Votre checklist de protection contre les ransomwares

kaspersky BRING ON THE FUTURE

Les ransomwares restent une menace grandissante pour toutes les entreprises. Une estimation stipule que 15,45 % de tous les utilisateurs d'Internet ont subi au moins une attaque par un programme malveillant en 2021[1]. Sans surprise, la cybersécurité est une priorité stratégique de plus en plus importante pour les entreprises.

Le risque d'infection par un ransomware a augmenté ces dernières années, en particulier avec la démocratisation du travail à distance en réponse à la pandémie. Les études suggèrent que cette ruée vers le télétravail a entraîné une réduction de la surveillance de nombreuses entreprises, ou un assouplissement d'un certain nombre de leurs protocoles de sécurité habituels.

En ce qui concerne les ransomwares, l'accent est principalement mis sur la restauration des accès aux données chiffrées le plus rapidement possible. Cependant, il est important de se rappeler que les cybercriminels exfiltrent souvent des fichiers à des fins de chantage en demandant de nouveaux paiements pour éviter la fuite d'informations sensibles.

Moins d'entreprises ont déployé des outils de sécurité réseau (-5 %) ou de surveillance des utilisateurs finaux (-6 %) en 2021[2]. Sans une surveillance et une sécurité des terminaux efficaces, le risque d'être victime d'un ransomware augmente considérablement.

Les terminaux ont toujours été un maillon faible dans la sécurité de l'entreprise, car ils représentent la surface d'attaque la plus vulnérable pour les pirates. Cependant, le travail à distance a déplacé ces points d'accès **en dehors** du périmètre réseau, ce qui complique encore la gestion de la sécurité. La prolifération des terminaux offre aux pirates un plus grand choix de cibles potentielles, augmentant ainsi leurs chances de réussite.

Pour éviter une épidemie importante, une stratégie efficace contre les ransomwares doit intervenir à plusieurs niveaux. Alors que le télétravail devient une habitude, les entreprises doivent affiner et renforcer la protection de leurs terminaux, en particulier dans la façon dont elles détectent et bloquent les infections par ransomware.

Ce guide sert de checklist pratique, pour vous aider à évaluer votre niveau de protection contre les ransomwares à la périphérie du réseau, et améliorer vos défenses, notamment :

- **1. Détection des ransomwares sur les terminaux**
- **2. Configuration des terminaux**
- **3. Dispositions en matière de sauvegarde**
- **4. Opérations de délestage**
- **5. Formation des utilisateurs**
- **6. Planification de la réponse aux incidents**

[1]Kaspersky Security Bulletin 2021. Statistiques – Kaspersky –https://securelist.com/kaspersky-security-bulletin-2021-statistics/105205/

[2]Cyber Security Breaches Survey 2021 – UK Department for Digital, Culture, Media & Sport – https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021

1. Détection des ransomwares sur les terminaux

Il est extrêmement important d'arrêter les ransomwares avant qu'ils ne prolifèrent. Plus une infection est identifiée et bloquée rapidement, moins elle causera de dommages et de perturbations.

En général, votre entreprise peut détecter un programme malveillant qui a été envoyé par email directement aux employés sur le serveur de messagerie, mais cela ne les empêche pas d'être piégés et de télécharger des exécutables externes via à une attaque par phishing ciblée bien conçue.

Vous pouvez améliorer vos capacités de détection des ransomwares en bloquant les fichiers exécutables suspects sur le terminal :

- **Déployez un outil puissant contre les programmes malveillants pour identifier et supprimer les fichiers exécutables suspects avant qu'ils ne puissent chiffrer les fichiers sensibles.**
- **Utilisez les capacités de Machine Learning des outils EDR (Endpoint Detection and Response) pour identifier et bloquer automatiquement les activités systèmes suspectes.**
- **Envisagez d'adopter une solution MDR (Managed Detection and Response) pour automatiser et accélérer les efforts de protection contre les ransomwares.**

Le déploiement de ces outils contribuera à contenir une infection, l'empêchant ainsi de se propager à d'autres systèmes et fichiers.

Il convient de noter que les organismes fédéraux et les agences gouvernementales renforcent leur position sur la façon dont les victimes répondent aux infections par ransomwares. En 2019, l'Internet Crime Complaint Center (IC3) du FBI a incité les entreprises à ne pas payer de rançons[3].

