HP WOLF SECURITY

RAPPORT : REFUS ET REJETS DES CONTRAINTES LIÉES À LA SÉCURITÉ INFORMATIQUE

HP WOLF SECURITY

SYNTHÈSE ET RÉSULTATS CLÉS

La pandémie a forcé les entreprises et leurs employés à abandonner le travail de manière traditionnelle en allant au bureau, pour rapidement adopter un nouveau modèle, au sein duquel le travail hybride dynamique est devenu la norme. Cependant, cette nouvelle manière de travailler n'est en rien une tendance éphémère. En effet, d'après notre rapport HP Wolf Security Travail hybride & cybersécurité : la frontière étroite entre usages personnels et professionnels, 23 % des employés de bureau dans le monde s'attendent à travailler principalement depuis chez eux une fois la pandémie terminée, et 16 % supplémentaires prévoient de partager leur temps entre le télétravail depuis leur domicile et le travail au bureau. Cette situation entraînera très certainement des répercussions majeures pour les entreprises de tous les secteurs.

Au cours de la pandémie, les entreprises ont dû radicalement s'adapter en l'espace de quelques jours seulement, et ont pu le faire en grande partie grâce aux technologies numériques. Mais ce que l'on oublie souvent, c'est que toute innovation numérique est impossible sans système de sécurité. Malgré leur rôle essentiel pour permettre aux entreprises d'exercer leur activité, les équipes responsables de la sécurité ont été dédaignées par des employés rebelles protestant contre les nouvelles restrictions qu'ils doivent respecter.

Dissimulée au sein du chaos créé par la pandémie forçant les employés à travailler depuis chez eux, une autre pandémie, moins visible, a discrètement vu le jour : la cybercriminalité. Cette tendance néfaste est observée dans de nombreux secteurs. Selon une analyse réalisée par KuppingerCole dans le monde entier en 2020, les appareils connectés à Internet sont la cible de 1,5 attaque par minute.

Malheureusement, cette ère d'innovation et de créativité renouvelée en termes de cybercriminalité s'est également accompagnée d'une période de changements et d'adaptation pour les entreprises. Elles doivent rapidement agir pour garantir la continuité de leurs opérations. Une cybercriminalité accrue, une visibilité réduite sur la sécurité, une force de travail de plus en plus éparse et difficilement soutenue par les services informatiques ont ainsi pu être constatées.

Se frayer un chemin au sein de ce nouveau labyrinthe sera un énorme défi pour les leaders responsables de la sécurité. Et ces efforts ne devront pas être isolés. Les utilisateurs possèdent désormais de nouvelles attentes vis-à-vis des technologies qu'ils utilisent au quotidien pour travailler, et recherchent une expérience fluide n'entravant pas leur flux de travail. Ils veulent que tout fonctionne rapidement et refusent d'être ralentis, en particulier les plus jeunes d'entre eux. Les équipes responsables de la cybersécurité ont donc un important défi à relever afin de sécuriser les environnements de travail s'appuyant de moins en moins sur une sécurité périmétrique. À cause de cela, ces dernières font naturellement face à un épuisement et à un découragement lorsque leurs efforts sont négligés. Afin de garantir aux entreprises un avenir sécurisé, il sera essentiel de créer des liens entre les utilisateurs et les équipes responsables de la cybersécurité.

Un leadership de qualité en matière de cybersécurité n'a jamais été aussi important, et le rôle des responsables de la sécurité des systèmes d'information (RSSI) évolue aujourd'hui avec la place grandissante accordée à la cybersécurité par les cadres dirigeants. Pour un succès optimal, les RSSI devront exploiter un large éventail de compétences afin de garantir que les risques sont bien connus et compris et qu'ils puissent être gérés efficacement. Pour cela, il sera essentiel de mettre en place une culture de sécurité positive au sein de l'entreprise, adoptée par tous les employés. Les mesures de sécurité seront conçues en gardant à l'esprit la facilité d'utilisation et la continuité des opérations, et les équipes chargées de la cybersécurité bénéficieront des outils de sécurité les plus avancés afin d'améliorer la visibilité et permettre une gestion à distance. Elles pourront ainsi être considérées comme des partenaires de sécurité et non pas des entités imposant des contraintes de sécurité.

Dans ce second rapport HP Wolf Security, nous avons regroupé des données issues d'une enquête en ligne réalisée par YouGov auprès de 8 443 employés de bureau du monde entier ayant adopté le télétravail depuis leur domicile au cours de la pandémie, d'une étude mondiale à laquelle ont participé 1 100 décideurs informatiques (équipes informatiques), ainsi que d'analyses de pointe effectuées par KuppingerCole. Ce rapport se penche sur la rupture actuellement perceptible entre les employés et les équipes chargées de la sécurité et met en lumière le besoin évident d'un changement.

