.

La politique d'HP est de se préoccuper en premier lieu de la sécurité pour tout nouveau produit, service ou solution développé(e). Les équipes de développement savent qu'elles doivent répondre aux questions de sécurité, et elles doivent savoir comment les connecter de façon sûre.

Plus que jamais, la sécurité doit être native, et non surajoutée. C'est la politique d'HP depuis des années.

La sécurité en profondeur

Une nouvelle approche de la cybersécurité se doit d'être une protection multicouche. La sécurité du réseau conserve son importance, mais doit être constituée elle-même à partir de réseaux segmentés. De nombreuses violations reposent sur une effraction initiale donnant accès à tout dans le système. Pensez à la bévue de John Podesta par rapport au phishing. Pour éviter que le vol d'une seule clé ne fasse tomber la place forte, il est essentiel d'entourer les informations sensibles de plusieurs barrières concentriques.

La prise en compte de la totalité des appareils est indispensable. La principale difficulté rencontrée par les Responsables informatiques réside dans la couverture de chaque appareil connecté au réseau, qui doit être protégé par un logiciel de sécurité - contre les virus, les logiciels espions et malveillants - mis à jour régulièrement et régulièrement inspecté pour détecter des anomalies. Mieux vaut utiliser les appareils eux-mêmes comme capteurs, collectant des informations en temps réel pour donner l'alerte en cas de violation du périmètre du réseau dont ils font partie.

Une gouvernance ne laissant rien au hasard en matière de sécurité doit être en place, chaque employé étant formé aux protocoles de cybersécurité. L'erreur humaine - cliquer sur le mauvais lien, se connecter à partir d'un appareil grand public - est l'ennemi numéro un du réseau. La formation des employés permet de répondre à la négligence humaine.

Sécurité des appareils

L'une des premières préoccupations est de contrôler quels appareils ont accès au réseau. La première solution - simple - souvent choisie consiste à avoir des réseaux Wi-Fi séparés pour les visiteurs et pour les employés, de sorte que les appareils externes non sécurisés ne puissent avoir accès au réseau principal. Ceci va de pair avec habituer les employés à utiliser ce réseau avec leurs appareils personnels.

L'autre solution consiste à assurer le contrôle des appareils des employés. Cette préoccupation doit alimenter la politique de la société concernant le BYOD (Bring you own device) ou le CYOD (Chose your own device). Un argument fort en faveur d'une politique CYOD réside dans la possibilité de contrôler quels équipements sont utilisés, de choisir ceux qui ont la meilleure sécurité, de gérer leur configuration et de mieux les surveiller.

Privilégier l'un des PC de notre gamme Elite à un portable bon marché vous assure de bénéficier d'une protection optimale. Chaque PC Elite dispose de la technologie HP SureStart qui vérifie le BIOS tous les quarts d'heure et réinitialise la machine si une anomalie est détectée, bloquant l'accès aux visiteurs indésirables. C'est cette fonction - ajoutée à beaucoup d'autres - qui a valu à nos PC de la série Elite 800 d'être déclarés « les PC les plus sûrs au monde. »

Les employés préfèrent se servir de leurs propres appareils pour deux raisons :
1. La technologie grand public est souvent supérieure à celle que l'on fournit sur le lieu de travail.
2. Les employés aiment utiliser les technologies qu'ils connaissent bien

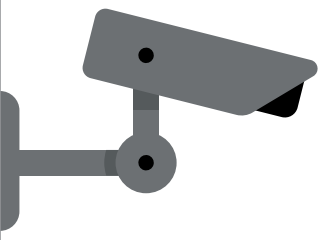
En leur offrant une politique CYOD disposant des bonnes ressources, avec les équipements les plus récents mis à jour régulièrement, les entreprises peuvent fournir aux employés des matériels supérieurs aux leurs, et assurer un meilleur contrôle de la sécurité de ceux-ci. C'est la raison pour laquelle nous proposons HP Device as a Service (DaaS).

Il est primordial d'inclure tous les appareils dans la stratégie de sécurité, même ceux que l'on oublie souvent. Lors d'une enquête d'IDC, 80 % des personnes interrogées ont déclaré que la sécurité informatique était importante dans leur activité, mais 59 % seulement reconnaissaient l'importance de la sécurité des imprimantes. Pourtant, plus de la moitié avaient subi une violation de sécurité impliquant la sécurité des imprimantes au cours des 12 derniers mois.