Kaspersky fait écho à ce conseil : « Ne payez pas. Tout paiement de rançon représente une contribution financière au développement de programmes malveillants et un signal aux cybercriminels indiquant que ce plan est rentable. Et cela pourrait ne pas fonctionner, vous pourriez ne rien obtenir du tout même si vous collaborez. »[4]

Le Federal Office for Information Security (BSI) allemand propose des conseils avisés : « La meilleure protection contre les demandes de rançon émanant des cybercriminels est de mettre en place des mesures de sécurité informatique systématiques. »[5]

La mise en place systématique de mesures informatiques signifie d'appliquer des protections sur les terminaux **à l'extérieur** du périmètre réseau similaires à celles appliquées à l'intérieur de celui-ci. Dans ce cas, une protection contre les programmes malveillants efficace et fiable ainsi que des outils EDR intelligents qui peuvent détecter automatiquement les activités de type ransomware.

2. Configuration des terminaux

La configuration des terminaux contribuera également à réduire les effets potentiels d'une infection par un ransomware. Pour les appareils de votre entreprise :

- Utilisez la liste autorisée du répertoire d'application pour vous assurer que vos employés ne peuvent exécuter que des logiciels autorisés. Une fois la restriction appropriée en place, ils ne peuvent pas installer d'application, ce qui réduit les risques d'exécution de fichiers exécutables infectés.
- Assurez-vous que les outils de sécurité des terminaux, ainsi que tout autre logiciel installé, sont configurés pour se mettre à jour automatiquement afin de bloquer les nouvelles menaces et de fermer la porte aux vulnérabilités potentielles avant qu'elles ne puissent être exploitées.[6].

Les bonnes pratiques en matière de sécurité suggèrent d'appliquer les mises à jour logicielles dans les 14 jours suivant leur publication. Malheureusement, à peine 43 % des entreprises le font[7]. Relativement facile à mettre en place, c'est une opportunité manquée d'empêcher la propagation des ransomwares.

[3]High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations – FBI Internet Crime Complaint Center –https://www.ic3.gov/Media/Y2019/PSA191002
[4]Five tips for protecting yourself from ransomware – Kaspersky –https://www.kaspersky.com/blog/ransomware-five-tips/41444/
[5]Ibid.
[6]Ransomware world in 2021: who, how and why – Kaspersky –https://securelist.com/ransomware-world-in-2021/102169/
[7]Cyber Security Breaches Survey 2021 – UK Department for Digital, Culture, Media & Sport – https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021

Les terminaux BYOD représentent un défi supplémentaire, car votre entreprise ne peut exercer qu'un contrôle limité sur l'appareil. Dans ce modèle opérationnel, vous disposez de plusieurs options :

- Encourager les employés à installer un outil de protection contre les programmes malveillants approuvé sur chacun de leurs appareils. La mise à disposition d'un logiciel gratuit est une bonne initiative, car il protégera les données personnelles des employés ainsi que les actifs de l'entreprise.

- Utiliser la technologie de sandboxing pour les données et applications professionnelles afin qu'elles soient maintenues à l'écart des applications personnelles. Si un employé accède à un programme malveillant en utilisant ses applications personnelles, la technologique de sandboxing fournit une mesure de protection contre la propagation.

Enfin, la protection des appareils personnels des utilisateurs sera un processus de compromis, en acceptant de mettre en place des mesures qui conviennent à l'entreprise et à l'employé. Lorsque cela n'est pas possible, votre entreprise devra envisager de fournir des méthodes d'accès alternatives ou de fournir aux employés des appareils appartenant à l'entreprise.

