COMPREHENSIVE CYBERSECURITY PACKAGE FOR MSPS SERVING NONPROFITS

Protecting Nonprofits: 5 Essential Cybersecurity Steps Every Leader Should Know

Nonprofit organizations manage sensitive donor data, financial records, and critical community resources. However, cyberattacks are increasingly targeting these entities due to limited cybersecurity resources. In fact, according to the CrowdStrike Global Threat Report, ransomware attacks on nonprofits increased by 30% in the past year.

Nonprofits must approach cybersecurity with the same seriousness as their core missions. Protecting donor data is critical to maintaining trust and operational continuity," states Jane Doe, CISO at Nonprofit Cybersecurity Initiative.

24/7 Monitoring Across Donor Databases and Communication Platforms

Nonprofits need constant visibility into sensitive data repositories and communication systems to detect threats promptly.

FIX Implement continuous SOC and SIEM monitoring, integrating platforms like Salesforce, Blackbaud, and cloud storage solutions.

Advanced Endpoint Protection

Volunteers and staff often use personal devices, increasing endpoint vulnerabilities.

FIX Deploy robust EDR/XDR solutions such as CrowdStrike Falcon to secure all endpoints effectively.

Identity and Access Management

Credential theft and phishing attacks target volunteer and staff accounts.

FIX Adopt multi-factor authentication (MFA) and real-time identity protection solutions to safeguard access.

Continuous Vulnerability Management

Legacy systems and outdated applications pose significant risks.

FIX Employ real-time vulnerability assessment tools to identify and remediate weaknesses proactively.

Compliance and Data Privacy

Nonprofits must meet strict regulations such as GDPR and regional data privacy laws.

FIX Utilize centralized log management and automated compliance reporting for audit readiness.

vijilan
IT Security: Enabled
vijilan.com
info@vijilan.com
+1 (954) 334-9988