Dans ce rapport HP Wolf Security, nous nous pencherons sur les éléments suivants :

- **Le refus des utilisateurs lié à des politiques de sécurité contraignantes :** nos données prouvent qu'un pourcentage significatif des employés a des doutes à propos des politiques de sécurité en place. Beaucoup d'entre eux les considèrent comme gênantes et ont tenté de contourner les technologies et contrôles de sécurité adoptés lorsqu'ils travaillent depuis leur domicile. Cette tendance est particulièrement notable chez les personnes âgées de 18 à 24 ans – notre future force de travail – ne doit en aucun cas être ignorée.
- **Les compromis, les risques et les rejets :** les données recueillies prouvent également que les équipes responsables de la cybersécurité peuvent apercevoir les risques de violations de données, mais se sentent souvent ignorées lorsqu'elles tirent la sonnette d'alarme. Ces dernières subissent des pressions afin de trouver un compromis entre les bonnes pratiques de sécurité et la continuité de l'activité des entreprises, dans un contexte général de conformité aux politiques réduite, de visibilité amoindrie et de cyber-risques accrus.
- **Le rôle des RSSI dans la création de liens au sein de l'entreprise :** sans interventions, les désaccords et risques peuvent s'accroître. Il incombe désormais aux leaders responsables de la sécurité d'ouvrir la voie à une force de travail dynamique, flexible et sécurisée. Les RSSI jouent un rôle positif et permettent de transformer des relations tendues entre des équipes chargées de la cybersécurité et des employés en partenariats fructueux. Plus que jamais, les RSSI devront s'appuyer sur leurs compétences de négociation, de communication et de gestion des individus.

POINT DE VUE
HP WOLF SECURITY :

JOANNA BURKEY, RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION, HP INC. :

« Alors que notre ancien monde professionnel articulé en grande partie autour de périmètres de sécurité établis laisse place à un modèle hybride de travail décentralisé suite à la pandémie, les entreprises qui ressortiront gagnantes seront celles qui accepteront le changement et s'y adapteront au lieu de combattre l'inévitable. Ce processus ne sera pas aisé. Il nécessitera un leadership robuste et une grande communication. Les équipes responsables de la cybersécurité devront accorder la priorité aux mesures de sécurité adaptées à ce nouvel environnement de travail hybride. Les utilisateurs, eux, devront participer plus activement à la sécurité de leur entreprise. »

CHIFFRES CLÉS

REFUS DE LA PART DES EMPLOYÉS DE BUREAU

Apathie

39 %	des employés de bureau interrogés âgés de 18 à 24 ans ne connaissaient pas avec certitude les politiques de sécurité des données déjà en place sur leur lieu de travail
36 %	des employés de bureau interrogés avaient bénéficié d'une formation leur apprenant comment protéger le réseau de leur domicile
54 %	des employés de bureau interrogés âgés de 18 à 24 ans étaient plus préoccupés par les deadlines que par le fait d'exposer leur entreprise à des violations de données

Frustration

48 %	des employés de bureau interrogés âgés de 18 à 24 ans estimaient que les politiques de sécurité étaient une gêne
37 %	des employés de bureau interrogés ont déclaré que les politiques et technologies de sécurité sont trop contraignantes
48 %	des employés de bureau interrogés ont déclaré que les mesures de sécurité mises en place entraînaient une grande perte de temps

Contournement

31 %	des employés de bureau interrogés âgés de 18 à 24 ans avaient tenté de contourner les mesures de sécurité

CHIFFRES CLÉS

REJETS LIÉS AUX ÉQUIPES INFORMATIQUES

Compromis

76 %	des équipes informatiques ont déclaré que la sécurité a été reléguée au second plan au profit de la continuité des opérations au cours de la pandémie
91 %	des équipes informatiques ont subi des pressions pour réaliser des compromis en termes de sécurité afin de donner la priorité à la continuité des opérations
83 %	des équipes informatiques estimaient que le télétravail à domicile était devenu une « bombe à retardement » et entraînerait des violations au sein des réseaux

Restrictions

91 %	des équipes informatiques ont mis à jour les politiques de sécurité en place afin de les adapter au télétravail à domicile
78 %	des équipes informatiques ont restreint l'accès à certains sites web et applications

Découragement

80 %	des équipes informatiques ont fait face à des contestations de la part d'utilisateurs
80 %	des équipes informatiques ont déclaré que la sécurité informatique était devenue une « tâche ingrate »
69 %	des équipes informatiques ont déclaré qu'elles se sentaient comme des « brebis galeuses » à propos des restrictions imposées aux employés

L'APATHIE ET LA FRUSTRATION SONT-ELLES LES CAUSES DE CES REFUS ?

L'adoption mondiale du télétravail a eu un impact sur tout le monde ; membres du conseil d'administration ou employés de terrain, nous avons toutes et tous dû nous adapter. La crise a été particulièrement stressante, mais la solidarité générale qui a pu être constatée est véritablement remarquable.

Pourtant, des perturbations et changements peuvent créer des tensions et exacerber les désaccords. Trois thèmes se dégagent clairement de l'enquête réalisée par YouGov auprès d'employés de bureau du monde entier :

- Tout d'abord, à quel point les employés travaillant depuis chez eux se sentent déconnectés et indifférents vis-à-vis de la cybersécurité, potentiellement à cause d'un manque de communication et de formation.
- Deuxièmement, l'effet négatif des politiques et outils de sécurité destinés à aider à gérer les risques liés au télétravail sur la productivité des employés et les conflits créés par tout cela.
- Troisièmement, et l'élément le plus préoccupant de tous, le fait que des employés contournent certaines mesures de sécurité pour effectuer leur travail et ne sont plus protégés par les solutions de cybersécurité en place.