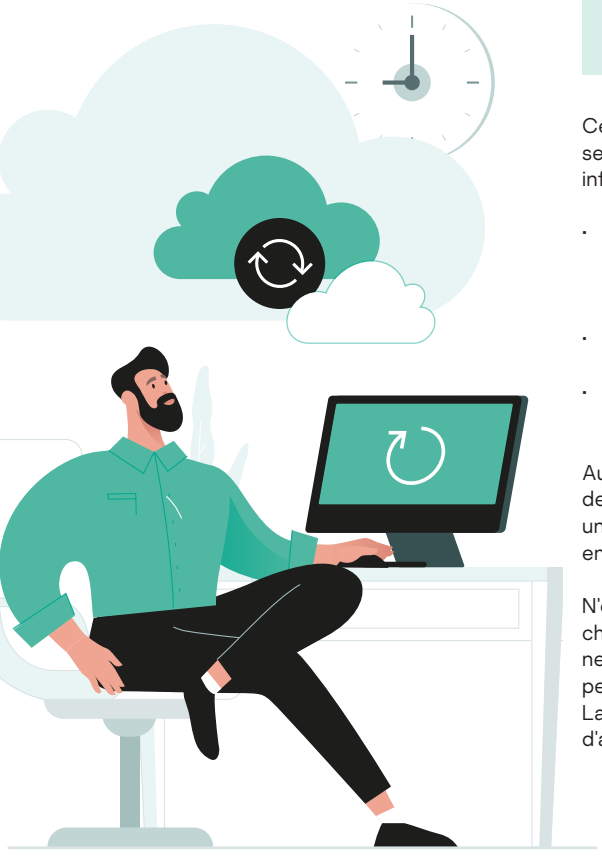
3. Dispositions en matière de sauvegarde

Une fois les fichiers chiffrés, il existe deux options : payer la rançon ou récupérer des copies « propres » des fichiers à partir d'une sauvegarde. Ce qui signifie disposer d'une procédure de sauvegarde fiable et robuste pour vos terminaux également.

Dans un déploiement idéal, les employés n'auraient pas la possibilité de stocker des données d'entreprise localement. Mais en réalité, ils enregistreront probablement des documents sur leur disque local, souvent dans le dossier Téléchargements ou sur le Bureau.

Pour vous préparer à un travail à distance plus sûr, vous devez vous demander :

- **Quelle est la probabilité que les données d'entreprise soient stockées localement ?**
- **Quelles données sont enregistrées ?**
- **Quels sont les risques si ces fichiers sont chiffrés ou rendus inaccessibles ?**
- **Comment sauvegarder ces données ?**



Ceci est un défi important en dehors du périmètre réseau. Votre façon de résoudre le problème sera déterminée par votre architecture technique, et, dans une certaine mesure, par les capacités informatiques de vos utilisateurs finaux. Voici les options à prendre en compte :

- Synchroniser les données de dossiers sélectionnés vers le stockage cloud ou un autre service distant, de préférence avec des sauvegardes immuables qui ne peuvent être écrasées ou modifiées.

- Sauvegarder sur un disque local amovible.

- S'appuyer sur les fonctionnalités intégrées au système d'exploitation pour créer des copies masquées automatiques et des points de sauvegarde.

Aucune de ces solutions potentielles n'est idéale, car il existe une menace inhérente à la réplication des ransomwares et aux fichiers chiffrés dans la sauvegarde. Cependant, vous devez identifier un moyen de capturer les données stockées localement, notamment pour respecter les obligations en matière de protection des données et de conformité.

N'oubliez jamais : la sauvegarde des données est votre dernière ligne de défense contre les fichiers chiffrés par ransomware. Gardez également à l'esprit qu'une sauvegarde et une récupération ne protègent pas votre entreprise contre les fuites de données, ou la divulgation. Les criminels peuvent toujours demander une rançon sous la menace d'exposer des informations sensibles. La seule défense face à ces attaques contre la **confidentialité** est d'empêcher les criminels d'accéder à vos terminaux.

4. Opérations de délestage

Plus le nombre de données et d'applications stockées sur un terminal est élevé, plus il y a de vulnérabilités potentielles à exploiter. Et plus ce terminal devient attractif pour les pirates. Ainsi, **en réduisant** la quantité d'applications et de données stockées localement, l'impact d'une infection par ransomware sera moindre.

