Network Attacks Are Coming:

Discover 5 Ways to Stay Safe

The FBI has issued warnings about the increasing threat of ransomware attacks, so now is the time to ensure your organization has taken the proper security precautions.

While no strategy can offer perfect security, proactively configuring your network, documenting and practicing breach scenarios, and implementing security controls will decrease your chances of suffering an attack. Below are five actions you can take that will collectively form a strong defense foundation.

1 Develop a Recovery Plan

Effective ransomware security requires a response plan in the event of a successful attack. Your plan should at a minimum answer the following questions:

- What is your communication plan? That is, who should be involved and how will they correspond while triaging an event? How will you communicate with employees and your community? Who will speak with law enforcement and the media?
- Where have you stored your backup data? What steps must you take to restore it? Who will take those steps during an event?
- What is your recovery sequence? What are the most important steps you must take to resume everyday operations?
- What vendors do you employ? Who is your point of contact with each vendor?

2 Backup and Secure Your Data

Regularly back up your data. Keep your information in a secure location that only authorized users can access.

- A multi-layered backup strategy simplifies the rebuilding of your network after an attack.
- Consider one or more cloud solutions, such as ENA TrustBackup, as key layers to protect your data. Keeping your data in the cloud will simplify the restoration process after an attack.
- Consider immutable backup data to prevent encryption of backups in the event of an on-premise ransomware attack.

3 Control Your Network

Limit the reach of malware by controlling your network traffic with firewalls.

- Implement administrative level access restrictions to limit access and therefore exposure to risk.
- Consider increasing your “East/West” visibility within your network. If you do so, in the event of an infection you will be able to more quickly identify and contain the threat.
- Solutions such as ENA NetShield and ENA NetShield UTM provide hosted and on-premise firewall services that can be deployed to protect the core or key network segments from attacks and unwanted traffic.

4 Run Security Scans and Install Patches When They Become Available

Malware takes advantage of security loopholes and bugs within operating systems or software.

- Run software updates or patches as soon as they are available. These updates repair vulnerabilities attackers might otherwise exploit.
- Scan your data before storing offsite. This can prevent the storage of infected data that could compromise backup efforts.
- Consider performing a network penetration test at least once a year.

5 Train Your Employees. Then Train Them Again.

Most ransomware attacks are caused by an end user’s poor cybersecurity practices.

- Employee security awareness training helps your users recognize phishing attacks. Many tools for training, student data privacy compliance, and phishing simulations are available on the market. ENA TrustCompute also includes a GoPhish Stack.
- Stress the importance of scrutinizing links and attachments to ensure they have come from a reliable source.
- Business email compromise (BEC) is a leading source of security risk. Stress to all users the importance of double-checking requests for money, gift cards, unusual spending, and sensitive personal data. Instruct users to always call the sender when confirming requests that seem out of the ordinary.

To discuss how your organization can effectively implement these strategies, please reach out to us at info@ena.com or consult these helpful resources:

- **Cyber Readiness Institute’s “Ransomware Playbook”**
- **National Institute of Standards and Technology’s “Data Integrity: Recovering from Ransomware and Other Destructive Events”**

ENA delivers transformative connectivity, communication, cloud, security, and data analytics solutions supported by exceptional customer care. For more information, please visit **www.ena.com**, call **866-615-1101**, or e-mail **info@ena.com**.