mti
A RICOH Company

Cyberattaques

Enjeux et solutions

Prévenir
les attaques

Limiter
la propagation

Protéger
ses données

Redémarrer
son activité

DELL Technologies
TITANIUM PARTNER

vmware®

1 PRÉVENIR LES ATTAQUES

Votre environnement est faillible, remédiez-y !

2 LIMITER LA PROPAGATION

Réduire la surface d'attaque

3 PROTÉGER SES DONNÉES

Votre survie passe par la sauvegarde orientée restauration

ET APRÈS ?

En cas d'attaque, réussir à redémarrer son activité le plus rapidement et le plus efficacement possible

EDITO

La sécurité au cœur de notre métier

Aujourd'hui, la sécurité est une composante indispensable et indissociable de l'infrastructure. Les infrastructures informatiques constituent le cœur d'expertise de MTI depuis plus de 30 ans, les problématiques liées à la sécurité font donc logiquement et intégralement partie de nos défis quotidiens.

Parce que la sécurité est bel et bien inscrite dans notre ADN, nous connaissons finement les enjeux associés. Ainsi, nous avons bien conscience que, même en adoptant les meilleures stratégies de défense, le risque zéro n'existe pas. Ce constat objectif et lucide est capital pour mettre au point une stratégie de sécurité pertinente dans l'entreprise.

Aucune solution ne permet d'éviter les attaques

Dans ce cadre, notre mission tient à retarder les attaques et limiter leur impact, mais également, à garantir la continuité d'activité des entreprises en proposant des solutions pour rétablir une situation de production le plus rapidement possible.

Ce livre blanc explore les axes à suivre dans une stratégie de défense, de remédiation des incidences d'une attaque, et de reprise solide de l'activité.

Bonne lecture !

Didier Pichon, Vice-Président des Ventes chez MTI France

La force de frappe des ransomwares

Les ransomwares représentent l'une des formes de cybercriminalité les plus répandues et les plus coûteuses. Selon l'ANSSI, ces attaques ont augmenté de 255 % entre 2019 et 2020 et font l'objet d'une véritable industrialisation par des attaquants très organisés[1]. Loin de tout amateurisme, l'activité des ransomwares repose sur de véritables business models rentables et très bien rodés, selon trois principales tactiques :

Le *RaaS*

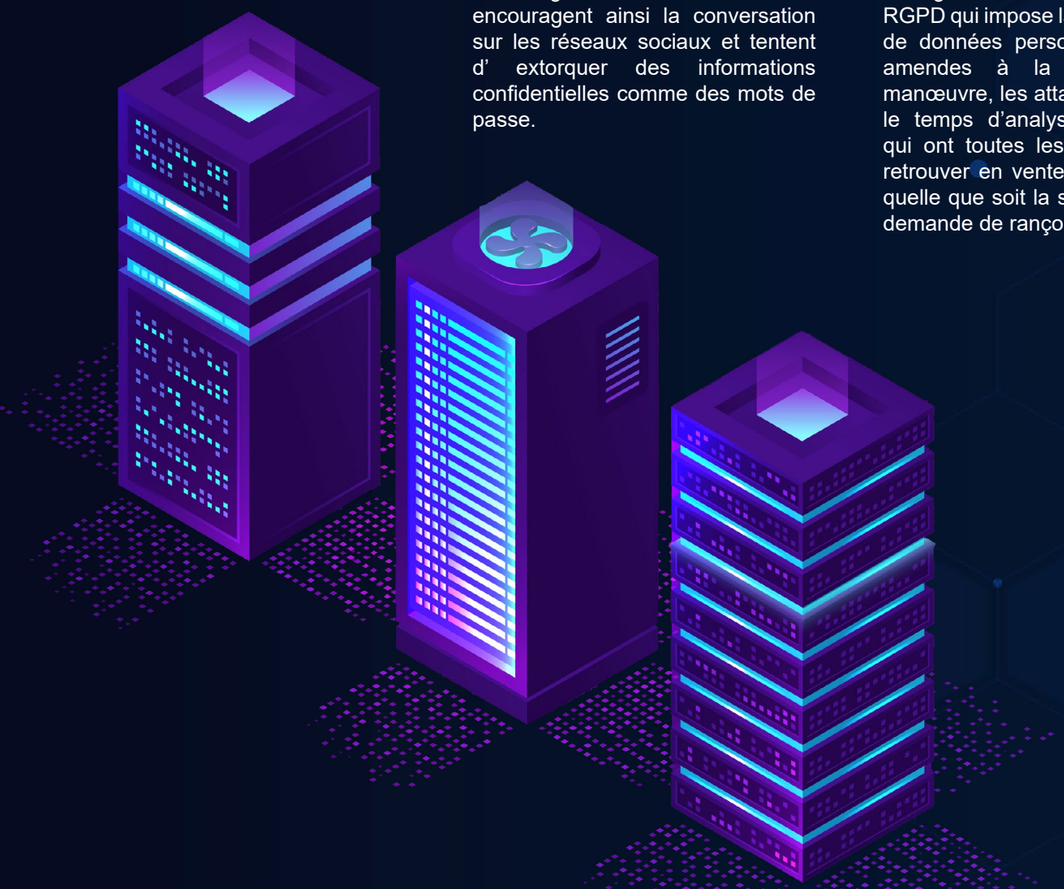
Le Ransomware-as-a-Service permet d'accéder sur le darkweb à des ransomwares prêts à l'emploi, service de "diffusion" et support post-attaque inclus.

