Explosion des ransomwares : les quatre protections à ne pas négliger

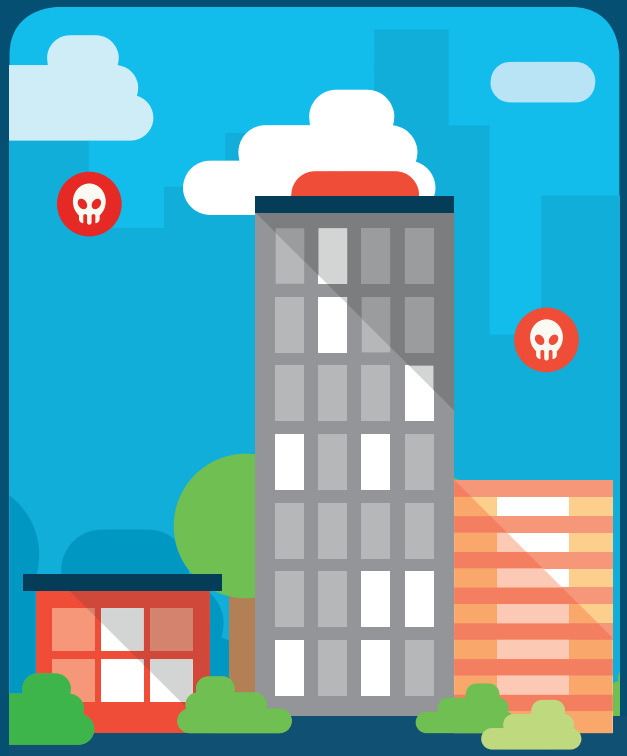
Ransomwares : vous savez que le risque existe.

Les problèmes posés par les ransomwares sont de plus en plus prégnants et ne sont pas près de disparaître. Vous n'êtes certainement pas serein en songeant au risque de perdre tout accès à vos systèmes stratégiques et à vos données. Aucune entreprise ne souhaite qu'un hacker la menace de perdre ses données si elle ne paye pas immédiatement une rançon.

Vous avez d'ailleurs sans doute déjà commencé à vous recentrer sur la sauvegarde et la récupération des données. La tâche est ardue, mais vous êtes bien conscient que vous ne pouvez pas y échapper. Mais au-delà ce ces mesures, savez-vous quelles protections vous devez mettre en place en priorité ?

Quatre d'entre elles sont incontournables.

Découvrons ensemble ces quatre protections à ne pas négliger.



Les quatre protections à ne pas négliger

Sécurité au niveau DNS

Sécurité de la messagerie

Protection contre les malwares sur les terminaux

Plan de gestion des incidents

Pour vous protéger contre les ransomwares, il vous faut bien plus qu'une bonne stratégie de sauvegarde. Vous devez prendre des mesures préventives, tout en préparant votre équipe à agir dès l'attaque.

Pour être efficace, une solution de prévention basée sur les risques doit non seulement prendre en compte les menaces, mais aussi vos vulnérabilités, la probabilité d'occurrence et la gravité de l'impact. Vous savez déjà quelles sont les menaces et ce que peuvent être leurs conséquences. Mais connaissez-vous vos vulnérabilités et les risques que vous soyez impacté ?

Les entreprises ont toutes les mêmes cibles vulnérables. Les collaborateurs.

Tout le monde peut se faire piéger et cliquer sur un lien malveillant ou ouvrir une pièce jointe nuisible qui télécharge un ransomware. Le terminal infecté propage alors le ransomware sur votre réseau vers les systèmes critiques. Les fichiers sont chiffrés, les systèmes sont ralentis ou désactivés et vous recevez une demande de paiement pour récupérer vos données.

Cette méthode d'attaque est tellement efficace que les hackers ne cessent de cibler de nouveaux utilisateurs chaque jour. C'est pourquoi la probabilité qu'une personne de votre entreprise fasse quelque chose qui augmente le risque d'infection par un ransomware est très élevée. Avec des utilisateurs, vous êtes forcément exposé. Vous êtes vulnérable à une attaque par ransomware.

En cas d'attaque par ransomware, savez-vous combien de temps il vous faudra pour tout restaurer à partir d'une sauvegarde ? Quelles seront les pertes induites par une interruption si longue ?

Pour restaurer rapidement les opérations, beaucoup d'entreprises sont tentées de payer la rançon. Ne le faites pas.

Stoppez les ransomwares avant que ce scénario se produise. Vous pouvez agir de différentes manières, mais voici quatre mesures essentielles à mettre en place pour vous protéger contre les ransomwares les plus virulents :

Pour plus d'informations sur Cisco Ransomware Defense, consultez le site :

www.cisco.com/go/ransomware

Les quatre protections à ne pas négliger.

Sécurité au niveau DNS

Internet ne fonctionne pas sans DNS (système de noms de domaine), et c'est également le cas des ransomwares. Les hackers ont besoin de la souplesse du DNS. C'est pourquoi les ransomwares n'ont généralement pas d'adresses IP codées en dur. Aujourd'hui, plus de 90 % des variantes de ransomwares permettent aux hackers de garder le contrôle grâce au DNS.

Comme vous exécutez déjà un DNS sur votre réseau, pourquoi ne pas l'utiliser pour évacuer les ransomwares hors de votre réseau ?

Avec la sécurité au niveau du DNS, vous pouvez bloquer l'accès aux domaines réputés malveillants. Ainsi, le système de l'utilisateur ne peut tout simplement pas se connecter à des sites malveillants, puisque la sécurité au niveau du DNS ne lui donne pas les adresses IP. C'est la première ligne de défense contre les ransomwares et elle est très efficace.

