COGNISYS

PENETRATION TESTING

Ransomware readiness assessment

Assess your organisation's ability to withstand a ransomware attack.

We identify weaknesses in technical controls, governance, policies, procedures, and staff training that could result in a compromise.

Prioritised, actionable improvements and remediation advice will be given by our expert consultants, based on current known ransomware and APTs. We help your organisation return to an acceptable risk level.

Why get a ransomware assessment?

Ransomware poses severe risks to organisations, causing data loss, downtime, and financial harm. Recovery can be challenging and costly. Protecting against ransomware is crucial.

If the worst were to happen, are you prepared? Our readiness assessment evaluates readiness and ensures preparedness, including reviewing policies, procedures, and governance to respond effectively and prevent future attacks.

Our service includes

External network penetration test

Internet-facing systems are the first port of call for ransomware gangs looking to infiltrate your organisation. It's essential that these are manually assessed by experts and vulnerabilities are identified and mitigated.

Continuous DNS monitoring to detect suspicious activities, such as DNS hijacking, DNS tunnelling, or DNS cache poisoning is essential to protect your data, network, and reputation.

Assumed breach assessment

Simulation of a real-world attack where it is assumed that a threat actor has successfully breached the system and has compromised a workstation or server. We will assess the configurations and protections.

Attempts will be made to execute non-destructive ransomware payloads to test the EDR configuration and ensure that real ransomware would be blocked and reported during a real attack. Additionally, Egress and C2 checks will ensure that in the event of a compromise, a threat actor would be unable to connect and exfiltrate data to and from the network and that such attempts are flagged as malicious and reported correctly.

Active Directory review and attack path management

Active Directory and Azure are hot targets for threat actors. We will perform a thorough assessment of the current AD/AAD environment and highlight risks that could lead to privilege escalation, admin access and access to sensitive information of interest to ransomware threat actors.

Governance, policies and procedures review

An in-depth review of policies and procedures related to ransomware prevention, such as incident response plan, business continuity plan, insurance etc.

Social engineering assessment

83% of cyber attacks in 2023 were phishing attacks, and business email compromise is a common entry point for ransomware. Are your employees as security aware as you think?

Our education and training will ensure that all staff know the risks of ransomware and their role in preventing an attack.

Vulnerability assessment

A great tool when combined with pen testing to detect potential vulnerabilities and misconfigurations commonly targeted by ransomware.

Backup and recovery procedures review

We will examine the system's backup process and ensure that all relevant data is backed up and is being stored appropriately and securely.

Governance, policies and procedures

An incident response plan is essential in the event of a ransomware attack. It provides a framework of steps and procedures to follow, which can help contain the attack, reduce the impact, and ultimately help to recover.

Having a dedicated point of contact is also important, providing a single individual responsible for leading the response and managing communications with internal and external stakeholders. Other documents that are important in the event of a ransomware attack include a backup plan, a communication plan, and a post-incident review.

BACK TO CONTENTS