CHECKLIST

Acronis

10 Simple Tips to Protect Your Organization from Ransomware

Ransomware attacks on businesses and institutions are now the most common type of malware breach, accounting for 39% of all IT security incidents, and they are still growing. Criminal ransomware revenues are projected to reach $11.5B by 2019. With a few simple policies and procedures, plus some cutting-edge endpoint countermeasures, you can effectively protect your business from the ransomware menace.

1 **Keep operating systems and applications up-to-date**
Ransomware attacks like the notorious WannaCry outbreak of 2017 often exploit software vulnerabilities that can be closed by installing the latest operating system and application patches, updates, and security releases. For instance, organizations that rely on Microsoft Windows should routinely review Microsoft Security Bulletins to learn about the latest security updates for Windows.

2 **Perform regular backups**
Regular full-image backups are the most foolproof way to defend against ransomware attacks. Backing up critical files regularly, preferably both to your company premises and to secure cloud storage, will let you turn back the clock to undo the effects of a ransomware attack. Your organization may lose some data and files produced since the backup, but everyone can quickly resume work without having to pay a ransom.

3 **Install anti-virus software and keep its signature database current** Endpoint anti-virus (AV) products provide a valuable defense against a variety of common malware attacks. Businesses should choose an AV product carefully and enable automatic updates to its signature database.

4 **Enable Acronis Active Protection in Acronis Backup**
Given that many new ransomware variants are able to evade AV defenses, your organization should also deploy modern data protection software with built-in anti-ransomware features, like Acronis Backup with Active Protection. This innovative technology uses behavioral heuristics and machine learning to automatically detect and terminate ransomware attacks, then automatically restore any files damaged before the attack was detected.

5

Close obvious vulnerabilities in your business email system

Your email administrator can make some simple configuration changes for all users that will make potential ransomware attacks more obvious. For example, make file-name extensions (like .pdf for Adobe Reader documents) visible by default. This will make it easier for users to identify potentially malicious, executable JavaScript files (with the file extension .js) trying to masquerade as a harmless Microsoft Word document (.docx). Consider company-wide AV scanning of all email attachments by default.

6

Teach users how to avoid becoming ransomware victims

Phishing emails crafted to appear trustworthy with personal information gleaned from sources like Facebook and LinkedIn are a common ransomware attack vector. Train your colleagues to be suspicious of emails from sources they don't explicitly know and trust. Sensitize employees to the risks of clicking on email links and opening email attachments, and encourage them to contact the sender about any slightly suspicious email.

7

Segment the business network to curtail worm propagation

Many ransomware variants are able to spread from an initially compromised machine to other servers and PCs on the network. Make this kind of propagation harder by subdividing your business LANs via technologies like Access Control Lists, private VLANs, and context-aware secure segmentation.

8

Grant administrative rights only to users and applications that absolutely need them

The greater the privilege level given to a user account or application, the greater the potential for harm if its credentials are compromised. Grant basic user privileges by default, and be reluctant to grant elevated application privilege levels via User Account Control.

9

Enable the newest security features in business applications

Popular business applications like Microsoft Office now include many "default-deny" security features, e.g., disabling of macro execution in Word or Excel attachments. Set these defaults company-wide to close some more attack vectors commonly used by ransomware.

10

Do not allow programs to launch from the AppData and LocalAppData folders

Many ransomware variants try to execute from certain system-level folders in an effort to masquerade as standard Windows processes. Create specific rules in your Windows installation to prevent files from executing from these folders.

DON'T BE A STATISTIC

Most ransomware victims are ill-prepared to respond, often losing critical data even if they pay the ransom, meanwhile suffering business consequences like lost revenues, angry customers and damaged brand reputation. With a few simple precautions, plus robust ransomware countermeasures like Acronis Active Protection, you can protect your valuable data and business in the most efficient, cost-effective way.

For additional information, please visit **www.acronis.com**

Acronis