Case Study

Implementing robust cyber security measures after cyber attack left a school vulnerable

On April 7, 2021, Lady Eleanor Holles School faced a **severe cyber security breach**, where attackers infiltrated the school's systems, compromising the Veeam Backup Server and subsequently gaining access to the VMware Server administration.

This breach resulted in the **deletion of crucial virtual machines** (VMs), rendering them irretrievable. The attackers escalated their actions by **wiping the first-level backups** on the Veeam server, **accompanied by a ransom message**. Subsequently, they targeted QNAP second-level backups in the Junior School, **encrypting a VM** (a remote desktop server) and leaving **another ransom message in the VM server administration**. Adding to the chaos, malware rendered school workstations inoperable, with **ransom demands appearing on printers.**

How did it happen?

The attackers exploited an **outdated RM network administrator password** that had lingered for four years. This password, known to former IT staff, could have been acquired through hacking into web services, utilising the same password, or deploying a key logger into a workstation via a malware attachment.

WDigest credential harvesting was identified as one of the techniques used on the Veeam backup server whereby WDigest stores clear-text credentials in memory, leaving them vulnerable to being stolen.

Immediate actions

Swift measures were implemented, including an immediate change of all administrator passwords and the introduction of separate passwords for different systems to eliminate a single point of compromise.

The Veeam backup server underwent reconstruction for recovery, and most VMs were restored from a **recently installed CT cloud backup service**.

Each VM underwent meticulous virus scanning, with necessary Windows updates applied before reconnection to the network.

Comprehensive cyber security protection for the future

Protective measures included **Microsoft 365 Advanced Threat Protection** for comprehensive protection against various threats, as well as anti-virus software deployed on all new network servers and workstations. The school had both first and second-level backups, supplemented by **CT Secure Cloud Backup which was, fortunately, installed a week prior to the attack.**

Following on from this event, the school implemented key measures for a more **robust security system:**

Unique passwords: Implementing distinct passwords for different systems.

Administrator account usage: Instructing IT staff not use the administrator account unless necessary.

Password renewals: Enforcing 90-day administrator password renewals for all accounts.

Air-gapped backups: Utilising air-gapped disk caddy backups disconnected from the network.

Cloud backup maintenance: Maintaining cloud backup services with sufficient capacity for all VMs.
W

Security best practices: Adhering to cyber security best practices for remote desktop usage.

Prompt security updates: Ensuring all security updates are promptly applied.

Director of IT Services at LEH School, reflected on the incident

While first and second-level backups were historically deemed sufficient, evolving attack strategies, such as the complete destruction of online accessible backups, exposed vulnerabilities. The recovered VMs from the old RM network revealed critical issues like the absence of anti-virus software, disabled firewalls, and unrestricted administration access via remote desktop.

Martin Taylor
Director of IT Services,
Lady Eleanor Holles School

LEH
LADY ELEANOR HOLLES

Is your school in need of a robust cyber security strategy?

Speak to a member of the team today.

T | 01246 266 130
E | info@ct.uk

ct.uk