Le *Big Game Hunting*

Il s'agit d'une attaque de cibles précises, grandes entreprises ou institutions identifiées comme capables de payer de grosses sommes d'argent. Les hackers mettent au point des ransomwares dédiés et peuvent, entre autres, pratiquer le social engineering auprès de personnes clés dans les organisations ciblées. Ils encouragent ainsi la conversation sur les réseaux sociaux et tentent d' extorquer des informations confidentielles comme des mots de passe.

La double extorsion

Il s'agit du format le plus ancien. Cette attaque commence par l'infiltration du système d'information de la cible, puis le chiffrement et l'exfiltration de ses données. Les attaquants brandissent ensuite la menace d'une divulgation des données que seul le paiement d'une rançon sous 72 heures annulera - un argument choc dans le cadre du RGPD qui impose la non-divulgation de données personnelles, lourdes amendes à la clé. Dans la manœuvre, les attaquants prennent le temps d'analyser les données qui ont toutes les chances de se retrouver en vente sur le darkweb, quelle que soit la suite donnée à la demande de rançon.



Les conséquences et les coûts mettent en péril les activités

Plus de 650 millions d'euros

Le montant des demandes d'extorsion par des groupes de cybercriminels auprès de 4 millions de victimes en quatre ans (2016 – 2020), montant recensé (mais non payé) dans le cadre de l'initiative No More Ransom d'Europol.

60%

C'est la proportion de PME et TPE qui mettent la clé sous la porte dans les six mois suivant une attaque, d'après plusieurs observateurs.

Moins de 10%

Après une cyberattaque, c'est ce que représente la gestion immédiate des premiers dommages par rapport aux dommages totaux : selon une étude récente Deloitte, les répercussions se mesureraient souvent sur plusieurs mois ou années. Au-delà des coûts directs, les coûts cachés sont plus rarement rendus publics : dévalorisation de la marque, perte de propriété intellectuelle, augmentation des primes d'assurances, procédures juridiques...

Facteur de risque supplémentaire : le télétravail

En déportant les données de l'entreprise au domicile des employés, le télétravail ouvre la brèche de réseaux domestiques moins solidement sécurisés que les réseaux professionnels. Les hackers ont été prompts à imaginer de nouveaux scénarios d'attaques tirant profit de ce contexte. Ils sont notamment à l'affût de profils d'administrateurs réseaux à approcher sur les réseaux sociaux. Ils cherchent ainsi à dénicher l'adresse de leur domicile et de leur messagerie personnelle en pratiquant le social engineering. Ensuite, s'infiltrer dans le réseau de l'entreprise via leur box Internet personnelle piratée est un jeu d'enfant.

