Cybersecurité : les enseignements tirés de l'expansion du télétravail

kaspersky BRING ON THE FUTURE

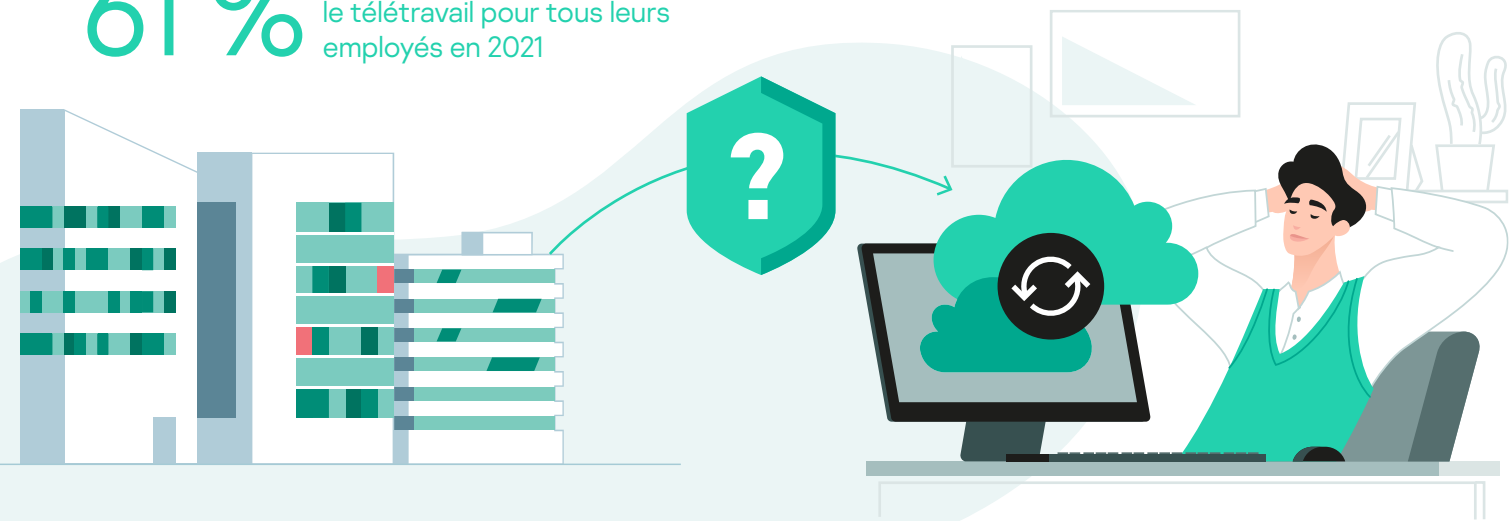
Les options de travail flexible et à distance ont toujours été populaires auprès des employés. Mais lorsque la pandémie a perturbé les opérations, quasiment toutes les entreprises ont été contraintes d'ouvrir leurs réseaux et leurs systèmes pour les opérations à distance.

Un rapport suggère que 61 % des entreprises ont mis en place le télétravail pour tous leurs employés en 2021. Les entreprises sont également désireuses d'encourager cette tendance : 24 % ont l'intention d'augmenter leur utilisation du travail à distance à l'avenir[2].

Mais de nombreuses entreprises ont précipité son déploiement. La priorité était de maintenir un certain niveau de productivité : pratiquement toutes les autres considérations ont été mises de côté en faveur de la rapidité.

Si cela était le cas dans votre entreprise, pouvez-vous être certain que vos dispositions en matière de travail à distance sont sécurisées ?

61 % des entreprises ont mis en place le télétravail pour tous leurs employés en 2021



90 % des professionnels de l'informatique pensent que les télétravailleurs posent un risque de sécurité et 54 % pensent qu'ils représentent un plus grand risque que leurs homologues sur site[3]. Il est évident que le télétravail peut impliquer des risques élevés, cependant, 26 % des entreprises déclarent ne pas disposer de personnel de sécurité suffisant pour gérer correctement leur force de travail à distance[4].