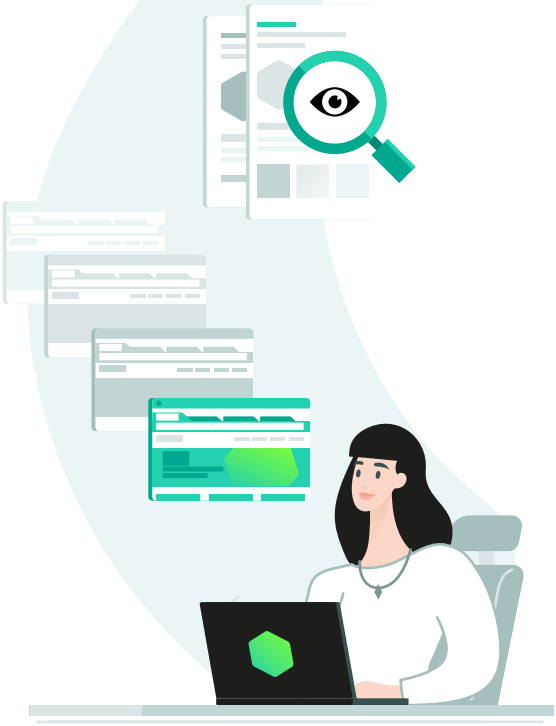
Les services cloud ont fourni un moyen de délester les applications, réduisant ainsi la quantité de données stockées sur l'appareil local. Par exemple, les outils de messagerie et de productivité peuvent maintenant être exécutés comme des applications Web dans le cloud, en veillant à ce que peu ou rien ne soit transféré localement. Nombre d'entre eux, en particulier les services de messagerie, offrent également une protection contre les programmes malveillants avancée pour analyser, détecter et bloquer les pièces jointes suspectes avant que vos utilisateurs ne puissent les télécharger.

La virtualisation offre une autre possibilité. Grâce au streaming d'application sur le poste de travail, les utilisateurs peuvent se connecter à une session hébergée dans le cloud ou le data center de l'entreprise. La session hébergée offre à l'utilisateur final une session similaire au poste de travail, mais toutes les données et tous les traitements sont effectués dans le système virtualisé.

Les sessions Bureau à distance (RDP) sont considérées comme le principal vecteur d'attaque pour les ransomwares[8]. Mais lorsqu'elles sont correctement paramétrées, cela créé une sandbox utile entre le terminal et les systèmes de l'entreprise, comme en témoigne l'utilisation intensive de RDP au sein du réseau d'entreprise.

Il est possible de bénéficier des mêmes avantages pour les télétravailleurs en renforçant la sécurité des terminaux, à savoir :

- **Mettre en place une stratégie de mots de passe fort pour éviter les attaques de force brute.**
- **Déployer une authentification multi-facteurs pour éviter que les sessions ne soient piratées.**
- **Utiliser des connexions VPN pour tout le trafic entre les terminaux et les serveurs RDP.**
- **Evaluer et renforcer les règles de pare-feu de périmètre réseau pour éviter les connexions non autorisées.**
- **Utiliser des outils de sécurité EDR pour évaluer l'activité afin d'identifier et bloquer automatiquement les activités suspectes.**
- **Choisir des ports de connexion RDP non standard pour éviter les tentatives de piratage spéculatives.**



Enfin, la clé est d'empêcher les pirates et les logiciels malveillants de compromettre une connexion ou une session RDP, ce qui implique de protéger correctement le terminal de l'utilisateur.

5. Formation des utilisateurs finaux

Les employés sont les actifs les plus précieux de toute entreprise, et ils peuvent jouer un rôle important pour éviter la propagation des ransomwares, s'ils savent quoi faire. Tous les employés, et pas seulement ceux à distance, doivent recevoir une formation régulière afin d'être équipés pour identifier les attaques de cybersécurité potentielles, et ce qu'ils doivent faire ensuite. Chaque jour, 2 % des employés cliquent sur un lien de phishing[9], et nous pouvons nous attendre à des chiffres similaires en ce qui concerne les ransomwares.

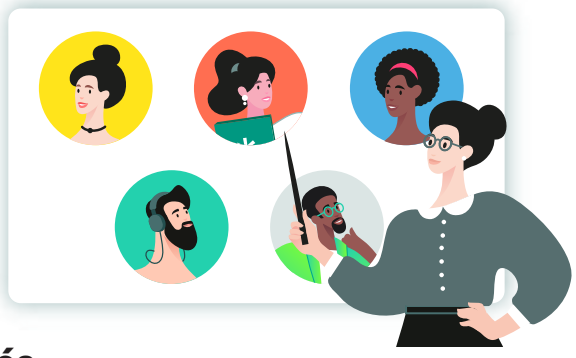
La formation doit être interactive, pratique et régulière, car les menaces de cybersécurité évoluent en permanence. Une présentation unique sur l'identification des emails de phishing et les exécutables suspects deviendra rapidement obsolète (et sera oubliée). Voici quelques facteurs à prendre en compte lors de la conception de la formation à la cybersécurité à destination de vos télétravailleurs.