Personne n'est à l'abri

Tous les secteurs sont touchés, même si certains se retrouvent davantage dans la ligne de mire des pirates à l'heure actuelle. C'est le cas des acteurs de l'éducation, des services numériques, des collectivités locales et des acteurs du secteur de la santé - en témoignent de nombreuses attaques d'hôpitaux en France depuis le début de l'année 2021 et la cyberattaque en décembre 2020 de l'EMA, agence médicale de l'Union européenne, ciblant des données sur les vaccins anti-Covid 19.

Selon le 6e baromètre du CESIN (Club des Experts de la Sécurité de l'Information et du Numérique), les organisations de toute taille sont concernées, puisque 30 % des entreprises victimes comptent plus de 5 000 employés, ce qui laisse la part belle aux plus petites structures[2].

Aujourd'hui, les ransomwares sont devenus inéluctables. C'est pourquoi se protéger ne suffit plus, il faut savoir se relever en cas d'attaque. L'entreprise doit absolument élaborer un plan pour rétablir ses opérations dans le sillage d'un ransomware. Il en va de sa survie.

[1] Etat de la menace rançongiciel à l'encontre des entreprises et institutions, ANSSI (Autorité Nationale en matière de Sécurité et de défense des Systèmes d'Information), 2021

[2] 6e édition du baromètre annuel du Cesin (le Club des Experts de la Sécurité de l'Information et du Numérique) réalisé par Opinion Way, 2021

1 PRÉVENIR LES ATTAQUES

Votre environnement est faillible, remédiez-y !

Première étape pour survivre aux ransomwares : limiter leurs points d'entrée

Tout ce qui est en production est une cible, stockage secondaire y compris. Si aucune protection infaillible n'est réaliste, il reste évidemment utile de limiter les risques.

D'où l'intérêt de faire un état des lieux de l'existant pour identifier les failles de sécurité et y remédier.

Ce "bilan de santé" de la sécurité informatique a tout intérêt à combiner un audit de l'environnement pour une vue d'ensemble et des tests d'intrusion (Pentest) pour vérifier de façon plus ciblée la résistance d'un composant à une attaque.

L'audit de sécurité

Il passe en revue l'infrastructure, dont les applications, les technologies déployées, leurs configurations. Concrètement, il nécessite d'y dédier un compte utilisateur depuis lequel accéder aux différents serveurs, pendant une période définie. Il implique de bien définir l'envergure, en particulier dans les entreprises multisites qui peuvent auditer tout ou partie de leurs sites.

Le Pentest

Il permet de cibler des composants de l'infrastructure pour vérifier leur robustesse. Il se déroule en quatre étapes : analyse de l'infrastructure, de l'application et/ou de la technologie, identification des failles, exploitation des vulnérabilités et analyse de l'impact dans l'organisation. Il y a un réel intérêt à réitérer régulièrement ce type de test pour vérifier la robustesse des solutions de remédiation déployées, et pour identifier l'émergence de nouvelles failles.

Ce bilan sert à identifier les failles et les risques, à réduire la probabilité de réussite des attaques, mais il contribue aussi à la conformité – notamment, certifications type ISO 27001 et PCI DSS – et à rassurer les parties prenantes de l'entreprise.

La démarche est d'autant plus pertinente que les failles de sécurité ne cessent de se multiplier : selon les derniers signalements de vulnérabilité recensés, les rapports d'erreurs de configuration ont explosé en 2020 avec une croissance de 310 %[3]. Parmi les raisons de cette envolée figurent souvent des migrations accélérées vers le cloud, provoquées par la pandémie. Par ailleurs, les problématiques d'accès restent majeures du fait de contrôles d'accès inappropriés, d'authentifications mal gérées ou d'escalade des privilèges au cœur des vulnérabilités. Colmater les brèches devient donc une priorité.

[3] *The 2021 Hacker Report, Hackerone, 2021*

Un audit avec Pentest sert à agir pour remédier !

