COGNISYS
Smarter Cyber Security

Lost or Stolen Device Assessment

Mobile devices have proliferated since the start of the pandemic. Ensure you're not introducing additional risk alongside improved mobility.

When these devices are lost or stolen, it is vital that this cannot present a risk of data loss or unauthorised access to your network and data.

This service is a test to determine how much information can be gained from a lost device.

This ranges from almost nothing, which is unusual for laptops in particular, right up to all the information held locally, including details to achieve remote access to a company's internal infrastructure.

01422 416 000
sales@cognisys.co.uk
cognisys.co.uk

Continued overleaf...

A Lost or Stolen Device Assessment is usually based on everything in a typical laptop bag, including all the information that would be found alongside the laptop.

The scope is something that can be discussed over a review call and tailored to each client's requirements.

The best test is to simulate a real-world scenario, rather than to analyse a laptop that has been separated from its owner, had its post-it notes removed, notebooks retained and anything else which would aid an attacker in trying to gain access to the device, network and data.

Smartphones and tablets usually present less risk than a laptop if properly secured but Cognisys check that the right configurations are in place.

Analysis and Exploitation

The assessment commences, analysing the findings and attempts made, where safe and permitted, to exploit any vulnerabilities discovered.

If access is gained to the device, attempts may be made to access key systems on the internal network, over a VPN or any other discovered remote access gateway, using stored credentials.

Overview

The following are assessed in this exercise:

- Insecure storage or recording of passwords.
- Cached or unlocked credentials.
- Missing security patches.
- Boot process analysis.
- Device/disk encryption.
- Password brute force attack/weak password policies.
- Sensitive data disclosure.
- Information leakage.
- Local security policy circumvention.
- Multi-Factor Authentication (MFA).
- Mobile Device Management (MDM).

Report

Cognisys presents its findings in a comprehensive yet simple report format.

This typically comprises: an executive summary, methodology, technical findings, and prioritised recommendations for remediation.

01422 416 000
sales@cognisys.co.uk
cognisys.co.uk