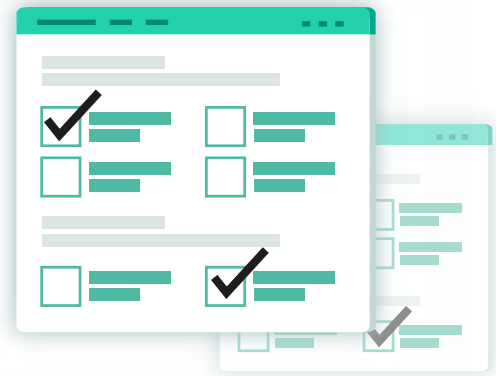
[8]How to secure RDP from ransomware attackers – Emsisoft –https://blog.emsisoft.com/en/36601/how-to-secure-rdp-from-ransomware-attackers/

[9]Mobile Security Index 2020 Report – Verizon – https://www.verizon.com/business/en-gb/resources/reports/mobile-security-index/2020/mobile-threat-landscape/user-threats/

Adapter la formation

Les attaques de ransomware les plus efficaces sont soigneusement ciblées sur des personnes et des rôles spécifiques. Il fait donc sens d'adapter la formation de la même manière. Finance, marketing, RH et cadres seront tous confrontés à des attaques légèrement différentes. Ainsi, les former dans leur propre « langage » aux menaces auxquelles ils sont susceptibles de faire face leur sera plus utile et sera plus efficace pour l'entreprise.



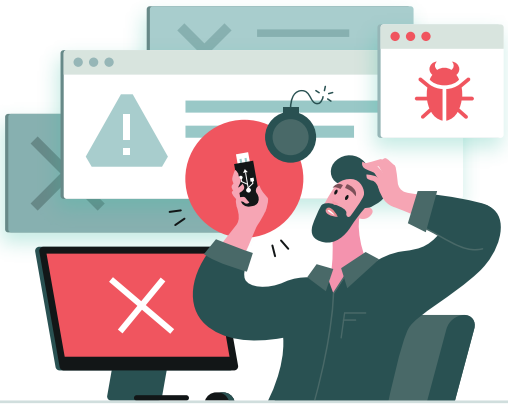


Tester vos employés

La connaissance a peu de valeur jusqu'à ce qu'elle soit utilisée, en particulier lorsque les enjeux sont si élevés. Tester les compétences de vos employés régulièrement garantit qu'ils pourront mettre en pratique leur formation si nécessaire. Les évaluations de routine mettent également en évidence les lacunes ou les possibilités d'améliorer leurs compétences et la sécurité de votre entreprise.

Aller au delà du phishing

Le phishing et les pièces jointes malveillantes sont la source potentielle d'infection par ransomware la plus évidente. Cependant, il existe d'autres facteurs que vos utilisateurs finaux doivent connaître. Les lecteurs amovibles infectés, les sites Web malveillants et la contamination croisée entre les activités professionnelles et personnelles peuvent tous introduire des programmes malveillants sur le terminal, et le réseau de l'entreprise. Vous devez vous assurer que vos employés sont formés et conscients de ces problèmes potentiels.

