Secure Backup Review

Organisations are increasingly being targeted with ransomware and malware attacks designed to gain access to backup environments and encrypt the backup data as a precursor to a wider-scale ransomware attack. This places utmost importance on implementing a robust backup solution that can resist targeted cyber-attacks and to allow organisations to recover from an attack when needed.

MTI's Secure Backup Review will assess your existing backup and recovery provision and highlight gaps between that and NCSC guidelines. The service includes a workshop, data discovery and output report.

The report covers any gap analysis vs NCSC guidelines, high level architecture if required and other recommendations.

> "Just to thank MTI for conducting a Secure Backup Review at Barnet Council with the purpose of assessing the existing backup and recovery solution and its level of alignment with NCSC guidelines. Your expert technical team performed a comprehensive review of our backup solution and offered recommendations to make the backup solution even more secure and compliant with NCSC guidelines. I would highly recommend your company to others and look forward to working with you on many more security related items in the future."
>
> **Paul Williams**
> IT Security Compliance Manager
> Barnet Council

The Service

The review starts with a workshop to understand the existing environment, operations and policies and gather the relevant information to provide guidance on any recommended remediation.

The workshop seeks to:
- Identify key personnel involved in backup and recovery operations to understand the current environment
- Understand any shortcomings, or issues with the current backup process
- Perform discovery work to capture all relevant client systems (where required)
- Discuss changes and potential mitigation of cyber threats and the recovery of backup data.
- Recommend technical remediation and improvements to the current backup function in alignment with NCSC guidelines

The output of the workshop will be a gap analysis vs NCSC guidelines and recommendations with rough costs for technical remediation where applicable.

Discovery

MTI will conduct a discovery exercise (an active scan against the environment to identify live hosts and volume of data) to obtain data that guarantees all critical systems are covered in the existing backup design.

Discovery Scans
The discovery scans can be carried out over a VPN or onsite. The non-invasive scan is designed to locate servers and establish the operating system.

MTI will conduct subnet discovery scans to identify:
- Host name and IP address of all live hosts
- Operating System type
- Disk size of all installed disks
- Consumed data capacity / volume of data to be backed up

The output of the discovery scan is a full asset list of hosts that need to be included in the backup program, along with the volume of data that will be backed up.

Typically, a five-day continuous effort discovery scan delivery either on-site or via a jump box. MTI can commence delivery as soon as access to the network is obtained.

Contact MTI
T: +44 (0) 1483 520 200
E: ukmarketing@mti.com
W: mti.com

Workshop

MTI will work with you to ascertain whether the current backup and recovery function is suitable for requirements.

The 2 hour workshop reviews:
- The type and features of the controlling backup software
- The current backup software and architecture
- Front-end data volume amount across geographical sites
- Estimated daily rates of change and Full/Incremental policy
- The data retention period for daily, weekly, monthly and yearly backups
- What data (if any) is off-line
- Future compound annual growth rate
- Data types to determine de-duplication and compression
- Total server count and mix between virtual and physical
- Server OS types and any hot-backup modules for databases
- Application types i.e. MS SQL, Oracle etc.
- Any shortfall in coverage of the current backup system to backup clients
- Any issues with the current backup environment
- What the critical data volume and servers are for a recovery operation
- Current 3-2-1 Backup conformity

Security Elements to be discussed:
- How do users administrate backups
- Network segregation
- Antivirus deployments
- Access Management solutions
- Logging and Alerting

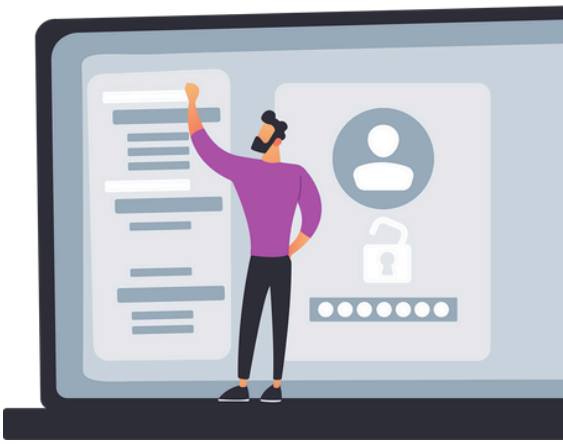
Output

The output of the entire workshop will be a high-level architectural design with indicative costs for a backup solution that can be implemented in line with, or as close as possible budget depending, NCSC's guidelines for a secure backup solution.

Deliverables

A report detailing the customer's conformity to:

- 3-copies of their backup data
- 2-copies of backup data on different media
- 1-copy of their backup data offline or immutable and off-site
- The segregation of access control via a privilege access management system
- The correlation and notification of security events relevant to the backup environment
- Vulnerabilities due to non-support operating systems
- Issues which deviate from industry best practices



Outcomes & Benefits

By undertaking this service, businesses will:

Ensure that their backup environments conforms to the NCSC guidelines

Mitigate the risk of malware and ransomware attacks

Ensure backup schedules and retentions follow best practices

Get technical remediation or solutions for issues uncovered in the assessment

By leveraging MTI's Secure Backup Review service as a foundation, businesses can gain valuable insights into their data protection posture and identify opportunities to enhance cyber resilience with solutions like Dell's DPS. This integrated approach not only mitigates the risk of data loss or breaches but also enables businesses to proactively defend against evolving cyber threats and regulatory requirements.

Contact MTI
T: +44 (0) 1483 520 200
E: ukmarketing@mti.com
W: mti.com