En réalité, en raison de l'entrée en vigueur des confinements, les entreprises ont été contraintes de mettre en place des dispositions de télétravail de masse aussi rapidement que possible. Même lorsque des systèmes de travail à distance existaient déjà, la plupart ne pouvaient être déployés correctement à grande échelle.

Dans de nombreux cas, cela a entraîné une explosion de l'utilisation du Shadow IT, alors que les employés se précipitaient à trouver les outils « suffisamment performants» pour la collaboration et le partage de données. La sécurité et le chiffrement n'étaient pas la priorité dans bon nombre de ces choix, ce qui a conduit à la sélection d'applications non sécurisées et inappropriées[5]. Ces mauvais choix ont considérablement augmenté le risque de perte, de vol ou de fuite de données, en particulier parce qu'ils de disposaient pas de mécanismes de contrôle centralisés qui permettraient aux équipes de sécurité informatique de surveiller ces utilisations et ces abus.

À mesure que le travail à distance a évolué, les entreprises ont commencé à rattraper leur retard. Au cours des 18 derniers mois, ils ont eu le temps d'évaluer les outils et de sélectionner ceux qui protègent le mieux les intérêts de l'entreprise. Néanmoins, ces dispositions restent incertaines en raison de leur assemblage initial.

Ce guide vous aidera à comprendre certains des risques auxquels vous êtes confrontés en termes de terminaux, d'infrastructure et de réseau. Il vous fournira également une feuille de route utile pour améliorer votre stratégie de sécurité à mesure que le périmètre réseau s'érode et que de plus en plus d'appareils inconnus et non fiables sont utilisés pour accéder aux ressources de l'entreprise.

Section 1 - Vos terminaux sont-ils protégés ?

Les appareils utilisés par les travailleurs sont un élément fondamental de votre stratégie de travail à distance. De nombreux responsables informatiques considèrent ceci comme le problème le plus dur à résoudre car les employés utilisent souvent leurs appareils personnels à des fins professionnelles. L'administration évolutive n'en deviendra que plus compliquée.

40 % des responsables informatiques signalent des difficultés à trouver le bon équipement pour leurs télétravailleurs[6], c'est pourquoi 61 % d'entre eux utilisent leur propre équipement[7]. Dans les cas où cela s'est produit, 27 % ont eu du mal à gérer la logistique d'installation des agents de gestion[8]. Toutefois, il doit y avoir un certain degré de contrôle des terminaux pour protéger les ressources de l'entreprise.

Voici quelques-unes des questions que vous devez vous poser :

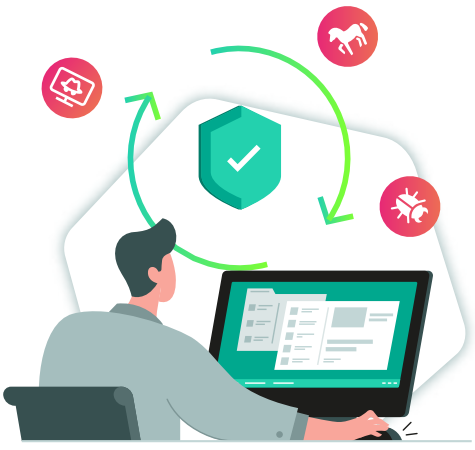
- **Doit-on verrouiller les applications et les systèmes d'exploitation pour éviter toute compromission ?**
- **Est-ce que nos utilisateurs falsifient les paramètres, mettant en danger les systèmes de l'entreprise ?**
- **Comment empêcher un croisement des données personnelles et professionnelles sur les appareils à usage partagé ?**
- **Sommes-nous trop concentrés sur les ordinateurs ? Qu'en est-il des smartphones et des tablettes ?**
- **Comment nous assurons-nous que les appareils client sont correctement corrigés et sécurisés ?**
- **Comment pouvons-nous nous assurer que les employés « respectent les règles » et n'augmentent pas les risques par négligence ?**
- **Comment prendre en charger et gérer les appareils personnels ? Où se situe la limite entre responsabilité professionnelle et personnelle ?**

À bien des égards, les terminaux sont la partie la plus compliquée à gérer de la technologie du travail à distance. La division des biens personnels et des opérations d'entreprise repose sur un compromis entre les deux parties, ce qui est totalement en contradiction avec les principes généraux de sécurité informatique. C'est également pourquoi 20 % des tentatives de piratage sont dirigées vers les appareils des utilisateurs finaux[9].