Le manque de prise de conscience de l'importance de la sécurité chez les employés est frappant, particulièrement chez les plus jeunes. Quand on leur demande s'ils comprennent clairement les politiques et consignes mises en place pour leur permettre de travailler de manière sécurisée chez eux, 39 % des employés de bureau interrogés âgés de 18 à 24 ans déclarent ne pas comprendre clairement ces politiques de sécurité, voire même ne pas en connaître l'existence. Un pourcentage 10 % supérieur à la moyenne mondiale pour tous les groupes d'âge cumulés (29 %). Étant donné qu'une telle négligence peut entraîner d'innombrables points d'entrée pour des personnes mal intentionnées, qui peuvent ensuite engendrer des incidents majeurs, ces statistiques sont bien loin d'être rassurantes.

Lorsqu'ils travaillent depuis chez eux, les employés font face à de plus grands risques de sécurité. Le réseau de leur domicile et les appareils qui y sont connectés deviennent des éléments cruciaux. Selon une analyse réalisée par KuppingerCole, les professionnels du monde entier chargés de la gestion du risque accordent désormais une importance toute particulière aux activités effectuées dans le cadre du télétravail pouvant avoir des conséquences néfastes sur l'infrastructure IT et les réseaux. De plus, une étude réalisée par l'Union européenne et citée par KuppingerCole a démontré qu'en 2020, 40 % des employés européens ont rencontré des problèmes de sécurité au sein de leur environnement de télétravail à domicile.

Illustration 1 – Pourcentage d'employés de bureau par pays ayant reçu une formation supplémentaire leur apprenant comment protéger le réseau de leur domicile dans le cadre du télétravail

MONDIAL	CANADA	MEXIQUE	ÉTATS-UNIS	ALLEMAGNE	ROYAUME-UNI	JAPON	AUSTRALIE
36 %	44 %	50 %	38 %	27 %	23 %	30 %	42 %

POINT DE VUE
HP WOLF SECURITY :

IAN PRATT, DIRECTEUR MONDIAL DE LA SÉCURITÉ, PERSONAL SYSTEMS, HP INC. :

« Le fait que des employés contournent activement les mesures de sécurité doit être une préoccupation majeure pour tous les RSSI ; c'est comme ça que peuvent naître des violations de sécurité. Si ces mesures sont trop contraignantes et ralentissent les employés, ces derniers trouveront un moyen de les contourner. Au lieu de cela, la sécurité devrait être intégrée dans la mesure du possible aux habitudes et flux de travail déjà existants, grâce à une technologie non-intrusive, délibérément sécurisée et intuitive pour les utilisateurs. Nous devons faire en sorte que travailler de manière sécurisée soit aussi simple que de le faire de manière non sécurisée ; pour cela, nous pouvons intégrer la sécurité directement aux systèmes. »

54 % DES EMPLOYÉS DE BUREAU ÂGÉS DE 18 À 24 ANS ÉTAIENT PLUS PRÉOCCUPÉS PAR LES DEADLINES QUE PAR LE FAIT D'EXPOSER LEUR ENTREPRISE À DES VIOLATIONS DE DONNÉES.

31 % DES EMPLOYÉS DE BUREAU ÂGÉS DE 18 À 24 ANS ONT TENTÉ DE CONTOURNER LES POLITIQUES DE SÉCURITÉ DE L'ENTREPRISE AFIN DE FAIRE LEUR TRAVAIL.

En dépit de cela, 64 % des employés de bureau interrogés n'ont bénéficié d'aucune formation supplémentaire visant à leur expliquer comment protéger le réseau de leur domicile. Les différences géographiques sont frappantes. Le Royaume-Uni se trouve en bas de la liste avec seulement 23 % des employés ayant bénéficié de ce type de formation ; le Japon ne fait guère mieux, avec seulement 30 %, contrairement aux États-Unis (38 %) et au Canada (44 %). De plus, seuls 36 % des employés ont profité de ressources techniques supplémentaires (comme des réseaux Wi-Fi sécurisés) afin de les aider à travailler de manière sécurisée depuis chez eux.

Ce manque d'implication vis-à-vis de la cybersécurité contribue à un sentiment d'apathie largement répandu chez les employés. Dans l'ensemble, 36 % des employés de bureau interrogés ont déclaré que respecter les deadlines était plus important pour eux que de considérer si les risques qu'ils peuvent prendre menacent potentiellement d'exposer leur entreprise à une violation de données. De plus, 8 % ne sont pas certains de connaître l'élément prioritaire parmi ces deux options, démontrant ainsi une apathie claire. Encore une fois, ces statistiques sont plus préoccupantes encore lorsque l'on se penche sur les personnes plus jeunes : plus de la moitié (54 %) des employés de 18 à 24 ans estiment que leurs deadlines sont plus importantes qu'une violation de données, et 9 % ne sont pas certains de leur réponse. Ces chiffres suggèrent un net manque de compréhension ou d'intérêt pour le rôle critique de la sécurité au sein de leur entreprise, et du rôle qu'ils peuvent jouer afin de la protéger contre des attaques.

Illustration 2 – Pourcentage d'employés de bureau par groupe d'âge s'accordant à dire que les outils de sécurité sont souvent plus une gêne qu'une aide utile

MONDIAL	18-24 ANS	25-34 ANS	35-44 ANS	45-54 ANS	+ DE 55 ANS
34 %	48 %	40 %	35 %	31 %	23 %

Une autre observation montre que certains employés de bureau estiment que les politiques et technologies de sécurité entravent leur travail quotidien. En moyenne, plus d'un tiers (34 %) des employés de bureau du monde entier déclarent considérer la sécurité comme une gêne. Encore une fois, ce chiffre est particulièrement notable chez les plus jeunes employés, avec 48 % des personnes âgées de 18 à 24 ans et 40 % de celles âgées de 25 à 34 ans faisant cette déclaration.

