Security

Solution brief: How to protect against ransomware

Eight best practices to prevent your data from being held hostage

Ransomware is a term used to describe malware that denies access to data or systems unless a ransom is paid to a cybercriminal. Every organization is susceptible to ransomware attacks. Fortunately, there are many steps you can take to minimize your organization's risk. Here are eight best practices to protect your organization against ransomware attacks.

1. Training and awareness

User training and awareness is paramount, and the first step to safeguard against ransomware. User instruction should include:

- Treat any suspicious email with caution
- Look at the domain name that sent the email
- Check for spelling mistakes, review the signature and the legitimacy of the request
- Hover on links to check where they lead to and if any URL seems suspicious, directly type the website or look it up on search engines vs. clicking the link in the email

2. Email security

You should deploy an email security solution that scans all attachments besides filtering for spyware and spam. Along with periodic user training and risk assessments, you should also conduct phishing vulnerability tests.

3. Anti-malware

Whether personal or corporate devices, endpoints are particularly at risk if they are not managed by IT, or don't have the right anti-malware protection. Most anti-virus solutions are signature-based, and prove ineffective if not updated regularly. The newer ransomware variants are uniquely hashed and thereby undetectable using signature-based techniques.

Many users also turn off their virus scans so that it doesn't slow their system down. To address these limitations, there are endpoint security solutions that use advanced machine learning and artificial intelligence to detect malware. They also have a small footprint, causing minimal performance overhead.

4. Mobile endpoints

Management of endpoints is also a growing challenge as devices with multiple form factors and operating systems are introduced to the network. Mobile devices are particularly vulnerable as noted in the 2016 Dell Security Annual Threat Report with emerging ransomware threats on the Android™ platform. Choosing a solution that is able to automate patching and version upgrades in a heterogeneous device, OS and application environment, will go a long way in addressing a range of cyberthreats including ransomware.

For remote users who are outside the enterprise firewall perimeter, VPN-based access should not only establish a secure connection but also conduct a level of device interrogation to check for policy compliance on the endpoint. If an endpoint does not have the required security updates then it will not be allowed on the network or it will be granted access to only a limited set of resources.

Specifically, for Android mobile device users, the following steps are recommended:

- Do not root the device, as it exposes the system files for modifications
- Always install apps from Google Play store, as apps from unknown sites or stores can be fake and potentially malicious
- Disable installation of apps from unknown sources
- Allow Google to scan the device for threats
- Take care when opening unknown links received in SMS or emails
- Install third-party security applications that scan the device regularly for malicious content
- Monitor which apps are registered as Device Administrators
- For corporate-managed devices, create a blacklist of disallowed apps

5. Network segmentation

Most ransomware will try to spread from the endpoint to the server/storage where all the data and mission critical applications reside. Segmenting the network and keeping critical applications and devices isolated on a separate network or virtual LAN can limit the spread.

6. Backup and recovery

Another safeguard against having to pay ransom is a robust backup and recovery strategy. Back up data regularly. There will be less data loss in case of infection if there is a remote backup. Depending on how quickly the compromise is detected, how far it has spread and the level of data loss that is acceptable, recovery from a backup could be a good option. However, this calls for a smarter backup strategy that is aligned to the criticality of your data and the needs of your business around recovery point objectives (RPO) and recovery time objectives (RTO). Recover the most critical data in the least amount of time. Finally, just having a strategy is not sufficient. Periodic testing of disaster recovery and business continuity is just as important.

7. Encrypted attacks

Having the right enterprise firewall that is able to scan all traffic irrespective of file size is also critical. With the rapid increase in SSL encrypted traffic, as indicated by the Dell Security Threat Report, there is always a risk of downloading encrypted malware that is invisible to traditional firewalls. Hence it is important to ensure the firewall/IPS is able to decrypt and inspect encrypted traffic without slowing down the network significantly.

Another recommendation is to show hidden file extensions. For example, sometimes malware can enter the system with a .pdf or .mp3 icon, but in reality it is an .exe file.

8. Monitoring and management

The enterprise firewall should be able to monitor both incoming and outgoing traffic, and block communication with blacklisted IP addresses as ransomware tries to establish contact with its command and control servers.

> An effective approach for blocking ransomware requires broad coordination of security training, technology and management.

If a ransomware infection is detected, disconnect the infected system immediately from the corporate network. As soon as a new malware variant is detected, the firewall should have an automated update and centralized management process to roll out updates and policies quickly and consistently across all nodes. In addition, it is crucial to update your software and operating systems regularly.

Conclusion

Dell Security solutions can enhance protection across your organization by inspecting every packet and governing every identity. As a result, this protects your data wherever it goes, and shares intelligence to safeguard against a variety of threats, including ransomware.

Learn more about our next-generation firewalls.

For More Information

About Dell Security

Dell Security solutions help you create and maintain a strong security foundation with interconnected solutions that span the enterprise. From endpoints and users to networks, data and identity, Dell Security solutions mitigate risk and reduce complexity so you can drive your business forward. www.dell.com/security

If you have any questions regarding your potential use of this material, contact:

Dell
5455 Great America Parkway,
Santa Clara, CA 95054
www.dell.com/security

Refer to our Web site for regional and international office information.