Protection against ransomware attacks

Application of NIST principles

pcd solutions
A CONVERGE COMPANY

Identify	Protect	Detect	Respond	Recover
Asset management, identification of applications, software and technologies; employees, clients and external partners involved in handling business critical data; governance, definition of roles and responsibilities; risk assessment and mitigation strategy; work environments and supply chain; communications and directives related to company policies; safeguards to limit damage in case of attack.	Knowledge of business-related issues, obligations and compliance requirements; identity management and access control; employee awareness and training; enterprise data encryption; system updates and security patch automation; review of security architecture, backup processes, end-of-life equipment disposal and information destruction.	Proactive data analysis, detection of anomalies or corruption; detection of workstation access or inappropriate action attempts; detection of attacks, intrusion attempts or abnormal network connections; investigation of any employee activity or action considered suspect; implementation of a continuous monitoring and detection process.	Implementation of communication plans with employees, clients and partners at risk; communication of the attack to authorities, application of laws and measures in effect; retrospective analysis of the incident to understand the exploited weakness, correct it and prevent another attack; adjustment of business continuity measures; automation, testing and re-testing of cyber recovery measures established for continuous improvement.	Following an attack, mobilization of required staff to process the incident and reduce its impact; coordination of service and data recovery; coordination of infected infrastructure, system, storage and network components repair; communication of repair status to employees, clients and partners.