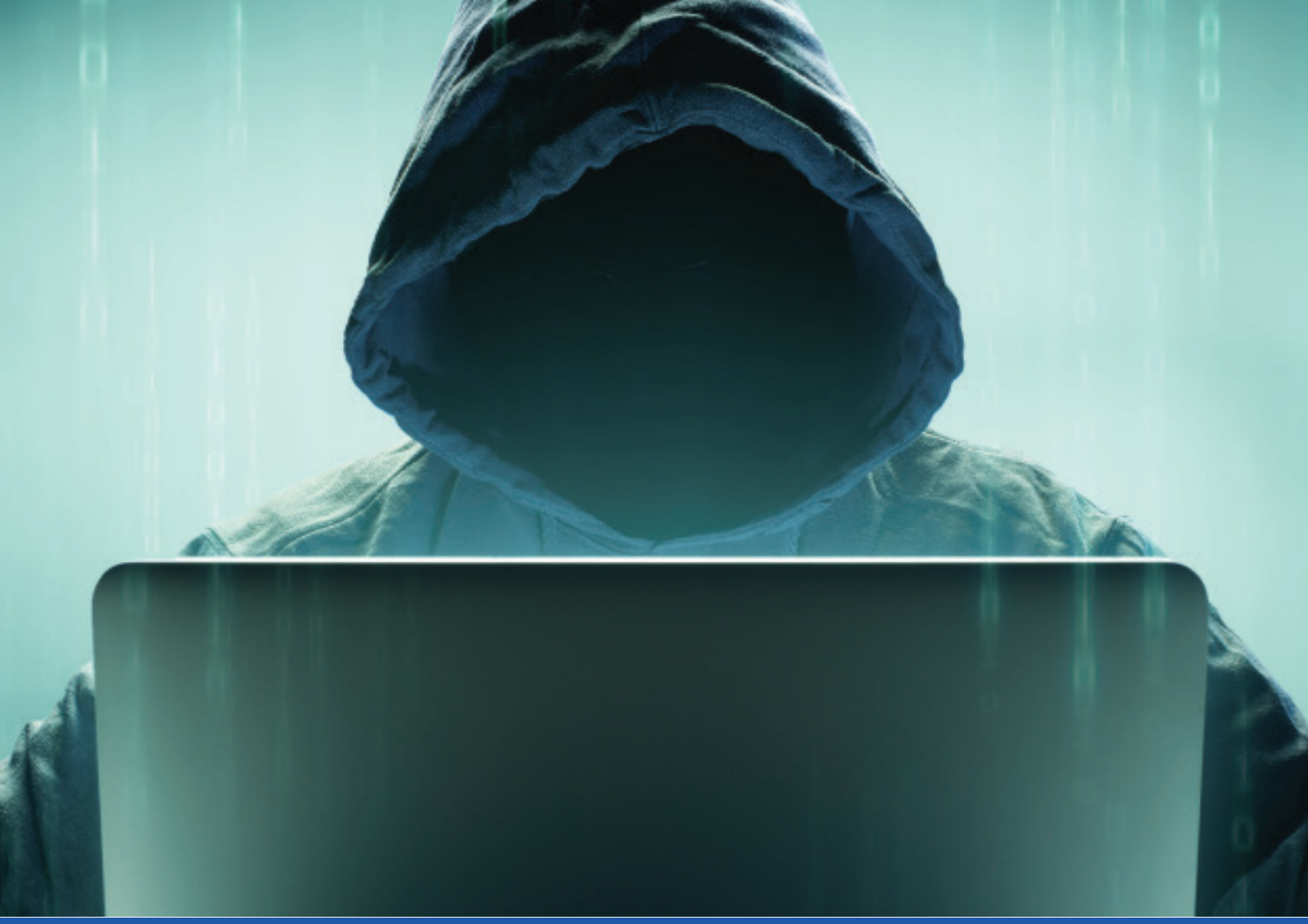


Comment se protéger des ransomwares

Ontrack®

1. La sécurité des boîtes email est essentielle

D'après McAfee, le **phishing par email** est encore l'un des principaux points d'entrée du ransomware, particulièrement dans le cas d'attaques ciblées.

