RANSOMWARE ATTACK CHECKLIST

online

Ransomware takes advantage of an organization's reliance on computerized systems by denying them access for financial gain. Ransomware attacks occur daily; they are a real threat and shouldn't be ignored. Fortunately, there are a few techniques we can use to defend against ransomware.

Common methods of infection include:

> ***E-mails:*** Infected attachments or links to infected servers.

> ***Drive-By Downloads:*** Visiting an infected site runs scripts to download and execute the malware.

> ***Fake Popup Ads:*** *Ads that direct to malware downloads ("Security Warning – WARNING 3 THREATS FOUND!").*

What you can do to prevent a ransomware attack:

Inventory Management

It's important to know what software and hardware is in your environment.

What to do:
Restrict the use of unauthorized/ non-business software and hardware and run periodic scans.

Back Ups

Make sure you have backups of your critical data and ensure that it cannot be modified from the original machine.

What to do:
Periodically test your backups to ensure they are reliable and that you are backing up the right files to be able to restore a system.

Patch Management

Keep up to date on critical patches on your platforms, including software suites and 3rd-party vendors.

What to do:
Critical and important patches need to be applied within one week of release.

Filters

Despite one's best efforts at training, clever attacks can still trick even a savvy reader.

What to do:
Preventive technologies, such as web and e-mail filters, should be part of a standard defensive environment.

Testing

Test your systems to make sure that you're protected.

What to do:
Periodically conduct phishing simulations and share anonymized results with end users as part of training.

Education

Education for your team and end users is critical when recognizing and defending against attacks.

What to do:
Your IT and security staff should have a plan in place to defend against ransomware and educate users.

Limit the Reach

Limit the reach of ransomware to help control the situation in an attack.

What to do:
Segment important systems from end-user machines. Place systems on a separate network and firewall off all traffic that's not necessary for cross-segment operations.

Safe Web Browsing

Blocking scripts is effective in reducing the threat of drive-by downloads.

What to do:
In addition to web filters, consider the use of browser plugins to disable malicious scripts and/or block ads. You can also use script and ad blockers.

Advanced Techniques

In addition, you might want to try a few advanced preventative measures.

What to do:
Consider application whitelisting or only allowing signed applications to launch. Implement technologies that remove browser access to the local operating system.