Néanmoins, 48 % des entreprises ont déjà mis en place des politiques strictes d'accès aux appareils, et 24 % d'entre elles doivent suivre dans l'année à venir[10]. Il se peut que ces entreprises déploient des périphériques d'entreprise ou des sessions VDI pour leurs utilisateurs, plutôt que de continuer avec des appareils personnels à haut risque.

Multi-niveaux

Tout terminal connecté aux ressources de l'entreprise doit être sécurisé à l'aide d'un logiciel contre les programmes malveillants. Empêcher les virus et les ransomwares de pénétrer dans le réseau est essentiel pour contenir la propagation et prévenir les dommages potentiels. Par exemple, 27 % des incidents de sécurité sont causés par des ransomwares [11]. Étonnamment, 91% des travailleurs à distance affirment que leur employeur **ne leur a pas** fourni une solution antivirus à installer sur leur appareil personnel utilisé à des fins professionnelles[12].



Il est essentiel d'utiliser des outils contre les programmes malveillants intelligents qui utilisent des méthodes heuristiques avancées et le Machine Learning pour identifier et bloquer automatiquement les activités et fichiers suspects. Ces outils proactifs réduisent de façon conséquente le risque de compromission, en particulier lorsque l'équipe de sécurité informatique ne peut pas toujours mettre à jour ou contrôler manuellement les appareils distants.

Phishing et usurpation d'identité

Le phishing et les escroqueries par email continuent d'être populaires auprès des cybercriminels car cela fonctionne. 22 % des incidents déclarés en 2020 impliquent le phishing[13]. La bonne nouvelle est que la plupart des systèmes de défense des emails existants continueront de fonctionner, quel que soit l'endroit depuis lequel les télétravailleurs accèdent à leurs boîtes mail, car ils sont hébergés sur le réseau de l'ntreprise (ou sur une plateforme cloud sécurisée).

Cependant, lorsque l'employé dispose d'un appareil à usage mixte, il existe toujours un risque qu'il soit victime d'un email de phishing ou d'une pièce jointe infectée provenant de son compte personnel. En contournant les défenses de l'entreprise, les pirates peuvent toujours acquérir des données et des informations précieuses en trompant les employés via des emails bien conçus.

L'installation d'un logiciel contre les programmes malveillants au niveau du poste de travail peut vous aider, mais les employés doivent également suivre des formations régulières sur l'identification et la gestion des emails. Ils doivent être activement encouragés à utiliser leurs connaissances sur leurs emails personnels, notamment car cela les aidera à éviter de souffrir de pertes personnelles.

Mise à jour et correction des terminaux

Une autre préoccupation majeure concerne la mise à jour et l'application de correctifs aux appareils connectés. Laisser des machines non corrigées est une invitation aux criminels pour en profiter.

Il se peut que les télétravailleurs doivent être rappelés au bureau pour des « bilans de santé » réguliers. Sinon, un calendrier devra être établi afin que les appareils puissent être mis à jour pendant la nuit, conformément à un roulement établi au préalable.

À l'avenir, la migration vers un système VDI hébergé pourrait constituer une meilleure option stratégique. Les images centralisées restent toujours sous votre contrôle, et peuvent être gérées et entretenues de la même manière que les appareils sur site existants.

Comportement de l'utilisateur final

Le comportement des employés a toujours été l'une des plus grandes préoccupations concernant le télétravail. En général, en termes de productivité. Cependant, les comportements sont en tête de la liste des préoccupations des responsables informatiques, avant même le phishing, les mots de passe faibles et une faible sécurité des terminaux et le shadow IT[14]. Pire encore, 52 % des responsables informatiques ont déjà eu le cas d'employés qui ont trouvé un moyen de contourner les systèmes et politiques de sécurité[15]. Il ne s'agit généralement pas d'un comportement malveillant, mais plutôt d'employés qui tentent de gérer les obstacles à l'efficacité et à la productivité. Cependant, chaque raccourci permettant de gagner du temps est également une menace potentielle pour l'intégrité du système.

