Indiana Information Sharing and Analysis Center

Small Business – High Risk for Ransomware

Why are small businesses and other small organizations at higher risk for a ransomware incident?

- Smaller organizations typically don’t have the technical support resources found in others. This lack of resources may result in environmental weaknesses targeted by ransomware.
- Small organizations with limited awareness budgets are prone to the human errors that result in ransomware.

Specific small business traits that increase the risk for ransomware.

- Support staff with elevated rights use the same ID for administration duties and non-administration duties
- Workstations and servers are not patched to current levels, often not patched going back some time
- Data is not backed up reliably, there is not a current copy disconnected from all networked devices
- Users more prone to mistakes in regard to clicking on phishing links, opening malicious attachments, navigating to nefarious websites

Goal 1 – Avoid Catastrophe

Assumptions

- The odds your organization will be affected by ransomware are 100%
- All data and resources will be encrypted and inaccessible
- You will not pay the ransom

Requirements to avoid catastrophe

1. Avoiding the Worst Case - Your organization must backup its data. A copy of that data that is relatively current, must be stored disconnected from the environment.

   Explanation – The most catastrophic outcome of a ransomware attack is that data is encrypted and cannot be recovered. In worst case scenarios, not only does data get encrypted, but back-up copies are encrypted as well. If there is a copy of the data that remains unencrypted business can eventually be restored after the environment is cleaned, though the downtime and cost to clean the environment and restore data should not be underestimated. If the backups are encrypted the organization will face a decision of lose the data, likely forever, or pay the ransom.
2. Avoiding having to deal with the worst case – Require a separate ID for each user with admin responsibilities used solely for admin duties. Do not allow this ID to surf the Internet or access a mailbox.

   Explanation – In the worst case scenario described above the mistake that triggers the ransomware infection of catastrophic magnitude comes via an error by someone with admin privileges. The infection then spreads to all storage locations the affected ID has access to which for small organizations is typically everything. By requiring admins to use a separate account, when they make the mistake that triggers ransomware, much less data will be encrypted. It will be limited to the access that the affected ID has. It may still be damaging but it won’t be catastrophic. Clean-up and restore times will be substantially less.

Summary

Small organizations have the deck stacked against them with the ransomware threat. Key ransomware protections such as patching programs, effective anti-virus software, email and Internet filters, least privilege, backup routines and user training are often not where they need to be. For smaller organizations, rather than focusing on preventing a ransomware infection they may be better assuming one will happen, being ready for it, understanding what can happen, and focusing on minimizing the damage and speeding recovery.