La moyenne des violations de sécurité avant la mise en place d'une politique de sécurité des imprimantes était de 9,9 par an, pour un coût moyen de 521 400 dollars (amendes comprises). Suite à la mise en place d'une politique de sécurité des imprimantes, ce nombre était tombé à 1,5, économisant 200 heures de temps d'employé par an et 250 000 dollars de frais connexes, y compris d'audit et de mise en conformité.[17]

[16] Les plus sécurisés selon les capacités de sécurité complètes et uniques de HP, sans coûts supplémentaires pour les fournisseurs, avec des ventes annuelles de plus de 1 million au 1er décembre 2016 d'ordinateurs HP Elite avec processeurs Intel® Core™ de 7e génération, graphiques intégrés Intel® et Intel® WLAN. Les plus fins par rapport à la concurrence avec des ventes annuelles de plus de 1 million d'appareils convertibles non amovibles intégrant le système d'exploitation Windows Pro et un processeur de 6ème ou 7ème génération Intel® compatible vPro™ au 1er décembre 2016.

[17] La valeur pour l'entreprise de la sécurisation des imprimantes - étude IDC 2015



Détection et contre-mesures proactives

77 % des dépenses de sécurité informatique vont aux technologies de prévention et de protection telles que les logiciels anti-virus et les pare-feux, selon une étude de PAC. Mais cette approche n'est pas efficace. L'étude a également montré que 67 % des entreprises interrogées avaient subi une violation de sécurité au cours des 12 derniers mois, et 100 % dans le passé.[18]

Les logiciels anti-virus, en particulier, sont d'une inefficacité choquante. Le fournisseur de sécurité Damballa a effectué des tests au cours desquels ils attaquaient délibérément un réseau pour mesurer la réaction aux virus. Il aura fallu plus de six mois avant que 100 % des fichiers malveillants soient identifiés. Il a fallu entre un et six mois avant que les entreprises découvrent qu'elles avaient été attaquées.

La sécurisation des terminaux ne peut plus reposer seulement sur la prévention. Le nombre croissant d'incidents dus aux virus et aux logiciels malveillants, plus les risques inhérents au BYOD et au télétravail, signifie que des violations sont inévitables. Personne ne propose d'abandonner complètement la prévention et la protection, mais à l'évidence, détection et réaction doivent remonter dans l'ordre des priorités.

Une surveillance continue en temps réel s'impose, idéalement en utilisant les terminaux eux-mêmes comme capteurs - donnant l'alerte à l'ensemble du réseau en cas de violation. Ceci permet à la sécurité informatique de réagir, en employant des processus tels que :

- Éteindre un appareil à distance
- Détruire un processus infecté ou propageant un logiciel malveillant
- Mettre en quarantaine un fichier ou un groupe de fichiers spécifique
- Interrompre la communication avec le réseau pour isoler les appareils infectés[20]

Accepter que des violations se produiront, et mettre en place les protocoles de réaction adéquats - ainsi que la technologie nécessaire pour les appliquer -, voilà la seule solution pour garantir la cybersécurité lorsque la prévention ne suffit plus.

« Aucune technologie ne peut fournir de sécurité si les gens la compromettent. »

– Joseph Steinberg [21]

Sécurité des employés

La sécurisation des appareils implique la sécurisation des utilisateurs.
Chaque employé doit être formé à la cybersécurité. Les collaborateurs doivent être conscients du risque de phishing, et du risque lié à la visite de sites web douteux ou du téléchargement des pièces jointes suspectes. Ils doivent être conscients de la politique concernant d'utilisation de mots de passe fiables, spécifiques pour chaque accès, et de l'importance de les stocker avec un bon gestionnaire de mots de passe.

Il doit avoir conscience de l'importance de mettre à jour régulièrement les logiciels de sécurité sur ses appareils personnels, pour alléger le travail de contrôle des équipes informatiques. Il doit être attentif à n'utiliser que des appareils sûrs pour se connecter aux réseaux de l'organisation et à éviter d'utiliser des appareils personnels sur des réseaux externes non sécurisés pour accéder à des données sensibles.

De nombreux experts de haut niveau en cybersécurité recommandent d'effectuer des simulations d'attaques par hameçonnage - allant jusqu'à construire de faux sites web, pour exercer chaque employé - et de créer de véritables cursus de formation à la cybersécurité. Car la plupart des attaques reposent sur l'exploitation des faiblesses humaines, qu'il s'agisse de négligences ou de malveillance.

