PROFICIO™

RANSOMWARE CHECKLIST

RANSOMWARE REMAINS THE MOST PROMINENT MALWARE THREAT

How prepared are you?

Ransomware attacks have evolved. Cybercriminals today are targeting larger organizations, using more sophisticated penetration techniques, and demanding seven-figure ransoms. In an environment where cyber insurance may not cover your losses and reputational risk is at an all-time high, here are some things you can do to better prepare your organization for a ransomware attack.

PROFICIO™

Average ransom fee requested $200,000[1]

1

Secure Backups

Just backing up systems and data is not sufficient. Today's attackers search for online backups and control or delete them before deploying ransomware. You should take steps to protect your backup files including having different copies in multiple locations, using network segmentation to isolate your backups, regularly scanning backups for malware, and implementing two-factor authentication for all backup administrator accounts.

Do you have secure backups?

2

Leverage EDR

Endpoint Detection and Response (EDR) products are critical to stopping ransomware – but they must go beyond monitoring for signatures of known ransomware and detect suspicious processes that could indicate a zero-day attack is in progress. Ransomware attackers are constantly adapting their code to bypass EDR software and endpoint security vendors should use technologies like AI to better detect and block these attacks.

Is your EDR solution set up to detect the early signs of ransomware and able to protect against hackers attempting to turn off capabilities?

3

Hunt for Threats

To catch the early stages of a ransomware attack, collect and continuously monitor infrastructure and endpoint logs to detect precursors of threat activity. Map use cases to the MITRE ATT&CK framework to better classify ransomware attackers' techniques and tactics. Log events correlated with threat intelligence data should trigger investigations into activities like lateral movement, suspicious privilege escalation, or use of encoded PowerShell commands.

Do you proactively hunt for threats that could indicate a ransomware attack?

4

Enable Automation

Automating threat containment protects an organization by quickly blocking IP addresses of bad actors probing your network, stopping anonymous login attempts and isolating systems when a credible threat is detected. By using SOAR or XDR technologies, it provides time for incident responders to investigate indicators of ransomware attacks before they result in a damaging breach.

Are you using automation to increase productivity and reduce mean time to respond?

Average downtime after a ransomware attack 21 Days[2]

5 Close the Back Door

Attackers often try to exploit unpatched vulnerabilities or remote services. Reduce these risks by closing unnecessary network ports to reduce entry points for attackers and prioritize patching the most critical vulnerabilities based on their severity and risk of exploitation.
Is your team taking steps to ensure you're not leaving a back door open for cybercriminals?

6 Email Best Practices

Email is a favorite delivery channel for ransomware attackers. Phishing emails that contain malicious attachments or entice users to visit an infected website are significantly reduced by robust email security software and employee training.
Are your employees taught about email security best practices?

7 Assess Security Technologies

A defense-in-depth approach reduces the risks associated with dependency on a specific solution or vendor. Having multiple security monitoring tools at both the endpoint and network levels makes it easier to detect and discover ransomware related activities.
Do you frequently assess your security technologies at the perimeter, endpoint, core, and cloud and address any gaps found in your threat coverage?

8 Incident Response Plan (IR)

If an incident does occur, you want your team to be prepared so that your companies' downtime will be minimized. Best practices include having a written Incident Response (IR) plan and routinely practicing the process, including getting networks back online using your segmented backups.
Is your IR plan documented and practiced on a regular basis?

PROFICIO™

Ransomware attack will occur every 11 seconds[3]

9 To Pay or Not to Pay

One of the toughest questions to ask when an incident occurs is: Will you pay the ransom? Before you are in a critical situation, it's best to have your policy in place, so you know if your organization and cyber insurance provider would be in support of paying a ransom and if so, how much would they be willing to spend and how would they plan to pay it.
Have you had a conversation with your team about the potential need to pay a ransom if your networks are attacked?

10 Reach Out for Help

Making sure your internal teams are prepared is critical to minimizing the impact of a breach, but often you'll need outside parties to help you recover from the incident. This includes incident response firms, cyber insurance providers, outside legal counsel, and depending on the size of your company, law enforcement agencies.
Do you have relationships in place to help you manage the recovery process of a ransomware attack?

It's not a matter of if you will be attacked... but when.

Being prepared for a ransomware attack on your organization is critical. Proficio is a Managed Detection and Response (MDR) service provider delivering 24/7 security event monitoring and incident management from our global SOCs to help you reduce risk and be better prepared for an attack. Whether you need a fully managed security service or are looking to extend your current team, we offer flexible, customizable solutions to fit your needs. Contact us to learn more about how Proficio can help you be prepared for a ransomware attack.

Contact Proficio at info@proficio.com | Proficio.com

1 National Security Institute, 2021 - 2 Coveware, 2021 - 3 Cybercrime Magazine, 2019