KDDI France

LIVRE BLANC

COFFRE ANTI RANSOMWARES

Protégez vos sauvegardes dès aujourd'hui contre les ransomwares

www.fr.kddi.com

KDDI France

EDITO

PME, hôpitaux, mairies… Rien qu'en France, les attaques par ransomware se multiplient, faisant de ce type d'attaque l'une des menaces les plus redoutées en cybersécurité. En octobre 2024, Free a été victime d'une cyberattaque majeure ayant compromis les données personnelles de 19 millions d'abonnés, mettant en évidence des failles de sécurité internes et soulignant les risques grandissants liés aux intrusions numériques.

En 2023, les attaques par ransomware ont ainsi ciblé plus de 93 % des sauvegardes des entreprises selon Veeam, révélant une fragilité inquiétante des systèmes traditionnels. L'impact de ces attaques ne se limite pas au paiement des rançons – dont le coût moyen s'élève à 250 000 euros – mais entraîne aussi des perturbations opérationnelles et une atteinte considérable à la réputation des organisations quant à son manque de protection des données.

Or les entreprises peinent à répondre à ces menaces, les solutions de sauvegarde classiques s'avérant insuffisantes ou mal anticipées. Sans compter que le coût économique annuel des ransomwares a été estimé à 20 milliards d'euros, une somme qui reflète autant les rançons versées que les pertes liées aux interruptions d'activité..

Les sauvegardes, qui devraient constituer une barrière essentielle contre les ransomwares, sont elles-mêmes devenues des cibles privilégiées. Ce constat appelle à une refonte complète des stratégies de protection des données.

Agir de manière proactive est indispensable pour garantir la résilience des entreprises face à cette menace exponentielle. Ce livre blanc vous apporte des solutions concrètes, notamment le coffre anti-ransomware, qui permet de pallier les limites des sauvegardes traditionnelles et de mieux se prémunir contre ces attaques

COMPRENDRE LA MENACE DES RANSOMWARES

Pour comprendre l'ampleur du danger que représentent les ransomwares, il est essentiel d'en décrypter le fonctionnement.

Un ransomware suit un cycle de vie bien défini :

- **L'intrusion dans le système d'information** se fait par le biais de techniques d'hameçonnage ou de l'exploitation de vulnérabilités logicielles.
- **La phase de commande et de contrôle** permet aux attaquants de prendre le contrôle à distance du système compromis.
- Ensuite, ils effectuent **une découverte et un mouvement latéral** pour explorer le réseau et localiser d'autres systèmes vulnérables.
- **Le vol et le chiffrement des données** rendent les fichiers inaccessibles sans le paiement de la rançon.
- Les cybercriminels exigent **une rançon e**n échange de la clé de déchiffrement.
- Enfin, **la récupération ou la résolution** se fait soit après le paiement, soit via des sauvegardes sécurisées, évitant ainsi la dépendance au paiement de la rançon.

LES MÉTHODES LES PLUS COURANTES

Les ransomwares exploitent diverses méthodes d'infection, s'appuyant sur les failles humaines, techniques ou organisationnelles pour s'introduire dans les systèmes informatiques. Parmi les méthodes les plus répandues, trois se distinguent particulièrement : les courriels malveillants, les sites Web compromis et les accès non sécurisés aux système.

1 Les courriels malveillants : **la méthode reine**

Les courriels malveillants, ou phishing, représentent la porte d'entrée la plus fréquente pour les ransomwares. Ces messages aux airs légitimes contiennent des pièces jointes infectées ou des liens renvoyant vers des fichiers ou sites piégés. Exemple classique : un salarié reçoit un courriel prétendument envoyé par un partenaire commercial, avec une facture ou un document urgent à télécharger. En ouvrant ce fichier, il déclenche le téléchargement et l'exécution du ransomware. La sophistication de ces attaques ne cesse de croître. Certaines campagnes de phishing utilisent ainsi des techniques d'ingénierie sociale pour personnaliser les messages au maximum et augmenter leurs chances de succès. Pour cela, les cybercriminels analysent tout simplement les données disponibles en accès libre sur les réseaux sociaux ou les fuites de données pour identifier les destinataires, rendant leurs attaques particulièrement ciblées et retorses.