Quand on leur demande de détailler leur opinion, 37 % des employés déclarent que les politiques et technologies de sécurité sont souvent trop restrictives. En parallèle, 48 % d'entre eux s'accordent à dire que les mesures de sécurité apparemment essentielles résultent souvent en une perte de temps importante, en particulier dans le cadre du télétravail à domicile. Ce chiffre atteint les 64 % chez les employés de 18 à 24 ans. Parmi les personnes déclarant que les mesures de sécurité contraignantes leur faisaient perdre du temps, 82 % ont estimé cette perte de temps à 2 à 6 heures et 18 % l'ont estimée à plus de 6 heures chaque mois.

Sans surprise, 16 % des employés de bureau interrogés ont admis avoir contourné ces restrictions en ignorant les politiques de sécurité de l'entreprise afin de pouvoir faire leur travail plus facilement. Ce chiffre atteint les 31 % chez les employés de 18 à 24 ans.

COMPROMIS, RISQUES ET REJETS

Les changements rapides mis en place dans le cadre de cette transformation numérique ont permis de sauver des entreprises, des emplois et même des vies. Ils ont permis aux entreprises de non seulement survivre, mais même de prospérer. Ils ont également ouvert la voie à une nouvelle ère en termes de créativité numérique, car de nouveaux moyens innovants de partager des expériences de manière sécurisée pendant cette pandémie ont pu être découverts, dont beaucoup risquent certainement de devenir des habitudes durables.

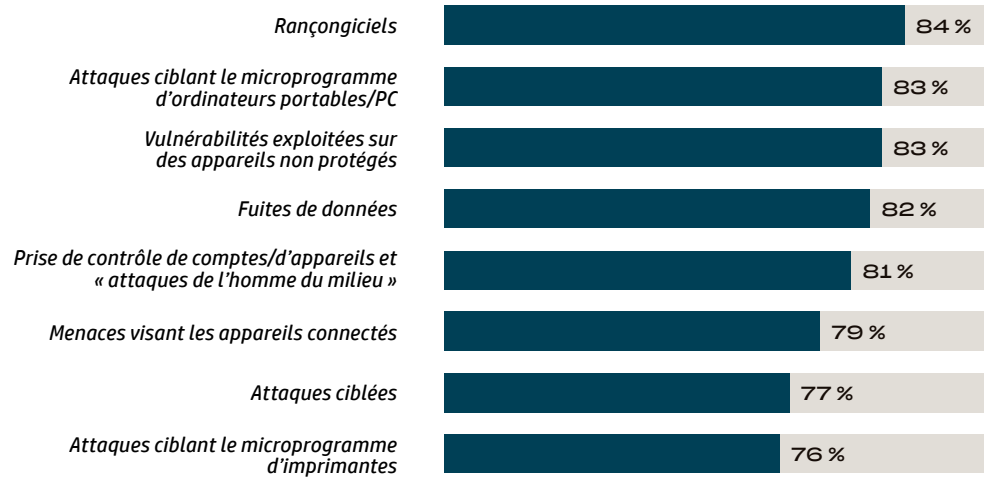
Mais les entreprises n'ont pas été les seules à innover : les cybercriminels l'ont fait, eux aussi. Trois thèmes se dégagent de l'enquête réalisée par Toluna auprès d'équipes informatiques :

- Tout d'abord, la diversité et l'envergure des menaces ciblant les entreprises, qui obligent les équipes responsables de la cybersécurité à redoubler d'efforts pour les protéger au mieux et causent un épuisement généralisé.
- Deuxièmement, les compromis ayant été faits par les équipes responsables de la cybersécurité afin d'assurer la continuité des opérations, que beaucoup considèrent comme paradoxaux.
- Troisièmement, le fait que les équipes chargées de la cybersécurité ont dû gérer les contestations des employés face à leurs efforts de sécurisation de leur entreprise.

Les équipes chargées de la cybersécurité font aujourd'hui face à une vague croissante de menaces provenant de personnes mal intentionnées de plus en plus expertes. Les nouvelles politiques et l'augmentation des restrictions sont souvent contestées. À cause de cela, 83 % des équipes informatiques interrogées dans le cadre de ce rapport estiment que le télétravail à domicile est devenu une véritable « bombe à retardement » qui pourrait entraîner des violations au sein des réseaux des entreprises.

Quand on les interroge au sujet du type et de l'importance des menaces ciblant aujourd'hui les entreprises, 84 % des équipes informatiques décrivent les rançongiciels comme un risque significatif, voire majeur. Ces menaces incluent également des vulnérabilités non corrigées et des attaques ciblant le firmware sur des ordinateurs portables (83 %), des fuites de données (82 %), des prises de contrôle de comptes/d'appareils (81 %), des attaques ciblées et des « attaques de l'homme du milieu » (79 %), des menaces visant les appareils connectés (77 %) et des attaques ciblant le firmware d'imprimantes (76 %).

