Ransomware Defence Assessment

autodata

Test the effectiveness of your ransomware defences and identify improvements to mitigate the risk of a breach

CREST

CHECK
IT Health Check Service

Our Ransomware Defence Assessment (RDA) is a blended approach of paper-based audit checks and hands-on manual testing. The RDA assesses your current administrative and technical controls, the teams and processes in place to detect attacks and the plans in place to restore business activities.

Our **four-level methodology** is aligned with a **'defence-in-depth'** strategy focusing on controls preventing initial access attempts through to the activities likely to occur in the event of a successful breach:

1. Audit Checks

This test takes the form of a Workshop Event, involving one of our Senior Consultants and your Cyber Incident Response Team (CIRP). The checks are divided into the three main stages of a ransomware attack:

Stage 1: Attack techniques used to gain a foothold on the infrastructure
Stage 2: Controls to mitigate the attacker accessing key internal assets
Stage 3: Procedures to contain the breach and recover business activities

2. Infrastructure Tests

A range of tests to ensure the host and service configurations are effective and appropriate across mail servers, third-party integrations, external services, data backups, workstations, Active Directory, remote access, segmentation testing and anti-virus software.

3. Attack Simulation

Simulated attacks are launched in a controlled and non-disruptive way on mail filtering and SIEM tools to confirm the effectiveness of the defences in place to detect attacks and the responsiveness of the associated teams.

4. Reporting

Once the above stages are completed, we produce a concise report containing both technical and non-technical recommendations for how the risk of a ransomware attack on your infrastructure could be reduced.

Benefits of our RDA:

- **Ransomware Security Workshop** - to determine how the configuration of your infrastructure compares with industry best-practice recommendations.
- **Detailed Assessment** - including configuration of key technical controls in place to mitigate the risk of ransomware attacks such as mail filters, anti-virus and network segmentation.
- **Simulated Attacks** - conducted in a safe and controlled manner to test the most likely internal and external vectors used to deliver ransomware payloads and the ability to detect malicious behaviour.
- **Concise Technical and Non-Technical Report** - overlaying the severity of each issue based on probability and potential impact to your environment and providing a view of short and long-term steps to mitigate ransomware risk.

256-260 Old Street, London, EC1V 9DD
t. +44 (0) 20 7749 7949 | e. sales@autodata.co.uk