Stadt Bergisch Gladbach
Der Bürgermeister
Federführender Fachbereich
Bildung, Kultur, Schule, Sport

Mitteilungsvorlage

Drucksachen-Nr. 0072/2025
öffentlich

Gremium	Sitzungsdatum	Art der Behandlung
Ausschuss für Schule und Gebäudewirtschaft	13.02.2025	zur Kenntnis

Tagesordnungspunkt

Erweiterte Informationen bezüglich der Anschaffung eines Virenschutzes für die Schulumgebung in Bergisch Gladbach

Finanzielle Auswirkungen:

	keine Auswirkungen:	Mehrerträge:		Mehraufwendungen:	
		lfd. Jahr	Folgejahre	lfd. Jahr	Folgejahre
konsumtiv:	X				
investiv:	X				
planmäßig:	X				
außerplanmäßig:	X				

Inhalt der Mitteilung:

Wie der Ausschuss für Schule und Gebäudewirtschaft in der letzten Sitzung gefordert hat, legt die IT-Schulverwaltung hier detailliertere Informationen bezüglich des anzuschaffenden Virenschutzes vor.

Die IT-Schulverwaltung betreibt momentan Hardwareserver sowie virtuelle Maschinen an den Standorten der weiterführenden Schulen sowie in Ihrem Rechenzentrum auf dem Zandersgelände.
Diese teilen sich wie folgt auf:
Hardware-Server am Standort Zanders:

- Proxmox01
- Proxmox02
- ProxmoxDMZ
- NextCloud01
- NextCloudBackup
- BackupServer
- Domaincontroller01

Virtuelle Maschinen am Standort Zanders:

- Domaincontroller02
- Nagios
- Filesystem
- Netbox
- Mailstore
- TrackIT
- WSUS (intern & extern)
- Hausmeisterserver
- FTP
- sFTP
- Datenbank
- FreeRadius
- openLDAP
- Wiki

Diese Hardware-Server und virtuellen Maschinen stellen für die IT-Schulverwaltung, sowie für die Schulen der Stadt Bergisch Gladbach folgende Dienste bereit:

- DHCP – Dienste
- LDAP – Dienste
- Domaincontroller
    - Intern

- NextCloud
    - Interne Nutzung
    - Externe Nutzung
- Datensicherung (Backup)
    - Backup interner Systeme
    - Backup der Schulsysteme
    - Backup von SchilD (verschlüsselt)
- Inventarisierungs– & Ticketsoftware
- Monitoring für die Server und Netzwerkgeräte

    - Interne Hardware/VMs
    - Hardware/VMs an den Schulstandorten
- Mailstore (Datensicherung E-Mailverkehr)
- WSUS – Dienste
    - Intern für Server & Clients
    - Extern für Server & Clients
- Dateiablage
    - Interne Dateiablage für Schul-IT
- Hausmeister Domänencontroller
    - Anmeldung über VPN
    - Geplant für alle Schulhausmeister
- FreeRadius
    - Zentrale Authentifizierung (in Planung)
- Zentrale Datenbank für einzelne Anwendungen
- Internes Wiki
- FTP-/ sFTP Server (Datensicherung Schild für die Schulen)
    - Wird über VPN durchgeführt

Des Weiteren betreibt die IT-Schulverwaltung jeweils einen Hardwareserver an den Standorten der weiterführenden Schulen. Hinzu kommen Hardware-Server an der GGS Bensberg und der GGS Heidkamp.
Auf diesen Servern werden mehrere virtuelle Maschinen betrieben, die unter anderem folgende Dienste bereitstellen:

- Backup in das Rechenzentrum der IT-Schulverwaltung
- DHCP
- Druckserver
- Active Directory
- SchILD (zentrale Datenbank)
- NPS (Radiusauthentifizierung in den Schulen)

Auf den virtuellen Maschinen für den Dienstleister, momentan NetCologne IT Services, wird das Identitiy Management sowie die Schulserverlösung UCS@School betrieben.

Insgesamt müssen 14 Hardwareserver sowie 27 virtuelle Maschinen lizenziert werden.
Hinzu kommen die Client-Geräte welche sich wie folgt aufteilen:

- 35 Computer für die Schulhausmeister.
- 183 Computer in den Sekretariaten der Schulen.
- 1053 Computer, welche in für den Unterricht genutzt werden.
- 398 Lehrerendgeräte, in den weiterführenden Schulen (lizenztechnisch bedingt).

Weiterhin wird der Virenschutz mit einer Laufzeit von drei Jahren ausgeschrieben. Die Gesamtsumme deckt die vollständige Laufzeit ab.
Nach Beauftragung der Dienstleistung ist folgender Ablauf geplant:

- Onboarding-Prozess
    - Aktivierung der Lizenzen sowie Übermittlung der MDR Kontaktdaten
    - Anstoßen des Onboarding-Prozesses durch Bestätigungsmail
    - Kickoff-Call mit Dienstleister
    - Workshop zur Einführung in Arbeit mit MDR
    - Workshop & Hilfestellung bei Konfigurationen des Virenschutzes & möglicher Integrationen

    - Schulung des Personals im Umgang mit XDR & den bereitgestellten Funktionen/Werkzeugen
    - Review nach 90 Tagen mit MDR Team des Dienstleisters zur Evaluation & Pen-Testing
    - Transition in den normalen MDR Betrieb
- Account Health Checks
    - Überprüfung der gesetzten Einstellungen & Richtlinien
- Erkennen von Cyberangriffen über das Monitoring des Software-Agenten auf Servern & Clients
- „Leadless Threathunts“
    - präventive Suche nach bekannten Sicherheitslücken/Bedrohungen
- Abhängig vom festgelegten Arbeitsmodus Reaktion auf gefundene Bedrohungen/Angriffe
    - Eigenständige Reaktion auf Angriff
    - Quarantäne des Systems
    - Abmelden von Benutzern
    - Sperrung von Benutzern
    - Sperrung von IP-Adressen
    - Beendigung von Prozessen & Diensten
    - Entfernung bösartiger Artefakte
    - Ursachenanalyse
    - Identifizierung kompromittierter Systeme
    - Unterstützung bei der Behebung
    - Analyse des Angreiferverhaltens/ der Bedrohung
- Wöchentliche und monatliche Berichte über die Aktivitäten des MDR Teams