Cet état des lieux de la sécurité informatique donne lieu à un rapport, socle de la prise de décision pour la remédiation. En effet, les résultats recensent les vulnérabilités repérées, mais aussi leur niveau de gravité, et les accompagnent de recommandations concrètes pour parer aux problèmes. L'entreprise peut donc, a minima, traiter les failles les plus importantes : logiciels et systèmes d'exploitation obsolètes, configurations inadéquates, ou encore comportements humains à risques.

CONFIGURATIONS : le point faible le plus courant

L'audit avec Pentest permet d'optimiser les diverses configurations identifiées comme lacunaires. En effet, la plupart des failles tiennent à une mauvaise configuration des technologies, ou plus exactement à une configuration orientée usage, mais pas sécurité. Par exemple, des droits d'accès trop vastes, pour trop de monde, permettent certes beaucoup de fluidité dans les opérations, mais ouvrent une vaste brèche quand les identifiants d'un utilisateur sont récupérés par des hackers. La reconfiguration de l'existant qui suit l'audit permet de fermer ce genre de porte aux ransomwares.

UTILISATEURS : l'éternel maillon faible humain…

Il arrive, en phase d'audit, de retrouver les mots de passe d'utilisateurs à disposition sur le darkweb : preuve que l'entreprise a déjà été attaquée, sans forcément l'avoir identifié !
À la source du problème, les réflexes et les comportements des utilisateurs face aux risques de sécurité. Moins ils sont informés, plus ils sont des cibles faciles. La remédiation consiste à mieux informer les utilisateurs, par exemple sur la bonne gestion des mots de passe ou sur les pratiques d'influence sur les réseaux sociaux via le social engineering. Dans ce cas de figure, un Pentest ultérieur permet de vérifier que de bons réflexes ont été acquis.

Audit & Pentest ciblés ransomwares

Un état des lieux propre aux ransomwares permet de vérifier la pertinence de l'existant face à cette menace en particulier, notamment les plans de réponse aux incidents et d'investigation (forensic) en cas d'attaque, les diverses protections déployées (filtrage de trafic, web, mail et solutions anti-malware, pare-feux), la supervision du réseau type SIEM (Security Event Information Management), les configurations VPN, la gestion des accès et de l'authentification, la conformité aux frameworks de référence.

Une attaque simulée de ransomware permet de mesurer la résistance du système. Celle-ci tient compte des diverses techniques d'attaque existantes - hameçonnage, approche Red Team, par ingénierie sociale, attaques sans fil, compromission des hôtes et services exposés à Internet, entre autres. Le bilan donne une vue très précise des défenses qui fonctionnent, comme des failles dues à des configurations erronées, les écarts et les omissions dans la ligne de défense. Autant de fronts sur lesquels passer à l'action de remédiation.

La remédiation va consister à assurer que l'entreprise est dotée d'un ensemble de contrôles correctement déployés et configurés, comprenant :

- Règles et processus de sécurité
- Contrôles et défenses techniques
- Supervision du réseau
- Plans et actions de réponse
- Alertes et notifications
- Contrôles d'accès et d'authentification
- Police de cyber assurance

2 LIMITER LA PROPAGATION

Réduire la surface d'attaque

La meilleure stratégie contre les ransomwares prend en compte le fait qu'une attaque peut toujours atteindre le réseau. Et ce, même si la probabilité d'attaque diminue drastiquement une fois que les brèches identifiées ont été refermées. Ainsi, l'entreprise doit garder un coup d'avance et "attendre" les hackers qui y pénètrent malgré tout, en y installant des entraves qui limitent leur action et la propagation des codes malveillants. Ce niveau de protection se déploie de façon transversale dans le réseau.