Illustration 3 – Niveau de menace estimé que posent les méthodes d'attaque suivantes pour les équipes informatiques avec l'augmentation du télétravail à domicile sur des réseaux potentiellement non sécurisés



Pourtant, malgré les menaces accrues, 76 % des équipes informatiques estiment que la sécurité a été reléguée au second plan au profit de la continuité des opérations au cours de la pandémie. Le même pourcentage déclare se retrouver dans une situation complexe, où on leur demande de garantir une sécurité optimale et où elles subissent des pressions pour permettre de faciliter les innovations. Et pratiquement toutes (91 %) ressentent des pressions pour faire des compromis en termes de sécurité afin de donner la priorité à la continuité des opérations ; 50 % de ces équipes décrivent même ces pressions comme « significatives ».

91 % DES ÉQUIPES INFORMATIQUES ONT SUBI DES PRESSIONS POUR RÉALISER DES COMPROMIS EN TERMES DE SÉCURITÉ AFIN DE DONNER LA PRIORITÉ À LA CONTINUITÉ DES OPÉRATIONS.

POINT DE VUE
HP WOLF SECURITY :

JOANNA BURKEY, RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION, HP INC. :

« Les RSSI doivent gérer un volume grandissant d'attaques à la rapidité et à la gravité croissantes. Leurs équipes doivent redoubler d'efforts afin de préserver la sécurité des entreprises, tout en facilitant la transformation numérique de masse qui s'opère malgré une visibilité réduite, alors que les employés n'ont pas encore réellement assumé leur rôle clé dans la sécurisation de l'entreprise. La sécurité doit devenir une responsabilité partagée par tous les employés de l'entreprise, qui doivent comprendre le rôle important qu'ils doivent jouer. »

69 % DES ÉQUIPES INFORMATIQUES ONT DÉCLARÉ QU'ELLES SE SENTAIENT PARFOIS COMME DES « BREBIS GALEUSES », CAR C'EST ELLES QUI DOIVENT DIRE « NON » AUX UTILISATEURS.

Illustration 4 – Pourcentage d'équipes informatiques par pays qui estiment que la sécurité a été reléguée au second plan au profit de la continuité des opérations au cours de la pandémie

	MONDIAL	CANADA	MEXIQUE	ÉTATS-UNIS	ALLEMAGNE	ROYAUME-UNI	JAPON	AUSTRALIE
OUI, DES PRESSIONS CONSIDÉRABLES	50 %	57 %	55 %	43 %	32 %	62 %	55 %	48 %
OUI, QUELQUES PRESSIONS	41 %	37 %	41 %	44 %	49 %	33 %	38 %	48 %

Bien évidemment, de tels compromis ne peuvent continuer. Notre nouveau monde professionnel devra être sécurisé et dynamique : il ne pourra pas se baser sur des compromis. Mais rétroactivement corriger des erreurs passées et effectuer des concessions n'est pas nécessairement chose aisée. Difficile aujourd'hui de faire marche arrière. Les employés s'attendent désormais à continuer à travailler avec le même degré de liberté dont ils ont pu bénéficier jusqu'à maintenant.

Si les équipes responsables de la sécurité se penchent naturellement sur comment réduire ces risques, elles ont également dû faire face à une résistance. 91 % des équipes informatiques ont mis à jour les politiques de sécurité en place afin de s'adapter à l'adoption accrue du télétravail à domicile et 78 % d'entre elles ont restreint l'accès à certains sites web et applications pour des raisons de sécurité. Mais parmi ces équipes informatiques ayant imposé des restrictions d'accès à certains sites et applications, 93 % ont déclaré avoir reçu des retours de la part des utilisateurs, qui ont exprimé leur frustration et indiqué que ces restrictions entravaient leur productivité.

Plus globalement, 80 % des équipes informatiques interrogées ont déclaré avoir très fréquemment fait face à des contestations de la part d'employés n'appréciant pas les mesures de contrôle mises en œuvre dans le cadre du télétravail depuis leur domicile : 18 % de ces équipes informatiques ont en effet précisé qu'elles reçoivent tous les jours des plaintes d'employés estimant que ces politiques ou systèmes de sécurité entravent leur travail ; 22 % d'entre elles recevaient ces commentaires tous les quelques jours et 27 % de manière hebdomadaire.

Par conséquent, les équipes responsables de la cybersécurité considèrent parfois leurs efforts comme vains. 83 % des équipes informatiques expliquent qu'essayer de développer et d'appliquer des politiques de cybersécurité pour leur entreprise est désormais impossible maintenant que la pandémie a flouté les frontières existant entre la vie personnelle et la vie professionnelle des individus. 80 % des équipes informatiques s'accordent à dire que la sécurité informatique devient aujourd'hui une « tâche ingrate » car les personnes travaillant à domicile n'écoutent souvent pas les conseils qui leur sont donnés.

Illustration 5 – Le télétravail fragilise l'équilibre entre sécurité et praticité

Les équipes informatiques ont mis à jour les politiques de sécurité en place afin de s'adapter au nombre accru de télétravailleurs	91 %
Les équipes informatiques restreignent actuellement l'accès à certains sites web et applications pour des raisons de sécurité	78 %
Les équipes informatiques s'accordent à dire qu'elles font face à des contestations de la part d'utilisateurs mécontents à cause des mesures de contrôle qui leur sont imposées lors du travail à domicile	80 %
Les équipes informatiques s'accordent à dire que la création de politiques d'entreprise relatives à la cybersécurité est une tâche ingrate	80 %
Les équipes informatiques confirment que l'augmentation du nombre de télétravailleurs a créé une bombe à retardement en termes de violations des réseaux professionnels	83 %
Les équipes informatiques sont d'accord sur le fait qu'essayer de développer et d'appliquer des politiques de cybersécurité pour leur entreprise est désormais impossible maintenant que la pandémie a flouté les frontières existant entre la vie personnelle et la vie professionnelle des individus	83 %

De ce fait, les équipes responsables de la sécurité informatique ont souvent le sentiment d'être considérées comme des trouble-fête ; 69 % des personnes interrogées ont déclaré qu'elles se sentaient comme des « brebis galeuses » à cause de commentaires d'autres personnes.

