(https://www.vpnet.net/)

CYBER ATTACKS ON THE RISE

Karla Soto

> **“Cyber-attacks continue to rise in SMB with 63% experiencing some form of breach or data loss.”**

PUT THESE 7 TIPS INTO PRACTICE AND SIGNIFICANTLY REDUCE YOUR EXPOSURE:

1. **Educate users** – Employees are still the weakest link (https://vpnet.net/error-humano-en-las-empresas/) when it comes to activating malicious content. Providing a short, non-technical seminar explaining how to identify fraudulent emails, can help your business reduce risk. VPNet provides end user training to help cover cyber security topics for non-technical audiences. #cybersecurityawareness

2. **Secure endpoints** – Devices such as laptops and mobile phones are the point of entry to your network. Traditional anti-virus is good enough to prevent known malicious attacks. Next-generation AV is best for detecting unknown threats that have

yet to be registered (no signature).

3. **Apply security patches** – hackers bet most companies are not applying security patches to protect against known vulnerabilities. One of the easiest and effective mechanisms businesses have the power to control is patch management. Verify that your IT staff is consistently monitoring, and actively applying, vulnerability patches announced by technology vendors.

Helpful tip*: ideally, these patches should be done monthly and no later than every three months.*

SCHEDULE YOUR EVALUATION TODAY
(https://vpnet.net/contacto/)

4. **Deploy firewalls** – Basically all cyber-attacks originate with an internet connection. With a firewall in place, you can filter all of your internet traffic (inbound and outbound) to detect and block most malicious attempts. Important advice: having a firewall doesn't mean that it's adequately configured to detect, block, or notify when an attack has been identified. Ensure that the firewall is properly configured to comply with your business needs, type of data you create and share, and comply with industry regulations such as PCI DSS or HIPAA.

5. **Enforce password policies** – define and implement a password policy that works for your business. It is recommended that passwords are changed every 90 days. Added security comes in the form of password complexity. You can decide passwords length, the use of special characters, and inclusion of numbers.

6. **Prepare an incident response plan** – define and document how your business will handle cybersecurity breaches or data loss. This includes how a user reports and escalates a potential incident. How your company will investigate the incident internally. And finally, how you will notify customers of the situation. There are

additional mechanisms and action plans that stem from a cyber incident that need to be dealt with like public notifications to deal with public news, go into damage control to protect your brand reputation (https://vpnet.net/retos-que-ejecutivos-enfrentan-con-tech-y-seguridad/) and the unexpected IT service cost to mitigate the breach.

7. **Build a cross-functional security team** – If your company has IT staff that is specialized in cyber security, networking, and data protection, it's important for you to have a conversation about their Contingency plan. This should cover the network design, IT services in place to help detect, block, monitor, alert, and automate mitigation controls. This must include everything from the point of entrance (Eg: internet & firewall) all throughout the network to servers, printers, WiFi access points, and finally the endpoint devices.

If you do not have dedicated IT staff specialized in dealing with cybersecurity issues, you can find support from a Managed Security Service Provider (https://vpnet.net/beneficios-de-colaborar-con-un-mssp-como-vpnet/) (MSSP) to help verify, optimize, and monitor your network security and data privacy needs.

DOWNLOAD PDF CHECKLIST
(https://vpnet.net)

Request a complimentary consultation with VPNet to determine if your business can withstand a malicious event. Schedule your evaluation today by sending your request to: nsantini@vpnet.net (mailto:nsantini@vpnet.net)

Read the full article posted by the Entrepreneur here (https://www.entrepreneur.com/article/358610?fbclid=IwAR2Z5_P-9vC7nmg-RlJ9ObgT6phYsYc2wSq9iyF8N7h_dQP4r-8nsF7juqA)

Contacto

PO BOX 193780
San Juan, PR
00919-3780

787-620-5950
info@vpnet.net

Navegar

Negocio

Residencial

Sobre Nosotros

Contáctenos

Nuestras redes sociales!

(https://www.facebook.com/vpnetpr/) (https://www.linkedin.com/company/1798729/)

(https://www.youtube.com/channel/UCqjCnCUViEnEhUoVErF8DbA/)

(https://www.yelp.es/biz/vpnet-cidra)