Protection contre les attaques ransomware

Application des principes NIST

pcd solutions
A CONVERGE COMPANY

Identifier	Protéger	Détecter	Répondre	Restaurer
Gestion des actifs, identification des applications, logiciels et technologies; Employés, clients et partenaires externes impliqués dans la manipulation des données critiques de l'entreprise; Gouvernance, définition des rôles et responsabilités; Évaluation des risques et stratégie d'atténuation; Environnements de travail, chaine d'approvisionnement; Communications et directives quant aux politiques de l'entreprise; Étapes de protection en cas d'attaque afin d'en limiter les dommages.	Comprendre les enjeux d'affaires, les obligations et exigences de conformité de l'entreprise; Gestion des identités et contrôle des accès; Sensibilisation et formation des employés; Cryptage des données de l'entreprise; Mise à jour des systèmes et automatisation des correctifs de sécurité; Revue de l'architecture de sécurité, des processus de sauvegarde, de disposition des équipements en fin de vie et de destruction des informations.	Analyse proactive des données, détection des anomalies ou corruptions; Détection des tentatives d'accès ou d'actions inappropriées sur les postes; Détection d'attaque, de tentative d'intrusion ou de connexion anormale sur le réseau; Investigation de toute activité ou geste jugé suspect d'employés; Mise en place de processus de surveillance et de détection en continu.	Mise en place des plans de communication aux employés, clients et partenaires à risque; Soulignement de l'attaque aux autorités, application des lois et mesures en vigueur; Analyse rétrospective de l'incident pour comprendre la faille exploitée, la corriger et prévenir contre une prochaine attaque; Ajustement des mesures de continuité des affaires; Automatiser, tester et re-tester les mesures de cyber-recouvrement établies dans une optique d'amélioration continue.	Suite à une attaque, mobiliser les effectifs requis pour le traitement de l'incident et en diminuer l'impact; Coordonner la restauration des données et des services; Coordonner la réparation des infrastructures et des composantes système, stockage, réseau infectées; Tenir les employés, clients et partenaires bien informés du statut des démarches de réparation.