TACTIQUES D'ATTAQUES SELON MITRE ATT&CK[4] :

ACCÈS INITIAL	Tentative d'entrée dans le réseau
EXÉCUTION	Amorçage d'un code malicieux
ANCRAGE	Implantation dans le système
ESCALADE DE PRIVILÈGES	Accès à des autorisations de niveau supérieur
CONTOURNEMENT DES DÉFENSES	Esquive des systèmes de détection
ACCÈS AUX INFORMATIONS D'IDENTIFICATION	Vol de noms de comptes et mots de passe
ANALYSE DE L'ENVIRONNEMENT	Exploration du système et du réseau interne
MOUVEMENT LATÉRAL	Contrôle de systèmes distants
COLLECTE	Recueil des données utiles
CONTRÔLE	Communication avec les systèmes compromis
EXFILTRATION	Vol de données
IMPACT	Manipulation, interruption ou destruction des systèmes et données

[4] Techniques catégorisées par le MITRE ATT&CK, "Adversarial Tactics, Techniques, and Common Knowledge"

Limiter la propagation Nord/Sud, de l'extérieur vers l'intérieur

Pare-feux et antivirus restent des outils de protection essentiels pour limiter la circulation des attaques de l'extérieur vers l'intérieur du réseau. La nouvelle génération d'outils permet de renforcer cette sécurité périmétrique afin de réduire davantage la probabilité qu'une menace n'infecte le réseau.

Analyse comportementale

Les antivirus classiques surveillent les paquets du trafic entrant pour identifier des comportements symptomatiques des cybermenaces recensées, donc connues, dans leurs bases de données. Or, plus vite on repère une attaque, plus vite il est possible de réagir. Afin d'accélérer l'identification d'une attaque en cours, les antivirus nouvelle génération supervisent le trafic de façon plus granulaire, au niveau des terminaux des utilisateurs et des serveurs. Ils peuvent ainsi repérer davantage de scénarios anormaux – l'effacement inhabituel de gros volumes de données, la modification de dates de plusieurs fichiers existants au jour même, ou un processus d'élévation de droits administrateur, par exemple. Dans sa fonction d'IDS (Intrusion Detection System), l'antivirus va être en mesure de donner l'alerte immédiatement aux administrateurs.

Identifier, mais aussi bloquer

Désormais, les outils d'IDS peuvent aussi devenir des IPS (Intrusion Prevention Systems). Ils réagissent à l'identification d'une menace en rejetant de façon proactive les paquets de réseau suspects pour les placer en quarantaine. L'IPS automatise ainsi le blocage des menaces, là où l'IDS requiert une intervention humaine une fois l'alerte donnée. Que l'entreprise utilise des IDS ou des IPS, elle doit veiller à ce que les bases de données des menaces connues de ses outils fassent l'objet d'une mise à jour sans faille.

Limiter la propagation Est/Ouest, à l'intérieur du réseau

Une menace a réussi à s'infiltrer dans le réseau malgré toutes les protections en place ? Qu'à cela ne tienne, l'entreprise a d'autres cartes en main pour bloquer sa propagation transversale dans le réseau.

Micro-segmentation du réseau

La micro-segmentation isole les différents environnements au sein du réseau et positionne un pare-feu sur chaque serveur (virtuel ou physique). S'applique alors une logique Zero Trust qui part du principe que rien n'est fiable, et que tout doit être contrôlé avant d'obtenir une autorisation. Dans la micro-segmentation du réseau, tous les flux de communication entre ports des serveurs sont d'office coupés, puis rouverts selon une liste blanche de flux nécessaires entre serveurs. Ainsi, les communications d'un serveur donné sont limitées à son seul usage, ce qui ferme la possibilité qu'un code malicieux ne se répande via ses ports légitimes.

Si un hacker s'attaque à un réseau micro-segmenté :

Il va en premier lieu effectuer une cartographie qui sera lacunaire, puisque la micro-segmentation l'empêche de voir tout le réseau. Il va donc opérer plus ou moins à l'aveugle. Une fois entré dans un segment du réseau, le hacker ne pourra pas exploiter les ports des serveurs pour diffuser son code malicieux, chaque port étant restreint aux seuls protocoles légitimes, sans accès au réseau entier. Enfin, dans le segment de réseau où il arrive, le code malicieux ne pourra pas faire d'énormes dégâts. L'analyse comportementale va rapidement détecter les anomalies déclenchées par son activité et donner l'alerte.

3 PROTÉGER SES DONNÉES

Votre survie passe par la sauvegarde orientée restauration

Puisqu'une attaque de ransomware a toutes les chances de toucher votre entreprise, la stratégie pour y survivre consiste à compliquer la tâche aux hackers quand ils passent à l'action, et à mettre précautionneusement de côté des jeux de données essentielles à l'activité et exploitables après l'attaque pour restaurer l'activité.