RÉSUMÉ

HP Wolf Security – Résumé des résultats de ce rapport :

- Si l'idée de frictions entre les employés et les équipes responsables de la cybersécurité n'est pas nouvelle, celles-ci ont été exacerbées par la pandémie, qui a détérioré les relations et amplifié ce problème.
- Un nombre significatif d'employés de bureau se sentent déconnectés et indifférents vis-à-vis de leur rôle dans la protection de leur entreprise.
- De nombreux utilisateurs sont exaspérés et se sentent ralentis par les mesures de sécurité informatique en place et décident ainsi de se rebeller ; un nombre préoccupant d'entre eux décident même de transgresser les limites imposées par ces mesures de sécurité informatique.
- Tout cela complique la tâche des équipes responsables de la sécurité, déjà débordées et subissant des pressions accrues pour protéger les entreprises. Beaucoup d'entre elles craignent qu'à cause de cette situation, des violations de sécurité soient imminentes.
- Les équipes responsables de la sécurité informatique ne se sentent pas appréciées à leur juste valeur, sont frustrées et estiment être incomprises lorsqu'elles tentent de mettre en place des limites de sécurité destinées aux utilisateurs. Leur travail est aujourd'hui devenu une tâche impossible et ingrate.

DERNIÈRES OBSERVATIONS HP WOLF SECURITY

RÉÉVALUER LES POLITIQUES ET RESTRICTIONS DE SÉCURITÉ AFIN DE S'ASSURER QU'ELLES SOIENT BIEN ADAPTÉES

La sécurité est un facteur clé. Nous l'acceptons au quotidien dans le cadre de nos vies personnelles, comprenant bien qu'il serait impossible de consulter notre compte bancaire, d'effectuer des achats en ligne, de communiquer et de faire d'innombrables autres choses sans elle. La sécurité nous fournit des barrières permettant de garantir notre protection.

Mais lorsqu'il s'agit de leur vie professionnelle, beaucoup de gens ont tendance à se concentrer sur ce que les mesures de sécurité les empêchent de faire plutôt que sur ce qu'elles leur permettent de faire en toute sécurité. Si ce point de vue peut paraître réducteur, il est également compréhensible. Dans le cadre de notre nouveau modèle de travail hybride, ajouter de nouvelles restrictions liées à la cybersécurité afin de protéger les employés est tentant, car ils travaillent souvent sans être protégés par les pare-feux de leur entreprise. Mais ces politiques et restrictions de sécurité ont été conçues pour des situations dans lesquelles le travail hybride était une exception et non la norme, et doivent aujourd'hui être réévaluées.

Les RSSI efficaces reconnaissent ce fait. Ils écoutent plus attentivement les utilisateurs finaux afin de comprendre l'impact des mesures de sécurité sur leur flux de travail et leur productivité, et afin de réévaluer ces mesures de sécurité en fonction des besoins de l'entreprise et de ses employés hybrides.

UN SOUTIEN ACCRU POUR LES ÉQUIPES RESPONSABLES DE LA CYBERSÉCURITÉ ÉPUISÉES

Comme le prouve ce rapport, la pandémie a été une période difficile pour les équipes responsables de la sécurité, car les cyberattaques sont devenues plus sophistiquées et les employés moins visibles et moins respectueux des mesures de sécurité en place, rendant ainsi la protection des entreprises plus complexe.

Alors que les équipes responsables de la sécurité s'adaptent à ce nouveau monde professionnel hybride, elles recherchent de nouveaux moyens de sécuriser les terminaux en dehors du réseau de l'entreprise et de bénéficier de capacités avancées de gestion à distance, tout en choisissant des solutions aussi discrètes que possible afin d'éviter que les utilisateurs les contournent.

Les équipes responsables de la cybersécurité ne devraient plus être les seules à endosser la responsabilité de la sécurité des entreprises. Cette dernière devrait également être assignée en partie à chaque employé. Tant que les entreprises ne réaliseront pas que la cybersécurité s'applique à tous les employés, elles resteront de plus en plus vulnérables aux attaques et il sera de plus en plus difficile pour elles d'attirer ou de conserver des talents au sein des équipes responsables de la cybersécurité déjà en sous-effectifs.

