Report

How to Protect Your Organization from Ransomware Attacks

A special report from Tunde Odeleye, director of penetration testing services for Insight Cloud + Data Center Transformation (CDCT).

April 2020

Key takeaways:

- Ransomware instances are prevalent, warranting specific security measures be taken
- Choose effective and secure technologies that are properly managed and maintained
- Make use of tools like multifactor authentication, as passwords alone are insufficient protection
- Audit and update backup processes to secure against the risk of having data held hostage

Over the last two months, I've had the opportunity to assist four separate organizations in responding to some nasty ransomware attacks. While we have a plethora of security solutions out there, these attacks have shown no decrease in frequency or impact, with the most recent being the attack on Cognizant in mid-April.

From these response engagements, as well as my own experience conducting penetration testing engagements, I gained some valuable insight. The following, simple yet effective strategies can help mitigate the risk and severity of ransomware attacks.

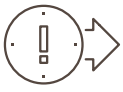
1. Choose the right endpoint security solution

There's no easy way to say this, but the fact of the matter is all endpoint security products are not created equal.

You want to make sure you've selected a solid product that works. It doesn't have to be the best, but it has to work well for your users and your mission. You also want to ensure the endpoint security solution is properly deployed across the organization.

Most endpoint security solutions protect against automated and manual threats by leveraging the following key capabilities:

Incoming threat detection and prevention (pre-execution)



Execution-based threat detection and prevention (on-execution)

Continuous analysis and remediation post-infection (post-execution)

The unfortunate truth is, each of the endpoint security solutions in the marketplace do not possess the same level of threat intelligence, nor do they operate with the same level of remediation effectiveness.

When all else fails — and it will at some point — your endpoint solution will literally be your last line of defense. So, choose wisely. If you're unsure of which solution to choose, I strongly recommend you engage someone knowledgeable who can help you make the right selection.

2. Monitor your Active Directory changes (especially group policies)

In each of the recent ransomware engagements I led, I noticed the client did not proactively monitor their Active Directory® (AD) changes, especially group policies.

The attackers, in each case, modified an existing group policy to create a scheduled task which would run an executable at a future date. This is by far the easier and quickest method for distributing an attack throughout an environment.

Monitoring AD changes, particularly during off-hours and weekends, is a very effective way to sniff out the signs of an attack before it gets out of hand.

3. Implement a workstation isolation strategy

This, in my opinion, is the most effective strategy for mitigating lateral movement of malicious attackers in any environment.

The default security posture for most organizations allows workstations on the same subnet (in some cases enterprise-wide) the ability to communicate with one another. If you think about it, is there a reason why a workstation should be able to communicate with another workstation? The answer generally is "no," as most network communications are clients (i.e., workstations or servers) talking to servers (i.e., on-prem or in the cloud).

With that in mind, if you limited workstation-to-workstation communication, a compromised workstation (Patient Zero) could not be used as a threat agent to attack other workstations. Patient Zero would only be able to target server resources, which should make it easier to detect the attack, assuming proper server hardening and technical controls are in place.

The funny thing is, most environments already have access to a perfect solution in Windows® Defender Firewall, which can be managed with AD group policies. This can be part of a broader endpoint hardening strategy, which many government and educational users have not undertaken. **Workstation isolation is a very effective security strategy, but hardly ever used in most environments I've seen.**

4. Implement a vulnerability management program

Notice, I did not say "patch." While patching is extremely important, it is not enough.

If you think about it, the goal of patching is to close security gaps within software applications. However, those aren't the only gaps you should be concerned about.

Your security gaps could also be configuration related. You can have the most up-to-date systems/applications on the planet, but if your internal systems are relying on insecure protocols, such as NTLMv1, that's a disaster waiting to happen.

As a result, I recommend organizations implement a continuous vulnerability management program involving regular scanning of external and internal assets, as well as prioritizing remediation based on the severity of the identified vulnerabilities, which may or may not be patch related. Then, remediate accordingly.

5. Implement Multifactor Authentication (MFA)

Yes, we've all been told to use strong passwords, but the fact of the matter is passwords alone are not enough.

In every single incident I responded to, MFA was not in use. If you only use passwords to authenticate a user, even if they are strong passwords, you are taking on risk. Requiring a second form of authentication helps ensure identity, as it's usually something that isn't as easy for an attacker to obtain.

Here's a simple rule of thumb:

If it is externally facing,
MFA is a must for everyone.

If it is internally facing,
MFA is a must for all admin accounts.

This is ultimately based on your risk tolerance, however the aforementioned rules are a good starting point.

6. Make regular offline backups

Backups must be **comprehensive** and performed **regularly** with **offline** copies. This means the offline copies are not continuously addressable or accessible from production networks.

In one incident, the client's enterprise backup solution was completely deleted by attackers, **however their offline backups in the cloud literally saved them from several thousands of dollars in ransomware payment**. In a separate instance, the client had to pay several hundred thousand dollars, as they had no other choice due to the criticality of the encrypted business systems.

Surely, there are numerous things not on this list that could serve as additional protections against ransomware. The goal here is to summarize some simple and effective strategies that can easily be implemented to provide quick wins in the war against ransomware. It is my hope that this information helps your business from becoming the next victim, as no organization or institution deserves the stress, costs, and reputational damage that can be done.

If you have questions about these strategies, or would like to discuss your organization's security posture with our experts, we would be happy to help.

Contact us to speak with our security team

Learn more about our security services

Explore our approach and capabilities

Meaningful solutions driving business outcomes

We help our clients modernize and secure critical platforms to transform IT. We believe data is a key driver, hybrid models are accelerators, and secure networks are well integrated. Our end-to-end services empower companies to effectively leverage technology solutions to overcome challenges, support growth and innovation, reduce risk, and transform the organization.

Learn more at:
insightCDCT.com | insight.com

Insight PUBLIC SECTOR

IPS.insight.com