Cette stratégie d'entrave d'une part, de filets de sécurité d'autre part, se joue à différents niveaux pour récupérer les données critiques à des fins de restauration, quelle que soit la profondeur d'une attaque. Ainsi, elle s'applique de la donnée immédiatement générée en production (data primaire) à la donnée sauvegardée à plus ou moins long terme (data secondaire) et à la data sauvegardée hors site.

Data primaire

Au cœur de la production, la data primaire est l'une des plus sensibles, car en cas de perte, les incidences sont les plus lourdes financièrement, ainsi qu'en termes de temps de travail. Son stockage sur la baie de production permet de la récupérer rapidement, à un état antérieur récent, en cas de perte de données.

Data secondaire

Il s'agit d'une copie des données de production, sur un stockage différent. La data secondaire est destinée à une rétention à plus ou moins long terme, de quelques semaines à plusieurs années notamment pour répondre aux réglementations qui exigent des rétentions longues. La data secondaire sert de filet de sécurité si la donnée de production est irrémédiablement perdue. Pour renforcer sa disponibilité, la règle du 3-2-1 est une bonne pratique éprouvée : disposer de trois copies de vos données au moins ; stocker ces copies sur deux supports différents ; conserver une copie de la sauvegarde hors site.

Data hors site

Data secondaire également, la data hors site consiste en une copie supplémentaire à la première sauvegarde, située à un emplacement différent de la production et des autres supports de sauvegarde. Elle pose un filet de sécurité supplémentaire : si une attaque par ransomware compromet à la fois la data primaire et la data secondaire au premier niveau de sauvegarde, la data hors site reste disponible pour être réinjectée dans les opérations lors de la reprise d'activité.

À chaque type de données, la bonne façon de sauvegarder

À chaque niveau de données, la stratégie va anticiper les facteurs qui faciliteront une restauration en cas d'attaque : le RPO (Recovery Point Objective, soit l'état antérieur des données auquel l'entreprise peut tolérer de "reculer" pour restaurer l'activité) et de RTO (Recovery Time Objective, soit le délai acceptable pour reprendre l'activité après une attaque). RPO et RTO se définissent au cas par cas selon la nature des données, sachant que plus elles sont critiques, et leur restauration urgente pour relancer l'activité, plus elles ont besoin de RPO et RTO réduits.

Agir sur la data primaire : snapshots et CDP

Sur la baie de production, la stratégie consiste à stocker les données de travail en modification constante au cours des opérations. Le RPO visé est ici très réduit : il est possible de récupérer les données à un état antérieur très récent, de quelques minutes seulement, voire à la seconde près. Plusieurs solutions permettent une telle granularité :

Les snapshots :

Ces instantanés de stockage consistent à capturer une image des données à un instant T. Automatisés, ils interviennent à une fréquence prédéfinie par jour ou par heure. Ils permettent de récupérer une image des données à quelques minutes d'intervalle, sans arrêter la production, et peuvent aussi servir de base pour une sauvegarde sur disque ou sur bande. Ils sont aujourd'hui disponibles sur toutes les baies et s'avèrent simples à activer.

Protection Continue des Données (CDP) :

Pour une granularité plus fine que les snapshots, les solutions de CDP permettent aux blocs de données modifiés de se loguer au stockage à chaque opération d'entrée/sortie. Il est alors possible de revenir à un état antérieur des données à la seconde près.

Best practice face aux ransomwares

Les processus de protection de la donnée au niveau Hardware sont rarement identifiés par les scans qu'effectuent les attaquants avant de passer à l'action. Il est donc primordial de ne pas négliger ces technologies, qui, "oubliées" par les hackers, peuvent ainsi vous sauver la mise.

Etant donné qu'elles peuvent être gourmandes en espace disque, il convient de les paramétrer au mieux en trouvant le bon compromis entre RPO et volumétrie à provisionner. Il est nécessaire d'adapter la granularité du stockage de sauvegarde au temps disponible pour repérer une perte de données. En effet, le constat d'une attaque est rarement immédiat et plus la journée de travail avance, moins les équipes ont de latitude pour identifier un problème.