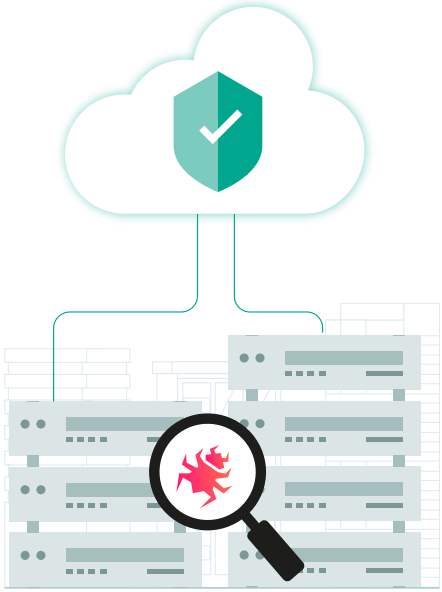
Ce problème est complexe lorsqu'il s'agit d'appareils à usage mixte appartenant à l'employé. Les entreprises devront trouver un compromis avec leurs employés sur la façon d'interagir avec les systèmes de l'entreprise. En particulier, lorsque les utilisateurs ont dépensé en moyenne 348 $ de leur propre argent pour mettre à niveau ou améliorer leurs outils technologiques tout en travaillant à domicile en raison de la pandémie[16]. Encore une fois, les sessions VDI ou sandbox locales peuvent fournir des contrôles supplémentaires qui empêchent les solutions de contournement sans franchir la limite entre professionnel et personnel. 93 % des entreprises ont déjà mis en place une politique de sécurité pour le travail à distance[17], elles doivent maintenant l'appliquer.

« Confiance zéro » sur le poste de travail

Bien qu'un modèle « Confiance zéro » soit déployé au niveau de l'infrastructure, il a également un rôle à jouer au niveau des terminaux. Les systèmes doivent être configurés pour surveiller et vérifier soigneusement l'activité à distance afin de contrôler et limiter l'accès si nécessaire.

Les mécanismes « Confiance zéro » permettront de résoudre de nombreuses incertitudes liées aux appareils « inconnus ». Les employés à distance bénéficient d'accès avec moins de privilèges, ce qui leur permet d'utiliser les ressources dont ils ont besoin pour faire leur travail, sans exposer d'autres systèmes qui ne leurs sont pas nécessaires. Des contrôles peuvent être appliqués au niveau des postes de travail, du réseau et de l'infrastructure pour une sécurité granulaire et une protection accrue des ressources de l'entreprise.

Section 2 : votre infrastructure est-elle protégée ?



Pour la plupart des entreprises, leur infrastructure de base doit déjà être bien sécurisée, du moins pour une utilisation en interne. Cependant, le passage au télétravail a fait des trous dans la sécurité du périmètre pour fournir un accès aux ressources centralisées.

À mesure que vos capacités de travail à distance évoluent, votre équipe de sécurité informatique doit se poser des questions difficiles :

- **Devons-nous migrer les télétravailleurs vers une infrastructure de bureau virtuel (VDI) ?**
- **Existe-t-il des applications internes qui pourraient être mieux sécurisées en migrant vers une alternative SaaS/hébergée dans le cloud ?**
- **Comment contrôlons-nous l'accès aux ressources internes ?**
- **Comment les données sont-elles protégées, en particulier si elles sont stockées en dehors du périmètre réseau ?**
- **Comment pouvons-nous atténuer les effets des programmes malveillants et des ransomwares ?**