Les Responsables informatiques ne doivent pas oublier que les employés constituent le maillon faible de n'importe quel réseau.

[18] PAC Incident Response Management 2015
[19] https://www.mag-securs.com/news/articletype/articleview/articleid/34566/categoryid/62/70-des-malwares-passent-au-travers-des-anti-virus.aspx
[20] The Essential Endpoint Detection Checklist – HP Now
[21] https://digitalguardian.com/blog/data-security-experts-answer-what-biggest-misconception-companies-have-about-endpoint-security

Conclusion

La sécurité informatique doit évoluer vers une politique de détection aux points d'extrémité comprenant les réactions proactives adaptées.
La protection des données de l'organisation dans le climat informatique actuel - confronté à la montée de la menace de la cybercriminalité et à la perte de contrôle du périmètre du réseau - demande deux choses : une prise de conscience et plus de ressources.

Le concept de réseau doit évoluer. L'idée du réseau en tant que barrière entourant un ensemble d'appareils n'a plus cours. Il est temps de voir la réalité en face. « Le réseau » est une chimère. Il émerge à partir des appareils connectés - chacun étant un terminal. Sécuriser le réseau signifie sécuriser le terminal. Et chaque terminal a deux composantes : l'appareil, et son utilisateur. Les deux doivent être pris en compte.

Mais assurer la sécurité avec ce nouveau paradigme est bien plus complexe que dans l'environnement PC connecté via Ethernet d'antan. Il faut plus de ressources, et il faut les réclamer. Et cela, 61 % des personnes interrogées par Ponemon en sont conscientes.

Pour y parvenir, l'astuce consiste à faire adhérer le reste de l'entreprise. Seulement 36 % des personnes interrogées considèrent qu'elles disposent du budget et des effectifs adéquats pour la sécurité des terminaux. 69 % disent que le département informatique ne peut faire face à la demande de support des employés. 71 % déclarent que leurs politiques de sécurité des terminaux sont difficiles à faire appliquer.[22]

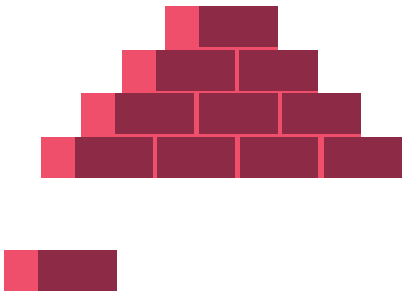
80 % des responsables sécurité informatique considèrent que le meilleur argument pour assurer le financement de leurs programmes de sécurité est le respect des contraintes légales, mais jugent également que ce n'est pas là, de loin, la principale raison de dépenser de l'argent. La conformité, c'est respecter les exigences minimales.[23]

Les décideurs informatiques doivent souligner l'importance de la sécurité, en accord avec la direction générale. Montrer ce que coûte une sécurité laxiste - frais de remise en état, perte de chiffre d'affaires, cours de bourse en berne - et insister sur les économies à long terme. Beaucoup de solutions de sécurité génèrent également des améliorations par ailleurs. Songez à la productivité accrue résultant de la sécurisation des imprimantes, et aux gains de productivité qu'apporte une technologie régulièrement remise à niveau dans le cadre d'un programme de CYOD souple, fourni par un tiers par abonnement (tel que le DaaS HP). On peut clairement argumenter de manière chiffrée.

Le défi est colossal. Et, au fil du temps - avec l'explosion de l'Internet des Objets et la sophistication de la cybercriminalité - il deviendra encore plus conséquent. Mais on peut y faire face. Avec la bonne technologie, la bonne stratégie, et les ressources adéquates, nous pouvons défendre nos points d'extrémité. Nous pouvons faire en sorte que nos données soient en sécurité.

Pour plus d'informations sur HP Device as a Service, et sur la manière dont il peut vous aider à appliquer un programme complet, souple et sécurisé de CYOD, **cliquez ici**.

Découvrez aussi notre gamme d'appareils les plus sécurisés comme la série **HP Elite**, et plus d'informations sur les solutions de sécurité HP **ici**.



Recevez toute l'actualité en vous inscrivant sur
hp.com/go/getupdated

[22] Rapport de Ponemon sur l'état des terminaux 2016

[23] https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697