C'est pourquoi la bonne pratique tient à resserrer la granularité du stockage des données de production au fil de la journée, en commençant par des snapshots dont la fréquence peut augmenter graduellement, et en finissant avec une solution de CDP sur la dernière heure de travail.

Agir sur la data secondaire : WORM et analyse d'intégrité des données

Les copies de données sur les baies de sauvegarde font partie des cibles privilégiées des attaques. La parade consiste à la fois à ralentir les hackers, à l'image d'une porte blindée sur le chemin d'un cambrioleur, et à assurer que les données sont disponibles et saines pour repartir en production dans un scénario de reprise d'activité à la suite d'une attaque.

WORM – *Write Once, Read Many* :

Le WORM bloque toute nouvelle écriture sur un volume de données de sauvegarde et n'en permet plus que la seule lecture. Dans la mesure où les malwares effacent ou chiffrent les données, le blocage d'écriture par WORM est tout indiqué pour entraver les manœuvres des hackers : même si ces derniers réussissent à récupérer les mots de passe administrateurs, avec une baie utilisant le WORM en mode "Compliance", ils ne peuvent ni altérer, ni effacer les données contenues. Le WORM rend ainsi la sauvegarde inaltérable pendant un temps déterminé (de quelques heures à plusieurs années). Effectué sur disque, le WORM permet de plus une sauvegarde et une restauration rapides.

Analyse d'intégrité des données :

Il est essentiel de s'assurer que les données sauvegardées sont saines et ne contiennent aucun malware pour les utiliser dans une restauration viable de l'activité. Cette analyse est régulièrement mise à jour sur l'identification de nouveaux malwares et appliquée aux données de sauvegarde. Si un malware au sein des données de production est passé entre les mailles du filet au moment de leur copie sur le disque de sauvegarde, l'analyse d'intégrité permettra de l'identifier rapidement.

Best practice face aux ransomwares

WORM et analyse d'intégrité combinés préparent le terrain d'une reprise d'activité sans heurt. Toutefois, la sauvegarde pose la contrainte de maîtriser les volumes dans les espaces de stockage. Or, plus la période de rétention est longue, plus l'espace sur les baies de sauvegarde est monopolisé à long terme.

Il y a donc des choix à faire sur le type de sauvegarde en fonction du type de données – autrement dit, il ne s'agit pas de tout sauvegarder tout le temps derrière une porte blindée en mode WORM.

Aussi, le WORM qui bloque des volumes pendant plusieurs mois doit se destiner aux données les plus critiques pour l'activité, et à celles dont la reconstruction représente la plus lourde charge : messagerie, "filers" et bases de données. D'où l'importance de passer ces données par le filtre de l'analyse d'intégrité pour disposer de données "wormisées" parfaitement saines.

En cas d'attaque, le duo WORM et analyse d'intégrité donne la garantie d'alimenter la reprise d'activité avec les données essentielles, récentes et fiables.

Agir sur la data hors site : installer un Air gap

La sauvegarde hors site met en œuvre un support additionnel pour y répliquer la copie des données sauvegardées, en un autre lieu, sur un autre réseau – et "wormiser" les données critiques à ce niveau également. Le "hors site" s'entend physiquement : un emplacement différent dans le cloud, chez un hébergeur, sur bandes stockées à un endroit différent de la production. Il peut également être virtuel, grâce à des solutions d'"invisibilisation" des bandes qui restent sur place, mais sortent du radar de la sauvegarde, donc des hackers qui s'y introduiraient.

Toutefois, pour répliquer les données à fréquence régulière, la sauvegarde hors site et la sauvegarde primaire communiquent par ports de réplication, qui bien souvent restent ouverts pour permettre une réplication au fil de l'eau. Pour renforcer la protection des données répliquées, ultime recours de restauration en cas d'attaque profonde dans le système d'information, il convient de fermer complètement leurs accès.