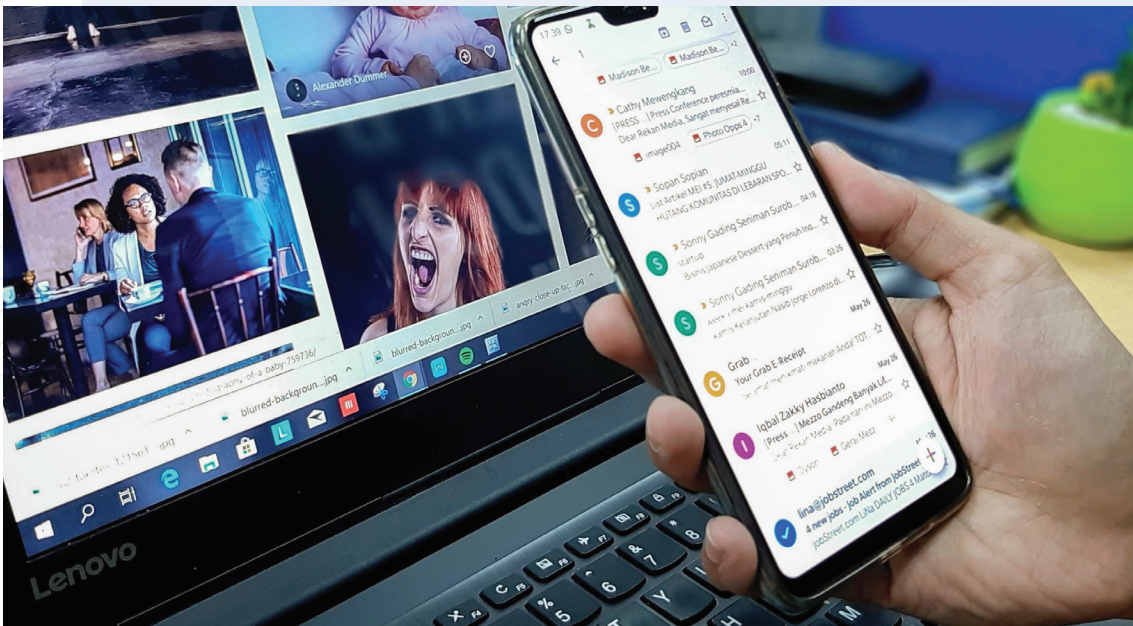
Ainsi, sécuriser cette principale source de vulnérabilité est essentiel pour quiconque administre un réseau ou se connecte à Internet.

La plupart des individus déclenchent une attaque ransomware en ouvrant ce qui semble être un email normal contenant le virus dans un document, une photo, une vidéo ou tout autre type de fichier. La plupart des hackers aujourd'hui **n'ont pas besoin de compétences avancées** pour insérer un malware dans un fichier. Il existe de nombreux articles et tutoriels YouTube avec les instructions détaillées sur la façon de procéder.

En gardant ceci à l'esprit, vous devez toujours **éviter d'ouvrir un email provenant d'un expéditeur inconnu**.

Si vous recevez un email d'une source inconnue, informez votre responsable en sécurité des données ou l'équipe informatique de votre société immédiatement.

N'oubliez pas : mettre les systèmes informatiques et les données de votre société à l'abri est la bonne décision.



2. Sécurisez votre réseau et votre environnement informatique

Lorsqu'un ransomware infecte un ordinateur, il ne fait aucun doute qu'il s'agit d'un problème sérieux. Mais lorsqu'il se propage sur l'ensemble du réseau, cela peut virer au cauchemar et mettre en danger l'entreprise dans son ensemble.

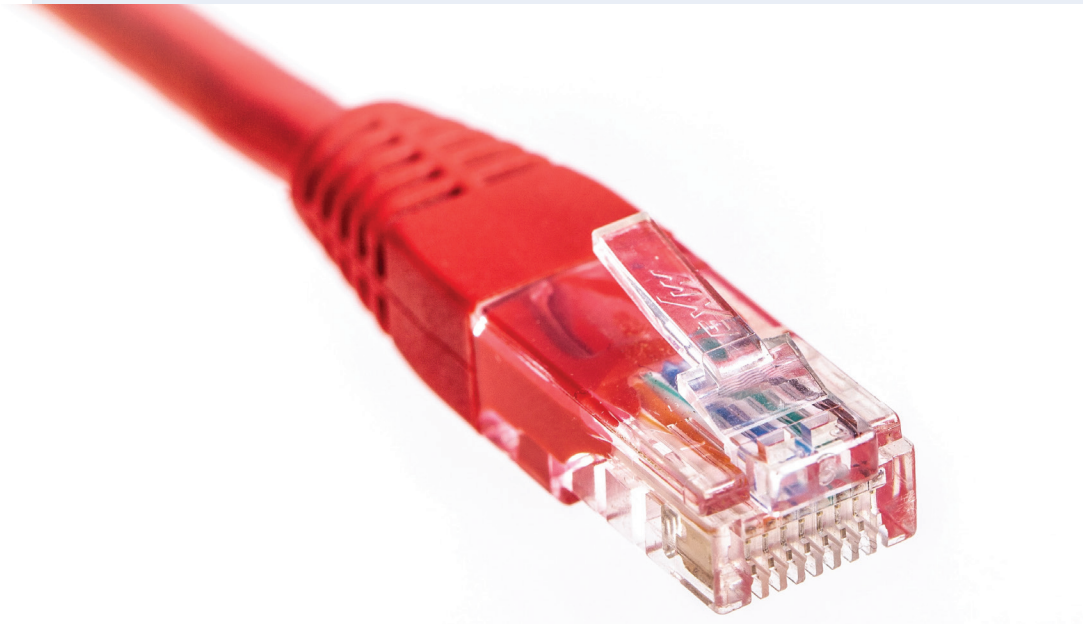
Les sociétés qui ne l'ont pas déjà fait doivent envisager l'implémentation d'un **logiciel de sécurité des données** qui contrôle tous les emails entrants avant que les destinataires ne les reçoivent.

