Ransomware – What to Expect When You Least Expect It
Douglas Jambor, CISSP, ISFCE, CCE  |  Senior Manager, DHG IT Advisory

What is a ransomware attack? Ransomware attacks can sneak into businesses when a user opens an email with an attachment or document. More aggressive forms of ransomware can be found embedded in websites (even trusted, legitimate websites) where hackers wait to infect visiting users’ machines. This type of attack is known as a watering hole or a drive-by download attack.

Ransomware attacks can cripple businesses and often happen at the most inconvenient times. Once a business is hit with a ransomware attack, a majority, if not all, key business processes can come to a halt until the event is resolved by IT professionals. If the security posture is poor, businesses can struggle to recover from a ransomware attack typically, due to the fact that the necessary precautions leading up to the attack were not taken. Businesses can face the encryption of their workstations, servers and databases housing core business data, including email servers.

Once a network is encrypted, the business ceases to function. This is when the painful lessons begin. Whether you have IT staff members or the IT staff function is outsourced, the worst information to learn is that there are no backups of your data or that the backups are encrypted, as well. In this case, there are limited options for data recovery or the data may be completely unrecoverable. An external incident response team of digital forensic specialists can be called in, but ransomware variants are sophisticated and thorough often leaving businesses with limited options to either: 1) pay the ransom, or 2) rebuild from scratch and lose all business data.

At this point, the only way to usually recover data is to attempt to pay the ransom. Paying the ransom does not guarantee whether or not you will be able to unencrypt your data. By making initial plans now, businesses can begin to strengthen their overall security posture and prepare for a cybersecurity incident, including ransomware.
What can business do to survive a ransomware attack?
Begin by asking your IT staff, “if the network and our backups were hit with ransomware, how would we recover?” It all starts with having a clean digital hygiene with a strong security posture. Having your business audited for ransomware attacks, is how you can discover a way to properly prepare and respond to a ransomware attack.

Things to consider now before it is too late

1. Backups, backups, backups. The only silver bullet for surviving a ransomware attack is having appropriate backups. We recommend using cloud-connected backup appliances with different credentials for core data. Tape backups are still effective against ransomware attacks, as well. All virtual machines (VMs) should be fully replicated, stored on a separated domain and kept powered off for a quick, seamless recovery in the event of a security incident.

2. Ensure the patch management program covers key end-point applications (Adobe® Flash or PDF, Java™, Microsoft® Office). There are numerous appliances out there that can patch missing operating system patches. It is the missing application patches you must be vigilant for when it comes to many cybersecurity events. Make sure your patch management software or appliance provides visibility into missing applications patches. If you are missing this key control, this exposes your business to a security incident.

3. Implement spam filter. Many organizations still do not have a best-in-breed product to scan all incoming email messages, which blocks most threats. It should be configured to block all *.VBS, *.BAT and *.EXE files.

4. Disable all incoming macro script-enabled office documents on all inbound emails.

5. Purchase a next-generation antivirus solution for all endpoints. If current endpoint antivirus solutions cannot prevent most ransomware, this is most likely not the correct software. See https://www.av-test.org/en/ for a comparison of the best-in-breed solutions for businesses. If you have not upgraded your current antivirus solution over the past couple of years, it is probably outdated software.

6. Manage the use of administrator accounts. IT staff should implement the principle of least authority. No one should have administrator access unless absolutely necessary. Administrator access should only be used to perform job functions when necessary.

7. Stop the spread of ransomware via Group Policy. Setup policies that only allow executables to run from certain folders (%Windir%, Program Files, Program Files x86). Prevent executables from running in users’ directories and configure network shares with least privilege in mind.

8. Implement application whitelisting via AppLocker on the Windows domain controller. This is a built-in feature of the Microsoft server, which only costs time for IT staff to implement.

9. Perform an annual comprehensive penetration test. The penetration testing should include credentialed vulnerability scanning, so missing application patches (e.g., Adobe Flash or Java missing patches) are identified appropriately. We also recommend the penetration testing include a small measure of IT audit. This should include a network management and monitoring security controls review covering the top security controls within an organization. See SANS Institute CIS Critical Security Controls Top 20. Testing should include a social engineering assessment to understand end-user awareness levels currently within the organization. Based on the results of this testing, follow up by implementing an end-user awareness training program designed to continually raise awareness levels.

10. Ensure you have a well-documented incident response policy. This policy should contain information about the members of the incident response team, the role of each of the team member, the party responsible for testing the policy and how to execute the policy in the event of an incident. Having a policy that is comprehensive, in-place and practiced will assist the organization with the tools and resources to identify and recover from a security incident.

Being vigilant and implementing a strong security control environment is how organizations can survive ransomware and other cybersecurity incidents. Plan on starting these recommendations during the next year, as some of these changes take time to enable. Implementing these controls will help ease security concerns and position your business to be prepared in the face of cybersecurity attacks.

DHG Contact

Douglas Jambor, CISSP, ISFCE, CCE
Senior Manager, DHG IT Advisory
itadvisory@dhg.com