Vous ne devez donc pas négliger la sécurité au niveau du DNS.

Cisco Umbrella fournit une sécurité au niveau du DNS et est le composant clé de la solution Cisco Ransomware Defense.

Sécurité de la messagerie

Qui n'utilise pas la messagerie électronique ? Il est presque impossible de s'en passer pour travailler. Malheureusement, l'e-mail est aussi le point d'entrée le plus courant des ransomwares, les hackers trompant les utilisateurs avec des e-mails d'apparence fiable (mais pourtant faux). Et ces e-mails contiennent des pièces jointes ou des liens nuisibles.

Comme vous ne pouvez pas vous passer des e-mails, nous vous recommandons d'intégrer une solution de sécurisation dans votre système de messagerie électronique existant.

Protégez-vous contre les ransomwares en stoppant les spams et les e-mails de phishing. Supprimez les pièces jointes malveillantes. Les utilisateurs ne peuvent pas cliquer sur des liens nuisibles ou ouvrir des pièces jointes malveillantes s'ils ne les reçoivent pas. Réduisez les risques liés aux ransomwares transmis par e-mail.

Vous ne devez pas négliger la sécurité de la messagerie électronique.

La solution Cisco de sécurité de la messagerie avec Advanced Malware Protection (AMP) empêche les ransomwares d'arriver dans la messagerie en éliminant la menace. C'est un autre composant clé de la solution Cisco Ransomware Defense.

Protection contre les malwares sur les terminaux

Quels que soient vos efforts, les malwares trouvent toujours un moyen d'atteindre les terminaux des utilisateurs et de se propager sur votre réseau. Les utilisateurs accèdent à des sites web malveillants, téléchargent des fichiers nuisibles, installent des applications frauduleuses, ouvrent des pièces jointes sans se méfier et partagent des clés USB infectées. Il est impossible d'empêcher totalement les comportements à risque, et ce, en dépit de toutes les formations que vous dispensez pour sensibiliser les utilisateurs à la sécurité.

Il est essentiel de vous doter d'une protection avancée contre les malwares sur tous vos terminaux, des équipements des utilisateurs aux serveurs stratégiques.

Les terminaux sont des points d'entrée. Ils contiennent également vos données critiques. Vous avez besoin

d'une solution pour analyser et bloquer les malwares avant qu'ils s'exécutent sur les équipements et les hôtes.

C'est pourquoi il est impératif de ne pas négliger la protection contre les malwares sur l'ensemble de vos terminaux.

Cisco AMP pour Endpoints fournit une protection essentielle contre les malwares sur les terminaux. C'est le troisième composant clé de la solution Cisco Ransomware Defense.

Plan de gestion des incidents

Vous avez déjà renforcé votre programme de sauvegarde des données, car vous êtes conscient de l'importance de la continuité des activités et de la planification de la reprise après sinistre. Bien que cette tâche soit difficile et chronophage, la menace croissante présentée par les ransomwares la rend indispensable.

Bien sûr, vous ne pouvez pas commencer à restaurer avant d'avoir résolu la cause du problème. Savez-vous comment agir juste après avoir détecté une attaque ? Comment allez-vous intervenir pour contenir rapidement les dommages ? En l'absence d'un plan de gestion des incidents robuste, une attaque par ransomware peut créer le chaos.

Vous ne devez donc pas négliger l'importance de la planification de la gestion des incidents.

Les experts en gestion des incidents des Services Cisco vous aident à développer ce plan de gestion et à traiter les cyberattaques actives qui provoquent déjà des dommages. Nous encourageons nos services de gestion des incidents à compléter les technologies préventives de la solution Cisco Ransomware Defense.

Conformité avec les bonnes pratiques de cybersécurité

Les quatre protections à ne pas négliger s'appuient sur des références solides. Elles sont conformes aux bonnes pratiques actuelles plébiscitées en matière de cybersécurité comme les contrôles CIS (Center for Internet Security). Par exemple :

Contrôle CIS 3 : protection des configurations matérielles et logicielles sur les terminaux mobiles, les ordinateurs portables, les postes de travail et les serveurs. La sécurité au niveau du DNS fournie par Cisco Umbrella est l'une des nombreuses configurations sécurisées qui renforcent le système et diminuent les vulnérabilités.

Contrôle CIS 7 : protection de la messagerie et du web. La solution Cisco de sécurité de la messagerie avec AMP s'harmonise parfaitement avec ce contrôle.

Contrôle CIS 8 : défenses contre les malwares. Les solutions Cisco AMP pour Endpoints et de sécurité de la messagerie avec AMP fournissent les protections essentielles contre les malwares spécifiées par ce contrôle.

Contrôle CIS 19 : gestion et maîtrise des incidents. Les services de gestion des incidents Cisco vous aident à développer l'ensemble complet de contrôles des utilisateurs et des processus recommandés par le CIS. Ce que nous appelons « Plan de gestion des incidents » constitue l'infrastructure détaillée de gestion des incidents spécifiée par ce contrôle. Par ailleurs, nos spécialistes de la gestion des incidents vous aident à prendre les mesures correctives nécessaires lorsque vous subissez une attaque par ransomware active ou d'autres cyberattaques.

Ne vous limitez pas à quatre

Ne vous contentez pas de mettre en place ces quatre protections. La solution Cisco Ransomware Defense va plus loin et intègre les fonctionnalités suivantes :

Segmentation du réseau. Séparez de façon logique les composants qui ne devraient pas communiquer entre eux sur votre réseau.

Visibilité et politique cohérente. Bénéficiez d'une vue d'ensemble des composants de votre réseau et de la façon dont ils communiquent entre eux pour mettre en place une politique d'accès claire et cohérente.