Digital Resiliency and Cyber Safety at Bengeo Primary School

School Server Configuration

The school uses a physical server running Microsoft Server and two virtual servers running under ESXi. The physical server is BIOS password protected and the access to the actual ESXi host is password protected as well. Physical access to the host is restricted behind a locked door. Each individual virtual server is password protected using passwords unique to the school and the servers are not accessible externally due to firewall and geofencing restrictions.

Virtual servers are part of a Microsoft domain and are kept up-to-date with Microsoft security patches and updates which keeps them at the highest current security level provided by Microsoft as time moves forward. Both virtual servers at the school are protected by Acronis Cyber Protect for antivirus and antimalware, as long as live intrusion tracking and additional backup security. Access to data on the server is controlled via NTFS permissions. These are applied in a way that allow access, based on the user's role. The default is to be more restrictive and allow access as authorised by school leadership.

Remote Server Management

The server uses a Dell iDRAC management portal for out of band management. Connection requires SSL and a school specific password is required for access.

Staff Passwords

Staff passwords are required to meet Microsoft password complexity standards. Passwords are not required to be changed periodically, in accordance with best practice guidance from GCHQ and Microsoft. Password complexity is enforced on the schools Office 365 domain as well, this ensures that all credentials used are GDPR compliant and secure.

Support Remote Access

IT support staff gain remote access to the school's network through Senso. Access to Senso is determined by a user email, a GDPR compliant password and multifactor authentication code. Each support member of staff has an individual password protected login. Senso secures and encrypts the connection using the highest level of mutually available set of protocols. (SSL or TLS and AES).

Remote Desktop Server

The school has a Remote Desktop Server to allow staff to remotely access data in a more secure method. This places all of the schools internal data behind a GDPR compliant password wall. Remote access to this server is via Microsoft's RDP protocol, secured by an RDP Gateway. The RDP Gateway uses an SSL certificate specific to the school. Access to the Remote Desktop Server is controlled by domain group membership and requires the user's domain credentials to be used. Sessions are locked down to prevent copy/paste and file transfer between the remote host and client machines, meaning that at no point does any school data come into contact with any external devices.

Onsite Backup

The school uses Microsoft's Windows Server Backup technology. The destination is a NAS unit located on site in a different physical location from the server. The NAS unit is connected via an iSCSI connection

authenticated through CHAP, using a school specific password. Access to the NAS unit management portal is through a school specific password. Backups run daily and are checked on a weekly basis during site visits and any issues or failures are investigated as a matter of urgency.

Offsite Backup

To augment the school's onsite backup, critical data is also backed up to the cloud. Data is stored securely using Acronis Cloud Backup.

Backups to the off-site location are automated. Manual tasks require a school specific password to access the console.

Backups are reported to the help desk and schools IT consultant, they are also manually checked on a weekly basis.

School Email

The school uses Microsoft 365 for email. Accounts are provisioned manually, and passwords are subject to Microsoft complexity requirements. Passwords do not expire, in accordance with best practice guidance from GCHQ and Microsoft. Accounts of noted concern, such as the Head Teachers account or the School Business Manager's account require multifactor authentication for access. This will be rolled out to all staff moving forward. SMTP, IMAP and POP3 protocols are disabled by default, forcing connections by the more secure ActiveSync method.

We scan the email system daily for a number of security indicators, including suspicious geographical logins, unauthorised protocol use, forwarding to external accounts and inactive accounts. Notifications are also set up for a number of these elements to assist in a proactive approach to email security.

System Updates

The school uses WSUS. This is carried out at weekly intervals to ensure that Windows or other operating systems are current and up-to-date with the latest and appropriate vulnerability protection. At less frequent intervals, but at least annually, major OS updates and other devices such as switches will have firmware updates to enhance data security.