Conserver les données dans le réseau

En conservant vos systèmes et données au sein du réseau d'entreprise, vous réduisez immédiatement le risque de perte, de vol ou de fuite. L'utilisation de solutions VDI offre à vos utilisateurs une expérience semblable à celle d'un poste de travail classique et garantit que les données soient conservées à l'intérieur de votre infrastructure de client léger. Il n'est pas nécessaire de transférer des fichiers ou des données vers l'appareil local où le risque de compromission est plus important

Utiliser la puissance du cloud

Les applications basées dans le cloud et le SaaS sont généralement protégées par des défenses de sécurité de niveau professionnel. Il peut être plus approprié et plus efficace de migrer les applications hors du data center sur site. En plus de simplifier votre accès à distance à ces applications, l'activation dans le cloud peut accroître la sécurité globale de vos données.

Renforcer le contrôle des comptes

Les mots de passe restent une source continue de problèmes : en moyenne, les entreprises subissent 922 331 tentatives de collecte d'identifiants chaque année[18], tandis que 37 % des violations impliquent des identifiants volés[19]. Maintenir la sécurité des mots de passe dans le périmètre réseau a toujours été difficile. Mais les terminaux distants augmentent le risque d'exposition ou de vol des identifiants. La mise à niveau des contrôles de compte par l'utilisation de l'authentification unique (SSO) et l'authentification multi-facteurs (MFA) ou les alternatives sans mot de passe offre une couche de protection supplémentaire si les informations d'identification sont compromises.

Vous pouvez renforcer vos défenses en utilisant une authentification continue et à l'analyse des anomalies. Ces outils surveillent l'activité de l'utilisateur pour identifier et bloquer automatiquement les comportements suspects afin de limiter les dommages en cas de violation réussie.

Partage de fichiers

En plus de pouvoir accéder facilement aux données, les télétravailleurs doivent pouvoir collaborer avec leurs collègues. Il existe un risque important que les utilisateurs se tournent vers des comptes personnels avec des plateformes telles que Dropbox ou Google Drive, ce qui place les données hors de votre contrôle et augmente le risque d'exposition.

Vous devrez identifier et déployer des systèmes de partage de fichiers approuvés pour les travailleurs à distance, y compris des versions payantes et contrôlables de services tels Dropbox et Google Drive. Vos dispositions en matière de partage de fichiers doivent appliquer le chiffrement à toutes les données en transit et stockées.

Vous pouvez améliorer la protection de vos données à l'aide d'un courtier de sécurité d'accès au cloud (CASB). Le CASB agit comme proxy pour appliquer des règles aux données lorsqu'elles sont transférées depuis et vers le cloud. De cette façon, vous pouvez vous assurer que les données sont utilisées de manière responsable depuis n'importe quel appareil, y compris les smartphones et tablettes personnels non gérés.

Stockage dans un coffre-fort

Les ransomwares représentent une menace réelle et importante pour tous vos systèmes. Une infection non contrôlée peut mettre les systèmes de production et les sauvegardes hors ligne, ce qui rend la récupération complète presque impossible.

Le stockage dans un coffre-fort (à l'aide de sauvegardes immuables), empêche que les fichiers ne soient chiffrés. Il s'agit d'une couche de protection importante lorsque les utilisateurs distants introduisent inévitablement des ransomwares sur le réseau.

Adopter une approche « Confiance zéro »

Le changement stratégique le plus important que votre entreprise doit adopter à l'heure du travail à distance est celle de l'approche de sécurité « Confiance zéro ». Selon les directives émises par l'Agence nationale de sécurité américaine, le modèle de sécurité « Confiance zéro » fonctionne sur trois principes fondamentaux :

1. **Ne faites jamais confiance, vérifiez toujours** : traitez chaque utilisateur, appareil, application/charge de travail et flux de données comme indigne de confiance. Authentifiez et autorisez explicitement chacun d'eux, jusqu'au moindre privilège requis en utilisant des politiques de sécurité dynamiques.

2. **Supposez une violation** : exploitez et défendez consciemment les ressources en supposant qu'un ennemi est déjà présent dans votre environnement. Refusez par défaut et examinez attentivement tous les utilisateurs, appareils, flux de données et demandes d'accès. Consignez, inspectez et surveillez en permanence toutes les modifications de configuration, les accès aux ressources et le trafic réseau pour détecter les activités suspectes.