Une telle solution r**éduira drastiquement les risques** qu'un **virus se diffuse** à l'intérieur d'un réseau d'entreprise.

Les administrateurs et responsables informatiques doivent également envisager l'implémentation d'un logiciel de sécurité qui surveille automatiquement le réseau et ses fichiers à la recherche d'éventuelles menaces.

La solution alertera les administrateurs si une attaque ransomware tente de chiffrer d'importantes quantités de fichiers sur le réseau.

Dernier point, mais non des moindres : toujours **mettre à jour** vos **logiciels et systèmes d'exploitation** à l'aide des derniers correctifs lorsqu'ils sont disponibles. Comme il est souvent souligné, les attaques de hackers réussissent uniquement lorsque les politiques en matière de sécurité des données présentent des failles.



3. Formation des employés

Même les utilisateurs expérimentés en informatique commencent à paniquer lorsqu'ils se rendent compte qu'ils font face à une attaque ransomware. Il est donc primordial que **chaque employé dans une société sache exactement que faire** si une attaque ransomware se produit, y compris la direction et les responsables du département informatique.

Les protocoles concernant la conduite à tenir en cas d'attaque ransomware doivent non seulement faire partie d'un plan de continuité des opérations pour les cadres supérieurs ou les experts informatiques, mais des **directives précises** quant aux actions à mener doivent être visibles et assimilées dans chaque bureau. Celles-ci peuvent être simples mais efficaces, par exemple :

- Déconnecter les ordinateurs d'internet et du réseau interne,
- Essayer d'arrêter l'appareil infecté correctement et appeler immédiatement la sécurité et l'administration informatiques.

Les personnels de la sécurité et de l'administration informatiques doivent être informés en permanence des derniers développements en matière de cybersécurité et de hacking.

Par conséquent, il est impératif qu'une formation continue soit suivie, que les dernières actualités sur ces sujets soient consultées, et que les nouveaux développements dans ce domaine et les failles des réseaux ou des solutions logicielles soient assimilés.

4. Sécurisez le protocole de bureau à distance (RDP) de votre organisation

Si votre organisation n'a pas besoin d'utiliser le protocole RDP, le mieux est de le remplacer par une solution plus sécurisée. Si ce n'est pas possible, les **mesures** suivantes doivent être mises en place :

- Utilisez un VPN pour accéder au RDP de votre organisation, ceci permet de créer une connexion sécurisée entre les employés d'une organisation et internet. L'ensemble du trafic de données passe par un tunnel virtuel chiffré, ainsi les cybercriminels ne sont pas en mesure d'accéder à un système par la force brute,
- Assurez-vous qu'une authentification à deux facteurs est configurée,
- Les employés responsables de la maintenance d'importants services internes doivent disposer de l'accès maximum requis pour être en mesure de faire leur travail. Une authentification à deux facteurs doit être configurée pour tout employé ayant accès aux systèmes ou sauvegardes critiques,
- Disposez d'un plan de récupération en cas de sinistre à jour pour garantir que vous avez sous la main une sauvegarde des données critiques si votre RDP est compromis.

5. Faites en sorte d’avoir une sauvegarde à jour

Vous protéger signifie également disposer d’une sauvegarde de vos données.

Une sauvegarde hautement sécurisée est un élément primordial dans la préparation de votre organisation en cas d’attaque ransomware.

Vous devez tester votre sauvegarde de façon rigoureuse et fréquente, mais surtout, elle doit également permettre de restaurer les données en toute simplicité.

Cela signifie que si vous êtes frappé par un malware quel qu’il soit, vous serez en mesure de **reconstruire votre système** rapidement et sans problème. Si possible, assurez-vous que votre système de sauvegarde n’est pas connecté à votre réseau (ou alors seulement pendant la durée où vous en avez besoin), ceci vous permettra d’éviter que votre sauvegarde soit affectée par un malware également.

Que devez-vous faire si vous êtes frappé par une attaque ransomware ?

Si pour une quelconque raison un ransomware parvient à franchir votre ligne de défense, vous devez faire ce qui suit :

- **Ne jamais payer la rançon !** Accéder à la requête des malfaiteurs ne garantit pas que vous récupérerez vos données. Très souvent, et très certainement s'il s'agit d'un ranscam ou d'un malware wiper, vous ne récupérerez pas vos données, et vous vous retrouverez sans données et avec un gouffre dans vos finances,
- **N'essayez pas de déchiffrer les données vous-même.** Certains spécialistes en informatique peuvent avoir les compétences pour récupérer les données perdues, mais c'est risqué. Si les choses se déroulent mal, vous pourriez détruire vos données pour toujours,
- **Vérifiez votre sauvegarde !** Même si votre sauvegarde est manquante après une attaque ransomware, n'excluez jamais la possibilité d'une récupération. Les solutions possibles dépendent du type de support ou du système de stockage, ainsi que du type de ransomware.

Ontrack®
2, impasse de la Noisette
91370 Verrières-le-Buisson, France
24/7 +33 (0)1 69 53 66 99
www.ontrack.com/fr