POINT DE VUE
HP WOLF SECURITY :

JOANNA BURKEY, RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION, HP INC. :

« La cybersécurité doit être un processus auquel tous les employés peuvent prendre part. Les équipes responsables de la cybersécurité doivent garantir la protection de leur entreprise, mais les utilisateurs doivent également y participer activement. Le processus est le même que pour une sécurité physique : si votre bureau comprend un escalier, vous devez y installer un garde-corps et potentiellement de la moquette au lieu de le carreler, afin d'éviter que des personnes glissent et tombent. Mais dans le même temps, vous faites également confiance à vos employés pour qu'ils ne descendent pas les marches de cet escalier 3 par 3 en courant, risquant ainsi de se blesser. Les équipes responsables de la cybersécurité peuvent vous fournir ce garde-corps, mais il est toujours crucial que les personnes fassent attention. Dans cette nouvelle ère de travail hybride, je me focalise désormais sur comment garantir que chaque employé collabore activement afin de préserver la sécurité de l'entreprise. »

DÉVELOPPER UNE CULTURE DE SÉCURITÉ PLUS COLLABORATIVE

Les RSSI parviennent de plus en plus souvent à faire de la cybersécurité une priorité pour les cadres dirigeants et à mettre en avant l'importance cruciale de son intégration à chaque aspect de la stratégie d'entreprise. Ils doivent désormais s'associer à l'ensemble de leur entreprise afin de faire de la sécurité une composante intégrante de l'ADN de celle-ci.

Les équipes responsables de la cybersécurité doivent permettre une communication ouverte avec les utilisateurs finaux. Une communication claire, percutante et le développement de ressources de formation et d'éducation seront essentiels pour développer une culture de sécurité plus collaborative. Des changements simples comme expliquer la raison justifiant certaines décisions de sécurité ou favoriser les échanges avec les utilisateurs au lieu d'une formation à sens unique avant de déployer de nouvelles politiques permettront de considérablement transformer la manière dont celles-ci sont accueillies. En développant des partenariats et une collaboration liés à la sécurité avec l'ensemble des employés, la cybersécurité pourra devenir un élément clé de la culture d'entreprise.

Afin de créer ces liens, les RSSI devront s'appuyer sur un plus large éventail de compétences de gestion des individus et de communication et sur des équipes plus hétérogènes et à multiples talents, qui pourront inspirer et promouvoir la cybersécurité et ses avantages auprès d'un plus grand nombre d'employés.

HP WOLF SECURITY – UNE SÉCURITÉ NOUVELLE GÉNÉRATION POUR LA SÉCURITÉ DES TERMINAUX

Comme le montre ce rapport, les employés recherchent des outils de sécurité intuitifs et des restrictions modérées, et les équipes responsables de la cybersécurité subissant des pressions. Elles cherchent à alléger leur fardeau en termes de sécurité et à améliorer la visibilité sur les comportements des utilisateurs et les menaces. Pour répondre à ces deux besoins, la technologie a un rôle clé à jouer. Chez HP, aider nos clients à atteindre ces objectifs dans cette nouvelle ère de travail hybride est notre mission.

Intégrer une technologie de sécurité non intrusive aux terminaux permettra de grandement améliorer l'expérience de sécurité des utilisateurs tout en continuant à protéger l'entreprise de manière appropriée. Des appareils comme des PC et imprimantes équipés de fonctionnalités de sécurité intégrées garantiront une expérience utilisateur plus agréable et permettront d'assouplir certaines restrictions.

HP Wolf Security permet aux équipes chargées de la cybersécurité de proposer des outils faciles d'utilisation et d'aider à modérer les restrictions, tout en assurant une défense solide et une protection, une confidentialité et des informations sur les menaces améliorées, en recueillant des données au niveau des appareils afin d'aider à protéger l'entreprise tout entière.

Basé sur le principe de la confiance zéro (« Zero Trust »), HP Wolf Security aide à alléger le fardeau que représente la sécurité. Grâce à leurs fonctionnalités de sécurité robustes intégrées au matériel, les solutions HP Wolf Security peuvent s'auto-contrôler et s'auto-réparer tout en offrant des capacités de gestion à distance permettant une visibilité totale. Les équipes responsables de la cybersécurité peuvent ainsi réduire de manière proactive l'impact des menaces touchant directement ou indirectement le système d'exploitation ou dissimulées, tout en restant transparentes avec les utilisateurs.

HP Wolf Security combine des logiciels et fonctionnalités de sécurité renforcées grâce au matériel et des services de sécurité des terminaux de pointe dans le secteur. Ainsi, les clients bénéficient d'une protection intégrée robuste à tous les niveaux, du matériel au cloud et du BIOS au navigateur, sans restreindre l'accès aux sites web ni empêcher les employés d'ouvrir des pièces jointes d'e-mails. Ils peuvent ainsi travailler sans être interrompus. Les exemples de technologies de pointe assurant une protection non intrusive pour les utilisateurs incluent notamment :