3. **Vérifiez explicitement** : l'accès à toutes les ressources doit être effectué de manière cohérente et sécurisée à l'aide de multiples attributs (dynamiques et statiques) afin d'obtenir des niveaux de confiance pour les décisions d'accès contextuel aux ressources[20].

L'utilisation des principes « Confiance zéro » permet d'identifier et de limiter les problèmes plus rapidement, et de concevoir une infrastructure plus sûre et plus sécurisée pour vos télétravailleurs. La surveillance dépasse la simple évaluation de l'activité des utilisateurs. Toute opération ou interaction est évaluée, ce qui permet d'identifier les erreurs de configuration ainsi que les tentatives de piratage actives.

Section 3 : votre réseau est-il protégé ?

Vos utilisateurs ont besoin d'une connectivité sécurisée et fiable pour pouvoir accéder aux ressources de l'entreprise afin d'effectuer leur travail. Le déploiement de connexions VPN est relativement simple, mais leur gestion, leur maintenance et leur contrôle constitue une surcharge administrative importante.

Pour déterminer si votre réseau est correctement sécurisé pour le travail à distance, vous devez savoir :

- **Toutes les connexions entrantes et sortantes sont-elles sécurisées sur les appareils de nos collaborateurs à distance ?**
- **Comment traitons-nous le phishing et les site Web factices ?**
- **Comment nos utilisateurs accèdent-ils à Internet ?**
- **Quelles sont les menaces qui existent au sein des bureaux de nos utilisateurs ?**

La connexion entre l'utilisateur final et les ressources de l'entreprise est un autre point faible de vos dispositions en matière de travail à distance.

Chiffrer les connexions

Les connexions à un réseaux privé virtuel (VPN) sont désormais une méthode de connectivité standard, utilisée par 72 % des entreprises pour accorder l'accès au réseau d'entreprise[21]. En chiffrant le trafic entre les terminaux, vous pouvez empêcher la plupart des attaques par écoute courantes. À l'avenir, vous devrez vous assurer que des niveaux de chiffrement similaires sont appliqués à toutes les ressources distantes, y compris les plateformes cloud et SaaS.

Il existe cependant un petit point de préoccupation : seuls 43 % des télétravailleurs interrogés déclarent utiliser un VPN lorsqu'ils travaillent à domicile[22]. Il semblerait que de nombreux utilisateurs ne se rendent pas compte que leurs connexions sont chiffrées. Au lieu de cela, cela indique un manque de formation et de connaissances en matière de sécurité de base qui les aiderait à jouer leur rôle dans la protection de l'entreprise.

Secure Access Service Edge (SASE)

Les VPN sont utiles pour sécuriser les connexions entre les terminaux et le data center de l'entreprise, mais le réseau moderne utilise largement les actifs distribués tels que les services cloud. La technologie SASE unifie la technologie WAN avec des services de sécurité réseau tels que CASB (voir ci-dessus), Firewall as a Service et « Confiance zéro » dans un panneau de configuration centralisé.

SASE est fourni sous forme de service cloud, qui surveille l'identité de l'entité, fournit un contexte en temps réel, applique les politiques de sécurité/conformité de l'entreprise et évalue en continu le risque/la confiance tout au long des sessions. SASE est flexible, évolutif et capable de protéger les données sur site, dans le cloud et à tout moment lors du transit.

Filtrer les requêtes

Généralement, les applications antivirus des terminaux détectent et bloquent les requêtes réseau suspectes, mais que se passe-t-il si l'utilisateur final désactive les protections locales ? L'activation du filtrage DNS permet une couche supplémentaire de sécurité réseau, empêche les programmes malveillants de se connecter à leur base et réduit le risque que les utilisateurs se trouvent piégés dans des sites malveillants.

Politiques Wi-Fi

Le travail à distance n'est pas toujours limité au bureau à domicile. Les espaces de coworking et même les cafés sont désormais considérés comme des lieux de travail viables par vos employés. Cependant, la possibilité d'attaques de type « Man-in-the-Middle » et d'autres attaques et piratages de connexion sont un risque grave pour la sécurité.