KDDI France

2

Les sites Web compromis : **des pièges invisibles**

Les ransomwares se propagent aussi via des sites Web compromis ou des publicités malveillantes (malvertising). Lorsqu'un utilisateur visite un site légitime mais piraté, des scripts malveillants s'exécutent en arrière-plan pour exploiter les vulnérabilités de son navigateur ou des plugins installés, tels qu'Adobe Flash ou Java. Cette méthode est appelée drive-by download. Ces attaques sont particulièrement insidieuses car elles ne nécessitent aucune action volontaire de la victime, hormis la visite du site. Un collaborateur peut être redirigé vers un site compromis après avoir cliqué sur un lien présent dans un courriel ou sur une publicité en ligne. Dès que le ransomware est entré dans le réseau, le cybercriminel chiffre les données de l'utilisateur sans que celui-ci ne se rende immédiatement compte de l'infection

3

Les accès non sécurisés : **un point d'entrée direct**

Enfin, les accès non sécurisés constituent une méthode privilégiée pour les cybercriminels, en particulier dans le cadre des attaques ciblées. Les ransomwares exploitent des ports ouverts ou des mots de passe faibles pour pénétrer directement dans les systèmes informatiques. Les outils comme Remote Desktop Protocol (RDP), utilisé pour le télétravail, sont une cible fréquente. Dans cette optique, les attaquants utilisent des techniques de brute force (essais systématiques de mots de passe) ou des informations volées lors de violations de données pour s'authentifier. Un exemple courant est l'exploitation d'un compte administrateur mal sécurisé. Une fois que les cybercriminels ont obtenu l'accès, ils peuvent désactiver les logiciels de sécurité, propager le ransomware sur l'ensemble du réseau et cibler spécifiquement les sauvegardes

UN POINT COMMUN : LES RANSOMWARES EXPLOITENT L'ERREUR !

Ces méthodes d'infection partagent un point commun : elles exploitent des erreurs humaines ou organisationnelles. Un clic imprudent, une mise à jour logicielle manquée ou un mot de passe faible suffisent à ouvrir la porte aux ransomwares. D'où l'importance de mêler technologies de protection avancées et sensibilisation des équipes, pour réduire les risques.

En 2023, 72 % des ransomwares visaient directement les sauvegardes, soulignant l'importance pour les entreprises de sécuriser non seulement leurs données actives, mais aussi leurs copies de sauvegarde. Ces attaques exploitent les failles des systèmes existants, souvent mal configurés ou trop accessibles.

Dans ce contexte, la nécessité de comprendre la dynamique des ransomwares ne relève pas uniquement de la gestion de crise. Cela implique aussi de mieux anticiper leurs actions, afin de développer des systèmes robustes et de réduire les pertes éventuelles.

LES LIMITES DES SAUVEGARDES CLASSIQUES

Les solutions de sauvegarde traditionnelles, bien qu'indispensables, présentent des faiblesses face à la montée en puissance des ransomwares. Prenons l'exemple des sauvegardes locales : elles sont vulnérables aux attaques directes si elles ne sont pas isolées du réseau principal. Quant aux sauvegardes hors site ou dans le cloud, elles dépendent de configurations parfois complexes et peuvent être compromises par des erreurs humaines ou des failles de sécurité. Toutes PME, de la plus petite à la plus grande, peut dès lors voir ses sauvegardes cloud être chiffrées par un ransomware en raison d'un accès administrateur mal sécurisé. De quoi perdre plusieurs semaines de données, entraînant un ralentissement significatif de ses activités et des pertes financières importantes. La plupart des entreprises touchées par des ransomwares ont pourtant des sauvegardes en place, mais celles-ci sont aussi compromises. Ce constat met en lumière l'importance de solutions plus avancées pour résister aux cyberattaques.

