At Thales we recognise that everything in cyber space is under threat from attack. Stored data, networks and data transfer systems are all high risk targets and the results from attack can be devastating to both business and the individual.

To counteract this threat we have developed a range of vulnerability assessment techniques designed to help reduce the impact of these threats and maintain the integrity of systems and data.

In our specialist, and accredited, Cyber Centre we can recreate a network environment in order to carry out rigorous testing and analysis to establish the level of security risk and then develop solutions to overcome these threats.

Thales - protecting your networks, data and business assets
Customer Requirement

Undertake a vulnerability assessment of a control network for a UK utility company.

The Process

Thales identified the business assets that were core targets and most vulnerable to attack.

VA techniques were employed to perform an assessment of active vulnerabilities.

The Findings

Thales identified that whilst the configuration of the business assets were secure, connected network infrastructure had vulnerabilities which exposed the critical business assets to attack.

Vulnerabilities were identified in:

- Use of default passwords and usernames for ‘non-critical’ components that provided a path for attack to critical assets
- Missing patches
- Unprotected web pages to printer system, enabling interception
- Remote login pages available with minimal security

Recommendations

Thales provided recommendations that enabled the company to:

- Immediately resolve the identified vulnerabilities, by changing configurations of components
- Improve their processes and procedures
- Provide awareness for the staff to help the company undertake regular periodic testing of critical business assets and connected systems
- Recommendations for separating critical and non-critical networks with no impact to the business operations

Key Customer Benefits

This service provided the following benefits to the customer:

- For minimal cost the customer gained increased network resilience without any interruption or impact to their business operations. The increased resilience reduced the risk of disruption to the utility supply hence reducing the risk of fines from regulators
- Employees were made aware of cyber considerations and how to perform internal analysis, thus reducing the risk of future upgrades causing a vulnerability
- Increased awareness of cyber security for employees

For more information contact us at:
cyber@uk.thalesgroup.com