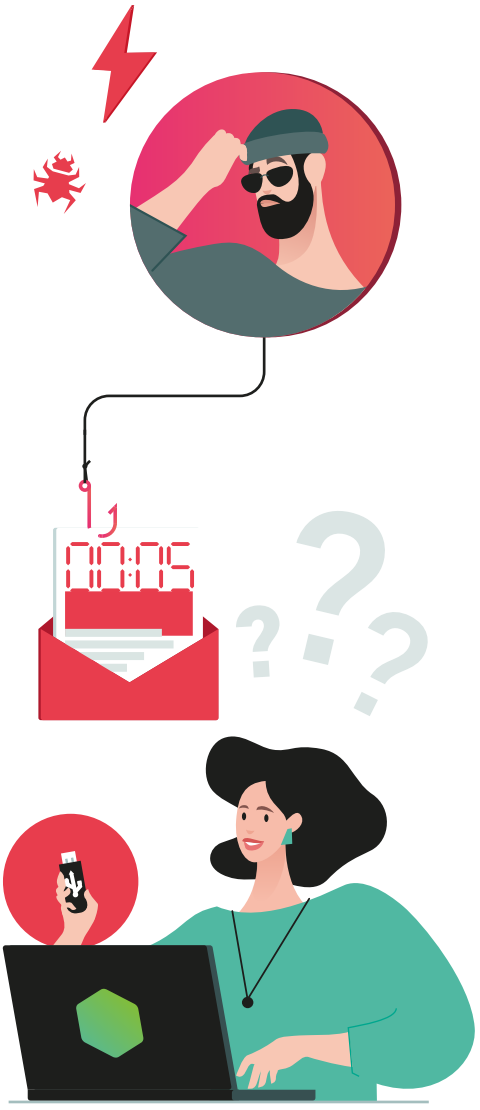


Rendez-la amusante (et/ou intéressante)

La cybersécurité peut être ennuyeuse, en particulier si ce n'est pas votre responsabilité première. Il est peu probable que vos utilisateurs finaux lisent (ou comprennent) les briefings hebdomadaires de la US National Cyber Awareness System par exemple. L'utilisation d'une approche ludique contribuera à accroître l'intérêt et l'engagement, en particulier à mesure que les concepts enseignés deviendront plus complexes. La définition d'objectifs et de défis, l'encouragement de la compétition et le plaisir du processus encourageront vos employés à rester connectés, et à continuer à améliorer leurs connaissances et compétences.

Investir dans vos utilisateurs finaux est une étape importante vers le renforcement de la protection de vos terminaux. En effet, minimiser l'erreur humaine est peut-être la manière la plus efficace de prévention des ransomwares. Cela aidera également vos employés à jouer un rôle efficace dans les premiers stades d'une infection par ransomware, aidant à minimiser la propagation et l'impact global sur l'entreprise.

6. Planification de la réponse aux incidents



32 % des entreprises ne disposent pas d'un plan officiel de réponse aux incidents pour gérer les incidents de cybersécurité tels qu'une infection par ransomware.[10]. Ces organisations assument un niveau de risque injustifiable, car elles rencontreront toutes un incident de programme malveillant dans un avenir proche.

L'élaboration d'un plan de réponse aux incidents aidera votre entreprise à évaluer les vulnérabilités et à prendre les mesures appropriées pour les atténuer. Ce plan vous aidera également à accélérer votre temps de réponse, ce qui est essentiel lorsque vous traitez des ransomwares où chaque seconde compte.

Bien qu'il soit propre à votre entreprise, tout plan de reprise d'activité d'un terminal après sinistre doit inclure :

- **Une stratégie de communication.** Vous devez vous assurer que les bonnes informations soient transmises à la bonne partie prenante au bon moment. Mais aussi que vos télétravailleurs soient en mesure de contacter des experts qui pourront les aider dans les premiers stades d'une infection.
- **Un plan d'attaque.** Décidez de la manière dont la gravité d'une attaque est déterminée et comment vous y répondrez. Allez-vous payer la rançon, ou essaierez-vous de récupérer les données à partir d'une sauvegarde ?
- **De la documentation accessible.** Il existe une très forte probabilité que l'infection d'un terminal empêche les employés d'accéder aux guides et aux instructions de réponse aux ransomwares. Vous devez vous assurer qu'il existe toujours un moyen d'obtenir ces informations, même si leurs systèmes sont en panne.
- **Un conseil aux employés.** Dès qu'un problème est détecté, vous devez désigner un spécialiste qui peut aider le télétravailleur. Il pourra l'aider dans les premières étapes d'atténuation et de récupération, et collecter des informations à inclure dans le rapport aux organismes de réglementation si la situation l'exige.
- **Une vigilance accrue.** Dès qu'une infection par un ransomware est détectée sur un terminal distant, votre équipe de sécurité informatique doit augmenter les niveaux de surveillance et de reporting pour évaluer si les systèmes centraux ont également été compromis. Ils peuvent ensuite déclencher le plan de reprise d'activité si nécessaire.

