



# **Ransomware** Prevention & Response Checklist

[WWW.PACKETLABS.NET](http://WWW.PACKETLABS.NET)



# Ransomware Prevention Checklist

## PEOPLE

- ☐ Conduct regular security awareness training to educate employees not to open or click on links from unknown sources

## PROCESS

- ☐ Keep relevant systems fully patched
- ☐ Run scheduled checks to identify available patches and install these as soon as feasible
- ☐ Employ zero trust principles in all networked systems by managing access to all network functions
- ☐ Segment internal networks to prevent malware from spreading among potential target systems
- ☐ Allow installation and execution of authorized apps only
- ☐ Configure operating systems to run only authorized applications
- ☐ Inform your technology vendors of your expectations (e.g., in contract language) that they will apply measures that discourage ransomware attacks

## TECHNOLOGY

- ☐ Check for lateral movement protocols within a target network. Do you have legacy LLMNR/NBT-NS? Are you using DHCPv6 unnecessarily? If so, disable them
- ☐ Check if your anti-malware solution is configured to detect and prevent ransomware. You'll likely find this capability in EDR/XDR solutions
- ☐ Check if backups to critical systems are domain-joined. If so, remove it from the domain
- ☐ Segment access to critical systems instead of using a flat-network. This makes the ability to traverse to your critical systems more difficult, which will give you more time to prevent a successful attack
- ☐ Prevent personally owned computers from joining the work network
- ☐ Separate standard user accounts from privileged accounts while also enforcing multi-factor authentication on every capable account
- ☐ Allow external access to internal network resources via secure virtual private network (VPN) connections only

# Ransomware Response Checklist

## IMMEDIATE RESPONSE

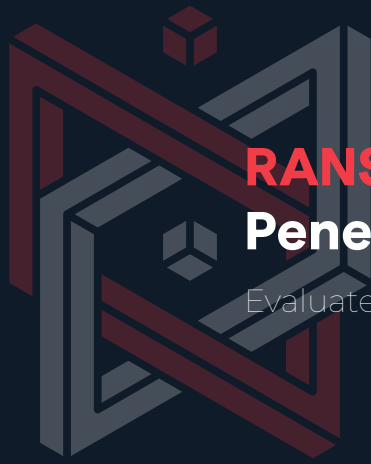
- ☐ Shut down systems and disconnect from network
- ☐ Isolate your backups
- ☐ Disable all shared drives that hold sensitive information
- ☐ Issue alert to customers and employees and provide next steps
- ☐ Contact law enforcement to report attack
- ☐ Assemble your task force and determine the scope of the damages
- ☐ Identify the attack path used to infiltrate network

## POST ATTACK ACTIONS

- ☐ Identify and mitigate vulnerabilities to avoid future attacks
- ☐ Restore files from backup

It is important to develop, implement, and regularly exercise an incident recovery plan with defined roles and strategies for decision making. This can be part of a continuity of operations plan. The plan should identify mission-critical and other business-essential services to enable recovery prioritization, and business continuity plans for those critical services.

Maintain an up-to-date list of internal and external contacts that need to be notified in the event of a ransomware attack including law enforcement, legal counsel, and an incident response team.



# RANSOMWARE Penetration Testing

Evaluate the preparedness and risk of a ransomware attack

## Overview

Ransomware penetration testing evaluates the preparedness and risk of a ransomware attack. Our comprehensive assessment identifies gaps in people, processes, and technology, to determine the likelihood and readiness for a ransomware attack.

In addition to a complete analysis of the security program against the Cybersecurity Framework Profile for Ransomware Risk Management (NISTIR 8374), and a technical assessment of security controls, a full penetration test is conducted to measure the robustness of your systems.

[Learn More](#)

## Why Conduct a Ransomware Penetration Test?

- ▶ Identify the impact of potential ransomware attacks
- ▶ Detect gaps in policies and processes
- ▶ Ensure backups are secure and uncompromisable
- ▶ Protect sensitive information
- ▶ Provide proactive protection
- ▶ Prepare your team for potential attacks

## Ransomware Penetration Testing Service Highlights



Identify lateral movement protocols



Protect sensitive information



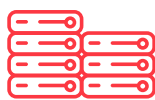
Detect evasion scenarios



Build response capabilities



Identify recovery capabilities



Technical assessment components



Non-technical assessment components



Preparedness evaluation

## Additional Resources



Learn more about securing your company against ransomware attacks.

[Read article >](#)



Learn more about the top 3 ransomware vectors and their preventative measures.

[Read article >](#)



Learn more about the pros and cons of paying ransom to malicious hackers.

[Read article >](#)

## Packetlabs Ltd.





Packetlabs is an IT consulting firm specializing in expert penetration testing. We offer a number of services to help strengthen your security posture including infrastructure penetration testing, web and mobile application testing, social engineering, red team exercises, source-code reviews and exploit development. Our clients are in a number of industries including government, finance, education, technology, media, retail, healthcare and energy.

Our slogan, "Penetration Testing beyond the checkbox" illustrates our commitment to the industry to provide expert-level penetration testing. Our consultants think outside of the box, find weaknesses others overlook, and continuously learn new ways to evade controls in modern networks.

[Get a Quote](#)

[Contact Us](#)

## The Packetlabs Advantage

-  Skilled OSCP certified Ethical Hackers
-  Full-coverage approach with 95% manual simulations
-  Reports are clear and concise and use narrative approach
-  Best value for your dollar