- **Élimination des risques liés aux malwares via la maîtrise des menaces et l'isolation :** la micro-virtualisation permise grâce au matériel isole de manière totale les menaces liées aux facteurs les plus couramment utilisés – e-mails, navigateurs et téléchargements – sans impact sur l'expérience utilisateur. Lorsqu'une tâche est finalisée, la micro-machine virtuelle – et toute menace contenue au sein de celle-ci – est supprimée, sans violation de données. Ainsi, même si un utilisateur clique sur un élément problématique, la personne mal intentionnée l'ayant créé ne peut accéder à aucune donnée et ne peut rien subtiliser.
- **Récupération rapide après une attaque à distance et réduction de la pression subie par le département informatique :** souvent délaissés, les imprimantes et scanners et leur mauvaise utilisation représentent une menace de sécurité croissante. HP Wolf Security résout ce problème en permettant une visibilité et une gestion exhaustives de chaque couche logicielle des imprimantes, y compris la possibilité de modifier le microprogramme et la capacité d'auto-réparation au cas où ces appareils auraient été compromis par un malware. La fonctionnalité de sécurité instantanée applique également immédiatement la politique de sécurité de l'entreprise aux appareils lorsqu'ils sont ajoutés au réseau. HP Security Manager permet aussi d'appliquer plus de 200 paramètres de sécurité aux modèles d'appareils compatibles.
- **Protection des applications clés contre les cybermenaces :** HP Sure Access Enterprise[2] applique la technologie d'isolation unique de HP afin de garantir la protection totale des applications essentielles contre tout malware présent sur le PC d'un utilisateur. HP Sure Access crée des micro-machines virtuelles renforcées grâce au matériel qui permettent de protéger les applications clés – formant ainsi une couche de sécurité virtuelle entre l'application et le PC utilisé. L'application et les données sont isolées de manière sécurisée du système d'exploitation et de toute personne mal intentionnée qui aurait pu y accéder.
- **Utilisation de données télémétriques sur les menaces pour transformer une faiblesse traditionnelle – les terminaux – en source de collecte d'informations :** recueillez des données uniques sur les menaces en permettant aux attaques de se dérouler dans un environnement sécurisé et contrôlé, afin de vous aider à mieux comprendre les menaces visant votre entreprise. Utilisez les informations cloud et données recueillies via les terminaux pour améliorer la collecte de données sur les menaces, tout en profitant d'un aperçu plus global de la sécurité de votre entreprise en automatisant les alertes liées à vos appareils d'impression connectés au sein de votre système d'outils de gestion des évènements et informations de sécurité (SIEM).

À PROPOS DE HP WOLF SECURITY

Conçue par les créateurs des PC[3] et imprimantes[4] les plus sécurisés au monde, la solution HP Wolf Security garantit une sécurité nouvelle génération[1] pour les terminaux. Le portefeuille de services HP offre une sécurité renforcée au niveau du matériel et dédiée à la sécurité des terminaux. Il a été conçu afin d'aider les entreprises à protéger leurs PC, imprimantes ainsi que leurs employés contre les cyberprédateurs. HP Wolf Security assure une protection et une résilience des terminaux intégrées au matériel qui s'étendent aux logiciels et aux services.

MÉTHODOLOGIE

Les résultats inclus dans ce rapport sont basés sur deux sources de données distinctes :

01 Une enquête en ligne réalisée par YouGov auprès de 8 443 adultes vivant aux États-Unis, au Royaume-Uni, au Mexique, en Allemagne, en Australie, au Canada et au Japon, anciens employés de bureau et travaillant chez eux autant ou plus qu'avant la pandémie. Ces données ont été recueillies entre le 17 et le 25 mars 2021. Cette enquête a été effectuée en ligne.

02 Une enquête réalisée par Toluna auprès de 1 100 décideurs informatiques au Royaume-Uni, aux États-Unis, au Canada, au Mexique, en Allemagne, en Australie et au Japon. Ces données ont été recueillies entre le 19 mars et le 6 avril 2021. Cette enquête a été effectuée en ligne.

03 *Le rapport The 2020 Cybersecurity Threat Landscape for Remote Workers as a Result of the COVID-19 Pandemic (Les menaces de cybersécurité pour les télétravailleurs en 2020 suite à la pandémie de COVID-19)* créé par KuppingerCole en mars 2021. Ce dernier fournit un contexte et une analyse liés à l'évolution de l'environnement de travail en 2020 en raison de la pandémie de COVID-19, et se penche sur les activités et habitudes des entreprises et employés dans le monde entier ainsi que sur les activités et tendances des personnes mal intentionnées liées aux vulnérabilités apparues à cause de ce nouveau contexte professionnel.

CLAUSES DE NON-RESPONSABILITÉ

[1] HP Wolf Security est le nouveau nom du service HP Security. Les fonctionnalités de sécurité peuvent varier selon la plateforme. Veuillez consulter la fiche technique du produit pour en savoir plus.
[2] HP Sure Access Enterprise requiert Windows 10 Pro ou Entreprise.
[3] Sur la base des capacités de sécurité uniques et complètes HP proposées sans frais supplémentaires par les différents fournisseurs sur les PC HP Elite équipés de Windows et de processeurs Intel® de 8e génération et supérieurs ou de processeurs AMD Ryzen™ 4000 et supérieurs, les ordinateurs HP ProDesk 600 G6 avec processeurs Intel® de 10e génération et supérieurs et les PC portables HP ProBook 600 avec processeurs AMD Ryzen™ 4000 ou Intel® 11e génération et supérieurs.
[4] Les fonctions de sécurité intégrées HP les plus avancées sont disponibles sur les appareils HP Enterprise et HP Managed avec microprogramme HP FutureSmart 4.5 ou supérieur. Basé sur l'étude réalisée par HP sur les informations relatives aux fonctionnalités publiées en 2021 pour les imprimantes de la même catégorie proposées par la concurrence. Seul HP propose un ensemble de fonctions de sécurité permettant de détecter et d'arrêter automatiquement les attaques, mais aussi de restaurer les terminaux avec un redémarrage d'auto-réparation, conformément aux directives NIST SP 800-193 pour la cyber-résilience des périphériques. Pour consulter la liste des produits compatibles, rendez-vous sur : hp.com/go/PrintersThatProtect. Pour plus d'informations, rendez-vous sur : hp.com/go/PrinterSecurityClaims.

HP WOLF SECURITY