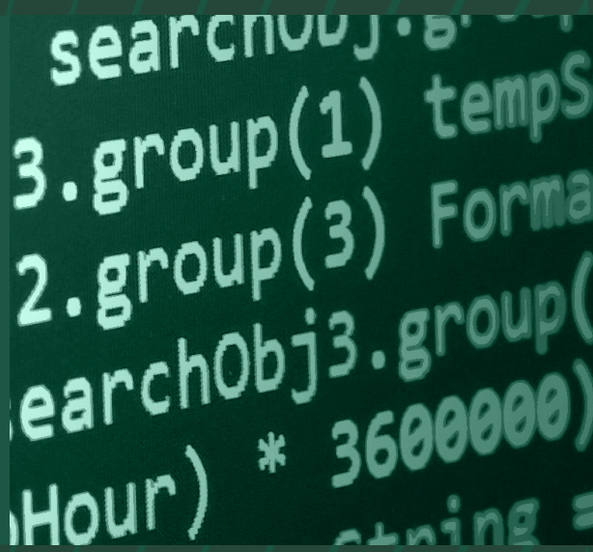
DELL Technologies

5 Recommandations pour survivre à une attaque par ransomware



1	2	3	4	5
Mettre en œuvre un plan de réponse aux incidents complet	**Mettre en place une stratégie de communication claire**	**Mettre en place une solution robuste de protection des données**	**Ne vous attendez pas à un retour immédiat à la normale**	**Mettre l'accent sur la formation et la sensibilisation**
Se concentrer sur la limitation de l'impact des attaques	Créer des modèles de communication en amont	Mettre les données sensibles en sécurité dans un coffre-fort de données isolé et immuable	Le paiement de la rançon doit intervenir en dernier recours	Effectuer des simulations d'attaque
S'entraîner, effectuer des tests et réaliser des mises à jour régulièrement	Communiquer de manière claire et opportune au sein de l'entreprise	Hiérarchiser la récupération par service/infrastructure	Vérifier la conformité aux exigences légales et réglementaires avant de payer	Encadrer et évaluer l'application des bonnes habitudes en matière de sécurité des employés
Constituer en amont une équipe de réponse aux incidents	Se préparer à communiquer avec l'extérieur, le cas échéant	Effectuer des exercices de récupération de ressources	Aucune garantie que le hacker vous restituera vos données même si vous payez la rançon	Utiliser des outils tels que les tests de phishing et la sensibilisation à la sécurité de la messagerie
Intégrer la cyberassurance à votre stratégie de résilience globale	Respecter les réglementations applicables en matière de notification	Ajouter des fonctionnalités telles que la « salle blanche » à votre objectif de temps de reprise (RTO)		
Inclure des plans de collaboration avec les forces de l'ordre		Vérifier l'intégrité des données récupérables		

Aujourd’hui, la question n’est plus de savoir si une entreprise sera victime d’un ransomware, mais quand elle le sera.

Les entreprises doivent planifier leur réponse à une attaque future qui aura su déjouer leur protection actuelle. Pour savoir ce qu’il faut faire en cas de sinistre, Jim Shook, Global Director of Cybersecurity and Compliance Practice, et Steven Granat, Principal Consultant, Cybersecurity Solutions and Strategic Partnerships, se sont entretenus avec Brian White, Senior Consultant, Product Marketing, Dell Data Protection.

> Vous devez impliquer les bonnes personnes, effectuer des exercices et simuler des actions pour que tout le monde sache immédiatement ce qu’il doit faire en cas d’attaque. »
>
> ***Steven Granat**, Principal Consultant, Cybersecurity Solutions and Strategic Partnerships, Dell Technologies*

Mettre en œuvre un plan de réponse aux incidents complet

Lorsqu’une attaque se produit, toutes les parties prenantes clés, soit la quasi-totalité des membres de l’entreprise et les tiers comme les fournisseurs, doivent savoir quoi faire. « Un plan de réponse aux incidents doit être rédigé et décrire une séquence d’actions claire », conseille M. Shook. Un plan complet présentera les étapes techniques, opérationnelles et de communication, de la réponse immédiate jusqu’au rétablissement complet de l’activité. Veillez également à conserver un document papier écrit, car les modes de communication numériques peuvent ne pas être opérationnels. « Il est essentiel de disposer d’un plan que l’on peut facilement retrouver sur une étagère », précise M. Granat.

Mettre en place une stratégie de communication claire

La plupart des entreprises devront communiquer avec les principales parties prenantes et, dans de nombreux cas, se conformer aux exigences réglementaires. Créez différents modèles pour les communications internes et externes, en fournissant des instructions systématiques sur qui doit être informé, dans quel ordre et à quel moment. Anticipez une panne des systèmes de téléphonie et de messagerie.

Mettre en place une stratégie solide de protection des données

L’un des principaux objectifs pour résister à une attaque par ransomware est de restaurer les données et de les récupérer aussi facilement que possible, tout en évitant de payer la rançon. Une stratégie solide de protection des données est un élément clé pour parvenir à ces résultats, mais elle devra englober à la fois la technologie et les processus. « Utilisez des données immuables et des coffres-forts électroniques pour stocker suffisamment de données de confiance ou qui peuvent au moins servir de points de validation qui vous permettront de récupérer les systèmes », conseille M. Shook. Assurer la protection des données est la première étape. Vous devez également constituer l’équipe et établir les processus nécessaires pour les récupérer. Des experts tiers peuvent vous aider, mais ils doivent intervenir dès le stade de la planification.

Ne vous attendez pas à un retour immédiat à la normale, même si vous payez la rançon

Le paiement d’une rançon, qui ne doit être envisagé qu’en dernier recours, ne garantit pas que tout revienne immédiatement à la normale. N’oubliez pas que vous négociez avec un criminel, et même si vous obtenez les clés pour décoder les données, il faut mettre en place une stratégie pour les données récemment récupérées. Pour commencer, vous devez tester les données déchiffrées et reconstruire tous les systèmes méthodiquement. Le fait de répéter avec attention différents scénarios avant même qu’une attaque ne se produise permettra d’atteindre une résilience optimale. « Il est essentiel de comprendre les différentes applications et dépendances de votre infrastructure technique pour un retour efficace à un état stable. Est-ce que je dispose d’une source de restauration viable et d’une cible récupérable ? Est-ce que je dispose de données exemptes de toute corruption ? Il s’agit là de considérations importantes », explique M. Granat.

Lors de la phase de récupération, vous devez également vous assurer que le hacker a réellement quitté vos systèmes. « Vous devez vérifier que l’incendie est éteint et découvrir ce qui a déclenché ce feu, car sans ces deux informations essentielles, vous êtes vulnérable aux attaques futures », explique M. Shook.

La formation et la pratique sont essentielles

La résilience numérique passe en grande partie par une formation complète et approfondie, allant de l’application des bonnes habitudes de sécurité dans les équipes à la mise en pratique régulière du plan de reprise d’urgence. « Il est essentiel d’impliquer les bonnes personnes, d’effectuer des exercices et de simuler des actions pour que tout le monde sache immédiatement ce qu’il doit faire en cas d’attaque », explique M. Shook.

Les ransomwares font partie du paysage actuel des menaces. Heureusement, grâce à la planification et à l’application de mesures de protection, vous pouvez en minimiser l’impact sur les plans opérationnel, financier et de la réputation. L’objectif est de revenir à la normale aussi rapidement et aisément que possible.

Découvrez comment relever certains des défis actuels majeurs en matière de cybersécurité sur **dell.com/cybersecuritymonth**

DELL Technologies