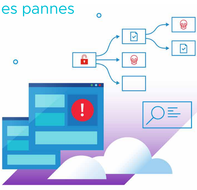
Protéger votre entreprise contre les rançongiciels

Pourquoi vous avez besoin de la DRaaS (Reprise d'activité sous forme de service)

Briser le mythe de la résilience : dans quelle mesure votre entreprise est-elle résiliente ?

Les enjeux sont élevés : conséquences des pannes



Les pannes non planifiées, occasionnées par des cyberattaques ou d'autres incidents graves, peuvent avoir une incidence sur :

- le chiffre d'affaires
- la cotation en bourse
- la productivité
- la confiance des clients
- la réputation de la marque
- la satisfaction des collaborateurs
- la conformité, les licences ou les accréditations

Vous n'y avez pas pensé ? C'est le moment !

Le saviez-vous ?

60 % des petites et moyennes entreprises ont subi une perte ou le vol de données sensibles au cours d'une période de 12 mois[1]

76 % des entreprises ont subi un événement qui nécessitait un plan de reprise d'activité (DR) au cours des deux dernières années[2]

Et puis, il y a les attaques par rançongiciel :

Une entreprise sera victime d'une attaque par rançongiciel toutes les **11 secondes** d'ici à fin 2021[3]

75 % des entreprises seront frappées par des rançongiciels d'ici à 2025[4]

La voie de la récupération peut être longue (et coûteuse)

La durée moyenne d'un arrêt complet de Data Center est de pratiquement **138 minutes**; l'arrêt total d'une installation de périmètre est supérieur à **45 minutes**[5]

Le coût moyen d'une interruption de service pour une entreprise s'élève à **250 000 $/heure**[2]

Vous cherchez à renforcer votre cyber-résilience ?

La reprise d'activité constitue la dernière ligne de défense. Un bon plan de reprise d'activité pose les bases de la cyber-résilience et vous aide à concevoir et à développer votre capacité de récupération dans l'éventualité d'une panne imprévue, afin de limiter toute interruption et tout dommage que votre entreprise pourrait subir.

72 % des entreprises présentent des capacités de reprise d'activité médiocres[6]

54 % des entreprises souffrent de « mirages de la confiance excessive »[6]

Qu'est-ce qui vous freine ?

Budget
Seules 45 % des entreprises considèrent que leur budget consacré à la sécurité est adéquat.[1]

Personnel
Seules 39 % des entreprises estiment que leurs collaborateurs ont l'expertise nécessaire pour se défendre correctement contre les cybercriminels.[7]

Excès de confiance
Un grand nombre d'entre elles estiment qu'il sera moins coûteux de payer la rançon. Le coût moyen d'une attaque par rançongiciel est de 4,62 millions de dollars.[8]

La bonne nouvelle : vous pouvez y remédier. Faites confiance à VMware Cloud Disaster Recovery™

Jusqu'à 60 % de réduction du TCO par rapport à la DR traditionnelle, sans investissement en amont, des coûts de main-d'œuvre moins élevés et aucune exploitation ni maintenance d'un site secondaire de DR

Protégez les charges de travail on premise et dans le Cloud de manière fiable et durable : réduisez l'empreinte carbone de votre DR de plus de 80 %

Adoptez le Cloud à votre rythme, éliminez la nécessité de configurer et de gérer un Data Center secondaire

VMware Cloud Disaster Recovery™

La reprise d'activité à la demande fournie sous la forme d'une solution SaaS gérée par le fournisseur, facile à utiliser et offrant la rentabilité du Cloud. Associez un stockage Cloud économique à une gestion SaaS simple pour assurer la résilience informatique à grande échelle.

- Tests sans interruption et orchestration des plans de retour arrière et de basculement
- Modèle de capacité de basculement avec paiement à la carte des ressources de DR
- Fonctionnalités de protection contre les rançongiciels : snapshots immuables dans le Cloud, récupération au niveau fichier et objectifs de point de reprise pouvant être réduits à 30 minutes
- Bilans d'intégrité automatisés de la DR toutes les 30 minutes
- Rapports d'audit intégrés et objectifs de point de reprise pouvant être réduits à 30 minutes

Prévoyez le meilleur, préparez-vous au pire. Disposez d'un plan de reprise d'activité pour protéger votre entreprise et les données de vos clients contre les pannes inattendues. Avec VMware Cloud DR, transformez votre plan en action.

Prêt à le déployer ? Démarrez ici

Sources :

1. Ponemon Institute, 10 Shocking data loss and disaster recovery statistics
2. IDC's Enterprise IT Infrastructure Survey, 4Q20:Insights on End-User 2021 IT Infrastructure Priorities and Adoption of Data Protection/Disaster Recovery Services and Solutions
3. Cybercrime Magazine, Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021
4. Gartner, "Detect, Protect, Recover: How Modern Backup Applications Can Protect You From Ransomware", publié le 6 janvier 2021, Nik Simpson et Ron Blair
5. Ponemon Institute, Data Center Downtime at the Core and the Edge: A Survey of Frequency, Duration and Attitudes
6. Gartner, Market Guide for Disaster Recovery as a Service, publié le 29 juillet 2021 - ID G00731593 par les analystes : Ron Blair, Jeffrey Hewitt
7. Ponemon Institute
8. Rapport IBM Cost of a Data Breach 2021