Air gap :

Sur le principe du coffre-fort, l'air gap consiste à mettre les données répliquées hors site dans un environnement complètement hermétique ("vault"). Des solutions permettent ainsi d'ajouter une couche de protection sur les disques de réplication et d'ouvrir les ports de communication uniquement au moment de répliquer les données de sauvegarde. En dehors de ces opérations, les ports sont automatiquement refermés. Dans les secteurs les plus sensibles – banque, défense par exemple – les baies comprenant les disques de réplication hors site avec air gap peuvent bénéficier en plus d'une protection physique, par porte blindée, accès par codes, ou autre dispositif de sécurité.

Best practice face aux ransomwares

l'avis d'expert de Dell Technologies

« Pour augmenter leur résilience face aux cyberattaques, qu'elles soient fomentées de l'extérieur par l'inoculation de malware ou de l'intérieur du firewall par un "insider", nous recommandons aux entreprises de sanctuariser leurs données vitales dans un "vault" :

- Isolé des réseaux de production par un "air gap" et physiquement sécurisé et interdit d'accès aux utilisateurs sans autorisation appropriée ;
- Alimenté périodiquement, via l'orchestration automatique de l'air gap, en données qui seront sécurisées dans un stockage immuable ;
- Mettant en œuvre l'analyse systématique de son contenu afin d'identifier la dernière occurrence des données exempte de toute corruption ;
- Disposant de moyens autonomes de restauration de la dernière bonne copie des données identifiée, permettant de s'affranchir de l'infrastructure de restauration opérationnelle pouvant être rendue inopérante par l'attaque. »

François-Christophe JEAN, CTO Data Protection Solutions France, Dell Technologies

Différents niveaux de protection :

PROTECTION NORD / SUD :
SÉCURITÉ PÉRIMÉTRIQUE

PROTECTION EST / OUEST :
MICROSEGMENTATION

PROTECTION DES DONNÉES :

1	2	3	4	5	6
RÉPLICATION	SNAPSHOT CDP	BACKUP WORM	DISASTER RECOVERY	AIR GAP	ANALYSE

ET APRÈS ?

En cas d'attaque, un plan est nécessaire pour redémarrer son activité le plus rapidement et le plus efficacement possible

Donner le coup d'envoi

Même avec un PRA, une entreprise peut avoir besoin d'aide dans la mise en œuvre de la relance – sans parler de celles qui n'ont aucun plan. Dans tous les cas, l'organisation a intérêt à désigner un chef de projet. Son rôle : aider à gérer la crise et trouver les moyens et les ressources adaptés au problème. Mieux vaut s'appuyer sur une équipe de consultants spécialisés qui pourront mettre en place le process et les étapes suivantes. Une réunion de crise permet de distribuer ces rôles.

Auditer le système

Avant toute relance, il faut vérifier que les traces de piratages ont disparu. Il est aussi nécessaire de voir à quel point le système a été infecté, pour ajuster la réponse.

Hiérarchiser les données à restaurer

La relance d'une activité prend du temps. Aussi, il faut aller à l'essentiel et traiter en priorité les données qui permettent de redémarrer la production dans les meilleurs délais.

Le bon ordre de relance :

1. Serveurs de sauvegarde,
2. Serveurs d'infrastructure (AD, DNS...),
3. Applications de sécurité : antivirus, firewalls virtuels…,
4. Bases de données critiques,
5. Applications critiques (propres à chaque activité, par exemple les applications liées à la fabrication et la remise en route des machines de production),
6. Applications de comptabilité, "filers", serveurs d'impression…,
7. Applications de DEV / Test.

Suivent les autres données et applications selon le cas de figure de l'entreprise, mais ces sept premiers niveaux de relance permettent de reprendre le cours des opérations au plus vite. Sans payer de rançon, sans perte de données dévastatrice, sans mise en péril de l'entreprise.

Se relever d'une cyberattaque est possible.

A RICOH Company

MTI France

Parc Claude Monet
3-5 allée de Giverny
78290 Croissy-sur-Seine

Standard :
+33 (0)1 30 09 52 00
FRinfo@mti.com

Abonnez-vous !

DELL Technologies
TITANIUM PARTNER

vmware®