Grâce à un plan de reprise d'activité après sinistre bien conçu, votre entreprise sera mieux positionnée pour réduire l'impact des programmes malveillants, contenant idéalement la propagation avant qu'elle n'atteigne les systèmes et données critiques.

[10]Cyber Security Breaches Survey 2021 – UK Department for Digital, Culture, Media & Sport – https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021

Conclusion

Depuis de nombreuses années, les responsables informatiques avaient des inquiétudes concernant le travail à distance, à juste titre. Cependant, les événements récents ont changé les pratqiues, et le télétravail est désormais la norme au sein des entreprises.

Dans le même temps, les ransomwares sont devenus un outil standard dans le kit du cybercriminel. Les attaques contre les entreprises sont fréquentes, efficaces et potentiellement dévastatrices. Avec la surface d'attaque plus étendue des télétravailleurs, il est très probable que toutes les entreprises soient infectée à un moment donné.

La protection des terminaux contre les ransomwares doit donc être une priorité stratégique. Dans le cas contraire, il pourrait être trop tard pour que votre entreprise réagisse efficacement lorsque l'inévitable se produira.

Les six facteurs décrits dans ce document aideront immédiatement votre entreprise à être mieux préparée contre les ransomwares. La prise en compte de ces facteurs améliorera immédiatement votre stratégie de sécurité des terminaux :

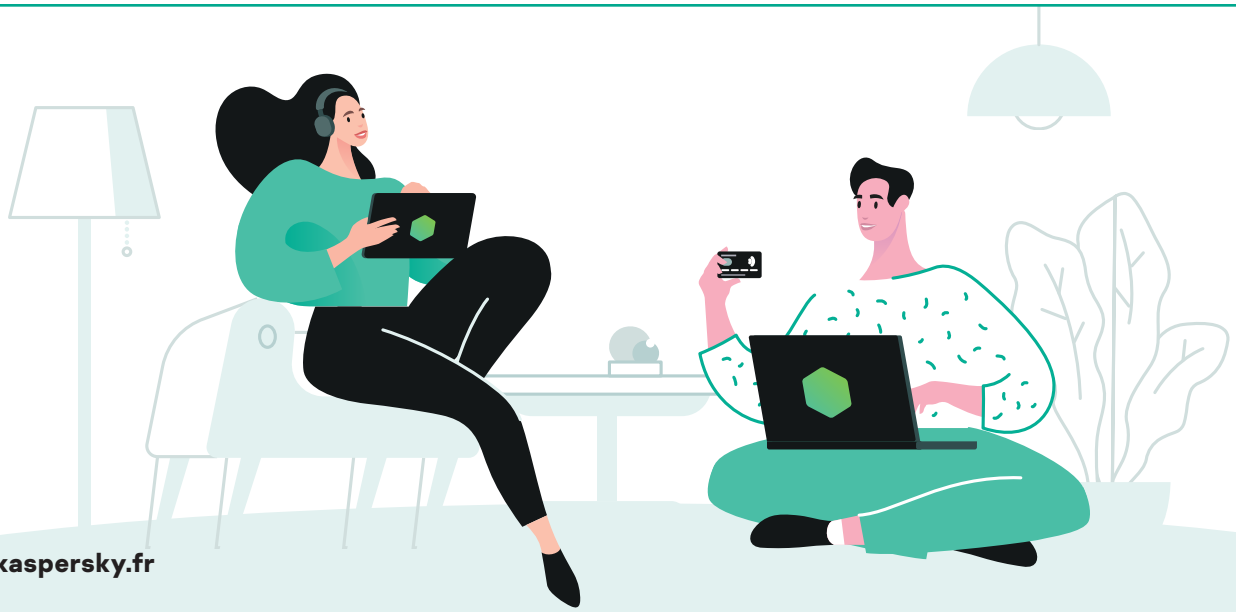
1. Détection et suppression des programmes malveillants
2. Configuration des appareils
3. Sauvegarde et restauration des données
4. Opérations de délestage
5. Formation
6. Plan de reprise d'activité après sinistre

Si vous souhaitez en savoir plus sur la protection des télétravailleurs et de votre entreprise contre les ransomwares, Kaspersky peut vous aider. Notre solution dans le 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 :

L'histoire de l'année : les ransomwares à la une
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



www.kaspersky.fr

kaspersky BRING ON THE FUTURE