QU'EST-CE QU'UN COFFRE ANTI-RANSOMWARE ?

Le coffre anti-ransomware représente une avancée majeure dans la protection des données d'entreprise. Pensé comme une solution de dernière ligne de défense, il combine des technologies de :

Segmentation réseau
Air gap
Immuabilité des données
Détection des anomalies

Contrairement aux sauvegardes classiques, ce coffre est isolé des environnements opérationnels, ce qui le rend inaccessible aux ransomwares. En pratique, un coffre anti-ransomware fonctionne en verrouillant les copies de sauvegarde dans un environnement sécurisé, souvent hors ligne. Cette isolation garantit que les données restent intactes, même en cas de compromission du réseau principal. De plus, des systèmes de détection automatisés permettent d'identifier rapidement toute tentative d'intrusion, facilitant ainsi une réponse rapide.

Pour les directeurs des systèmes d'information (DSI), cette solution permet :

Une récupération des données en cas d'attaque
Une résilience pérenne
Un retour sur investissement démontré

L'IMPORTANCE D'AGIR EN AMONT

Pour se prémunir efficacement contre les ransomwares, il est essentiel d'intégrer des outils spécialisés, comme le coffre anti-ransomware, tout en renforçant la sensibilisation des équipes. Cette approche repose sur des étapes concrètes. Ces mesures, soutenues par des technologies avancées, permettent de construire une défense robuste et de mieux gérer des menaces de plus en plus sophistiquées.

1. Isoler les sauvegardes critiques dans un coffre.
2. Configurer les accès avec des droits limités
3. Tester régulièrement les plans de récupération.
4. Mettre en œuvre des systèmes de détection automatisés.
5. Sensibiliser les équipes au rôle qu'elles jouent dans la protection des données.

UN EXEMPLE CONCRET DES BÉNÉFICES DU COFFRE-FORT

Une organisation publique régionale de 1 500 salariés, desservant 200 000 citoyens avec un budget annuel de 500 millions de dollars, était confrontée à des enjeux croissants en matière de cybersécurité, notamment face aux attaques par ransomware. Malgré des systèmes de sauvegarde traditionnels en place, ces derniers ne garantissaient pas une protection suffisante. Les sauvegardes, bien que coûteuses, restaient vulnérables aux cyberattaques, entraînant des risques significatifs de pertes de données et de temps d'arrêt prolongés.

Pour y remédier, l'organisation a déployé Dell PowerProtect Cyber Recovery. Ce système déploie un coffre-fort de récupération isolé permettant de créer des sauvegardes immuables.

En cas d'attaque, les données critiques sont restaurées rapidement, même si les sauvegardes standards sont compromises. La solution intègre également CyberSense, un outil de détection avancée qui analyse les sauvegardes pour repérer d'éventuelles corruptions ou infiltrations, ajoutant une couche supplémentaire de protection.

53% DE ROI

Selon une étude menée par Forrester Consulting

EN CONCLUSION ...

Face à la menace croissante des ransomwares, les entreprises n'ont d'autre choix que de revoir en profondeur leur stratégie de cybersécurité. La priorité n'est plus de simplement réagir aux attaques, mais de s'armer pour mieux les anticiper et en limiter les impacts. L'adoption d'un coffre anti-ransomware s'inscrit dans cette logique. Ce n'est pas seulement une réponse immédiate aux attaques, mais une mesure qui renforce durablement la résilience et la continuité d'activité. En combinant cet outil avec une sensibilisation des équipes et une surveillance régulière des systèmes, les organisations se donnent les moyens de protéger leurs données, leur activité et leur image. Il s'agit d'un investissement stratégique qui dépasse la simple protection technique : il témoigne d'un engagement envers la sécurité et la confiance des parties prenantes. En intégrant ces solutions, les entreprises posent les bases d'une démarche d'anticipation pérenne face à un paysage numérique de plus en plus incertain.