La connectivité VPN par défaut offre une certaine protection, mais vous devez également informer les utilisateurs sur l'utilisation du Wi-Fi public en toute sécurité, le cas échéant, et établir des politiques en conséquence.

Utilisation du réseau domestique

À l'heure de la domotique contrôlée dans le cloud, les réseaux domestiques de vos utilisateurs sont aussi de moins en moins sécurisés. Lorsque vous travaillez à domicile, votre entreprise n'a que très peu de contrôle direct sur le réseau partagé, ce qui pourrait être utilisé pour compromettre les appareils d'entreprise connectés, souvent par le biais d'appareils IoT mal sécurisés.

Vous devez investir dans des technologies qui renforcent vos appareils locaux afin qu'ils puissent mieux se défendre contre les programmes malveillants locaux, les attaques externes et les autres exploits qui pourraient être utilisés pour établir des connexions au réseau d'entreprise. La plupart des routeurs Wi-Fi domestiques offrent désormais des fonctionnalités de double réseau. Encourager les télétravailleurs à configurer et à utiliser le réseau secondaire pour séparer le trafic personnel et professionnel contribuera à empêcher le croisement. Seulement 7 % des entreprises utilisent actuellement cette méthode, ce qui représente une opportunité manquée importante d'améliorer la sécurité de bout en bout[23].

Conclusion : renforcer votre stratégie de sécurité concernant le travail à distance

Comme nous l'avons vu, une sécurité efficace pour le travail à distance est un processus en trois parties. Votre stratégie doit tenir compte de l'infrastructure, de la mise en réseau et des appareils utilisés par les employés pour accéder aux ressources de l'entreprise.

L'utilisation d'appareils personnels crée un double défi. D'abord, vous devez répondre aux préoccupations de vos employés qui pourraient penser que leur vie privée et leur autonomie sont violées. Vous devez ensuite identifier un moyen de gérer et de contrôler un réseau en constante évolution qui opère en dehors de vos contrôles existants.

À l'avenir, les entreprises devront renforcer leurs défenses à tous les niveaux : data center, réseau et terminal. Des outils tels que CASB et « Confiance zéro » aident à résoudre certains de ces problèmes, tout comme les efforts de normalisation des applications et des outils utilisés par les télétravailleurs.

À l'avenir, SASE sera crucial, permettant aux entreprises d'adapter la sécurité à l'évolution de leurs besoins. L'adoption est actuellement très faible (environ 1 %[24]), mais elle devrait s'accélérer rapidement, car les entreprises consolident leurs kits outils pour simplifier la gestion de la sécurité et la couverture. La sécurité deviendra enfin omniprésente, protégeant les systèmes et les ressources systématiquement, quel que soit leur emplacement. Lorsque cela se produit, la différence entre le travail à distance et les opérations sur site, d'un point de vue de la sécurité, sera négligeable.

Le travail à distance dissout-il le périmètre de votre entreprise ? Trop de tâches urgentes et pas assez de temps pour les traiter ? Vous souhaitez une solution EDR (et en avez besoin), mais sa complexité vous inquiète ? Voici comment Kaspersky peut vous aider à relever ces défis

Que vous souhaitiez renforcer vos défenses internes ou combattre les nouvelles menaces avec des conseils externes d'experts, Kaspersky peut vous y aider. Notre solution native du cloud Kaspersky Optimum Security vous permet de mettre votre protection à niveau contre les menaces nouvelles, inconnues et évasives, par le biais d'un système de détection et de réponse efficace et d'une surveillance sécurisée 24h/24 et 7j/7, sans frais exorbitants ni complexité. Plus de visibilité, plus de puissance, plus de contrôle.

