Ransomware Preparedness Tips – Guest Article from CBA Associate member Passpoint Security

Ransomware attacks can be devastating for organizations because computer systems are no longer available to use, and in some cases, data may never be recovered. If recovery is possible, it can take several weeks, but your corporate reputation and brand value could take a lot longer to recover.

Below we've listed the top three steps your organization must take to be prepared for a ransomware attack.

1. Have a Plan
    a. Identify your critical assets and determine the impact to these if they were affected by a malware attack.
    b. Plan for an attack, even if you think it is unlikely. There are many examples of organizations that have been impacted by collateral malware, even though they were not the intended target.
    c. Develop an internal and external communication strategy. It is important that the right information reaches the right stakeholders in a timely fashion.
    d. Determine how you will respond to the ransom demand and the threat of your organization's data being published.
    e. Ensure that incident management playbooks and supporting resources such as checklists and contact details are available if you do not have access to your computer systems.

2. Test your incident response plan

    This helps clarify the roles and responsibilities of staff and third parties, and to priorities system recovery. For example, if a widespread ransomware attack meant a complete shutdown of the network was necessary, you would have to consider:

    a. How long it would take to restore the minimum required number of devices from images and re-configure for use
    b. How you would rebuild any virtual environments and physical servers
    c. what processes need to be followed to restore servers and files from your backup solution
    d. What processes need to be followed if onsite systems and cloud backup servers are unusable, and you need to rebuild from offline backups
    e. How you would continue to operate critical business services
    f. After an incident, revise your incident management plan to include lessons learnt to ensure that the same event cannot occur in the same way again.

3. Make sure you have good backups
    a. Up-to-date backups are the most effective way of recovering from a ransomware attack, you should do the following.
    b. Make regular backups of your most important files - it will be different for every organization - check that you know how to restore files from the backup, and regularly test that it is working as expected.
    c. Ensure you create offline backups that are kept separate, in a different location (ideally offsite), from your network and systems, or in a cloud service designed for this purpose, as ransomware actively targets backups to increase the likelihood of payment.
    d. Make sure that the devices containing your backup (such as external hard drives and USB sticks) are not permanently connected to your network. Attackers will target connected backup devices and solutions to make recovery more difficult.

Passpoint
security

Yvette Johnson
Managing Partner
Security Consulting Practice
Direct - 404.697.4603
yvette@passpointsecurity.com
www.passpointsecurity.com