Ransomware Prevention Checklist

Ransomware can infect an entire network within minutes once it gains access to a system. Files will be locked or encrypted, while cyber-criminals demand payment for access to your data. If paid, these criminals may or may not provide the necessary fix. Worse yet, paying ransom encourages this malicious activity and may even make you a target for future cybercrime.

Take these measures now to secure vulnerabilities, and prevent ransomware infection.

Inventory Management

- □ Catalog all the software which is deployed throughout the network
- □ There are no unsupported operating systems (Windows XP or 2003) running on my network
- □ No unauthorized software (non-business file sharing, remote desktop, streaming, etc.)
- □ There are no unknown/unmanaged computers, access points, or other devices on the network

Patch Management

- □ All servers have managed Windows patches and are up-to-date
- □ All workstations have managed Windows patches and are up-to-date
- □ All other operating systems have regular patch maintenance and are up-to-date
- □ All applications and their patches are maintained and up-to-date
- □ Monitoring is in place

Firewall

- □ Running a business grade firewall, not a consumer firewall
- □ Advanced filtering, intrusion detection, layer 7 traffic classification, and firewall is fully managed
- □ Running latest version of firewall software and managed updates
- □ Monitoring firewall alerts

Antivirus Software

- □ Running a business grade AV, not a consumer AV
- □ All servers and workstations are running AV that is real-time scanning
- □ Centrally managed and updated
- □ Policies setup in AV to block execution of harmful executables, along with alerting
- □ Monitoring AV alerts

Backups

- □ All machines that have critical data on them are backed up
- □ Images of servers are done at least monthly
- □ File backups are run daily
- □ Following 3-2-1 backup rule (3 backups, stored on 2 different media, with 1 offsite)
- □ Testing restores from backups at least monthly
- □ Monitoring backup failure reports

Filtering

- □ Antispam/anti-phishing in place
- □ Filtering file attachments in email (.exe, scr, .com, etc.)
- □ DNS filtering in place
- □ Show file name extensions in Windows
- □ Don’t enable macros (for Microsoft Office documents)

Web Browsing

- □ Disable all unnecessary scripts/plug-ins
- □ Browsers are up-to-date and running latest versions of required plug-ins

Permissions

- □ Enforce principle of "least privilege" on systems and data
- □ Software restriction policies put in place to prevent programs from executing from common ransomware locations (temp folders, etc.)

Advanced Prevention

- □ Group policies
- □ Periodic port/vulnerability scans
- □ Inspect network periodically to disable any unnecessary/vulnerable services
- □ Segment network for servers, backup, data, end-points
- □ Disable bootable devices like CD/ DVD and unnecessary USB ports for flash drives, etc.
- □ Enable BIOS Password Authentication

Training

- □ Security awareness training: Offer examples of what to avoid
- □ Simulated attacks (phishing, etc.) with action plan (ex: Disconnect from network / Wi-Fi)

About NovaStor

NovaStor® empowers overwhelmed and underfunded IT administrators with all-inclusive, highly scalable data backup solutions for both physical and virtual environments. NovaStor redefines service by including personalized local, expert level professional services as part of every solution.

NOVASTOR

www.novastor.com
dcinfo@novastor.com

NovaStor Corporation
29209 Canwood Street
Agoura Hills, CA 91301 USA
Tel +1 (805) 579 6700
Fax +1 (805) 579 6710

NovaStor Software AG
Baarerstrasse 20
CH-6304 Zug
Tel +41 (41) 712 31 55
Fax +41 (41) 712 31 56

NovaStor GmbH
Neumann-Reichardt-Str. 27-33
D-22041 Hamburg
Tel +49 (40) 638 09 0
Fax +49 (40) 638 09 29