Plus d'informations sur https://go.kaspersky.com/EDR-Security_fr.html

Lecture recommandée :

Le machine learning dans la cybersécurité
Comment savoir de quel niveau de protection des terminaux vous avez besoin
Guide d'achat de solutions EDR
Boostez la cybersécurité de vos équipes en télétravail en renforçant vos systèmes

---

[1] ISC Cybersecurity Workforce Study 2021 – (ISC)2 – https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx
[2] Business and individual attitudes towards the future of homeworking, UK: April to May 2021 – Office for National Statistics – https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/articles/businessandindividualattitudestowardsthefutureofhomeworkinguk/apriltomay2021
[3] The Flexible Revolution: Are You Ready? – OpenVPN – https://openvpn.net/images/open-vpn-quick-poll/openvpn-remote-workforce-poll.pdf
[4] 2021 Remote Workforce Security Report – Cybersecurity Insiders – https://f.hubspotusercontent10.net/hubfs/8541268/2020_%20Guides/2021-Remote-Workforce-Security-Report-Axiad-Final.pdf
[5] Zoom security issues: Everything that's gone wrong (so far) – Tom's Guide – https://www.tomsguide.com/news/zoom-security-privacy-woes
[6] 2021 Remote Workforce Security Report – Cybersecurity Insiders – https://f.hubspotusercontent10.net/hubfs/8541268/2020_%20Guides/2021-Remote-Workforce-Security-Report-Axiad-Final.pdf
[7] COVID-19 Cybersecurity in the Remote Workforce – PC Matic – https://www.pcmatic.com/news/covid-19/
[8] 2021 Remote Workforce Security Report – Cybersecurity Insiders – https://f.hubspotusercontent10.net/hubfs/8541268/2020_%20Guides/2021-Remote-Workforce-Security-Report-Axiad-Final.pdf
[9] 2020 Data Breach Investigations Report – Verizon – https://enterprise.verizon.com/en-gb/resources/reports/2020-data-breach-investigations-report.pdf
[10] Digital Distancing: Why remote working demands better cybersecurity in a changed world – Computing – https://view.computing.co.uk/carbon-black-digital-distancing/p/1
[11] 2020 Data Breach Investigations Report – Verizon – https://enterprise.verizon.com/en-gb/resources/reports/2020-data-breach-investigations-report.pdf
[12] COVID-19 Cybersecurity in the Remote Workforce – PC Matic – https://www.pcmatic.com/news/covid-19/
[13] Ibid.
[14] Digital Distancing: Why remote working demands better cybersecurity in a changed world – Computing – https://view.computing.co.uk/carbon-black-digital-distancing/p/1
[15] 2021 Remote Workforce Security Report – Cybersecurity Insiders – https://f.hubspotusercontent10.net/hubfs/8541268/2020_%20Guides/2021-Remote-Workforce-Security-Report-Axiad-Final.pdf
[16] People are Working More by Not Going to Work, but Worry about Home Tech, Data Security and Personal Costs – Lenovo – https://news.lenovo.com/pressroom/press-releases/new-lenovo-research-people-are-working-more-by-not-going-to-work-but-worry-about-home-tech-data-security-and-personal-costs/
[17] The Flexible Revolution: Are You Ready? – OpenVPN – https://openvpn.net/images/open-vpn-quick-poll/openvpn-remote-workforce-poll.pdf
[18] 2020 Data Breach Investigations Report – Verizon – https://enterprise.verizon.com/en-gb/resources/reports/2020-data-breach-investigations-report.pdf
[19] 2020 Data Breach Investigations Report – Verizon – https://enterprise.verizon.com/en-gb/resources/reports/2020-data-breach-investigations-report.pdf
[20] Embracing a Zero Trust Security Model – National Security Agency – https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF
[21] Digital Distancing: Why remote working demands better cybersecurity in a changed world – Computing – https://view.computing.co.uk/carbon-black-digital-distancing/p/1
[22] COVID-19 Cybersecurity in the Remote Workforce – PC Matic – https://www.pcmatic.com/news/covid-19/
[23] Ibid.
[24] Hype Cycle for Enterprise Networking, 2020 – Gartner – https://www.gartner.com/en/documents/3987266

www.kaspersky.fr

kaspersky BRING ON THE FUTURE