

BMBWF - Präs/16 (IT-Didaktik)

Mag. Martin Bauer, MSc
Sachbearbeiter

martin.bauer@bmbwf.gv.at
+43 1 531 20-3538
Minoritenplatz 5, 1010 Wien

Antwortschreiben bitte unter Anführung der
Geschäftszahl.

Erght an:

Alle Bildungsdirektionen

Geschäftszahl: 2024-0.507.870

Rundschreiben

Titel:	Rundschreiben: Neuerungen im Bereich IT-Standardisierung sowie IT-Beschaffungen; Vorgehen bei Security-Vorfall
Rundschreiben Nr.:	29/2024
Sachgebiet:	Budget- und Rechnungswesen; Ressourcenbewirtschaftung; Schulerrichtung, -einrichtung, -ausstattung, -gebäudebetrieb
Verteilerkreis:	alle Bundesschulen
Personenkreis:	Direktor/innen und Verwaltungspersonal
Geltung:	unbefristet
Rechtsgrundlage:	IKT-Schulverordnung
Kernaussagen/Ziele:	Bildungsdirektion wirken bei Standardisierung und Dokumentation im IT-Bereich mit; Bildungsdirektionen sind bei bestimmten IT-Beschaffungen einzubinden; Standardisierter Ablauf bei Security-Vorfall
Ort der Veröffentlichung:	Rundschreibendatenbank des BMBWF
Veröffentlichende Stelle:	BMBWF

Um die **IT-Sicherheit an Schulstandorten** zu erhöhen und auf **IT-Sicherheitsvorfälle** vorbereitet zu sein, werden Maßnahmen in unterschiedlichen Bereichen angeordnet. Unter Mitwirkung der für die IT-Systembetreuung zuständigen Referate an den Bildungsdirektionen sind an den Bundesschulen die im folgenden beschriebenen Maßnahmen umzusetzen. Ergänzende Präzisierungen sind außerdem in den beiden Anhängen sowie online unter bmbwf.gv.at/it-standardisierung zu finden. Nähere Konkretisierungen und Vorlagen werden durch die Bildungsdirektionen vorgegeben.

Standardisierung der bestehenden IT-Infrastruktur

Für die Unterstützung durch die IT-Systembetreuung hat die Schule sicherzustellen, dass der Betrieb der für den Core-Infrastruktur-Bereich eingesetzten Komponenten (insbesondere Server, Firewalls, Switches) durch geeignete Maßnahmen (z.B. Garantie/Gewährleistung, Service- bzw. Wartungsvertrag, redundante Komponenten) gewährleistet wird.

Vorgaben der Bildungsdirektionen zur Konfiguration der IT-Systeme (insbesondere Server, Firewalls, Switches, Accesspoints, Azure Mandant) sind im Sinne bundesweit einheitlicher Standards jedenfalls einzuhalten.

Dokumentation der IT-Infrastruktur

Um bei Störungen und IT-Sicherheitsvorfällen möglichst rasch und umfassend reagieren zu können, ist es erforderlich, dass alle wesentlichen Bereiche der IT-Infrastruktur ausreichend dokumentiert sind.

Zu den zu dokumentierenden Bereichen gehören vor allem:

- **Dokumentation aller Server, Backupsystem und Netzwerkkomponenten** wie z.B. IP, OS-Version, Patch-Konzept, Zugangsdaten, Location.
- **Dokumentation aller VLANs** (IPs, GW, Mask, ID), **Externer IP-Adressen**, deren Verwendung und deren Absicherung.
- **Dokumentation zur Verfügbarkeit der Zugangsdaten externer Services** wie z.B. ISP, Website, Lernplattformen, Webuntis, Lizenzen und Lizenzportale.

Über Zugriff auf die Dokumentation müssen IT-Manager/innen am Standort, je nach Zuständigkeit bzw. Arbeitsplatzbeschreibung die IT-Systembetreuer/innen und im Anlassfall die Schulleitung verfügen. Die Vollständigkeit der Dokumentation ist periodisch zu überprüfen bzw. zu aktualisieren. **Auf Verlangen ist die Dokumentation der Bildungsdirektion oder vom BMBWF dafür autorisierten Personen auszuhändigen und zentral bereitzustellen.**

Vorliegen eines IT-Sicherheitskonzepts

Bestandteil einer funktionalen Dokumentation ist auch ein Sicherheitskonzept, das für den Fall eines IT-Sicherheitsvorfalls dabei hilft, den Schaden zu minimieren. Sollte ein solches Sicherheitskonzept noch nicht vorliegen, sollte dieses ehestmöglich und gegebenenfalls **unter Mitwirkung der Bildungsdirektion** erstellt werden.

Folgende Bereiche sollten durch das IT-Sicherheitskonzept abgedeckt sein:

- **Multi-Faktor-Authentifizierung (MFA)** zumindest für alle privilegierten Zugänge, die aus dem öffentlichen Netz erreichbar sind.
- Mittels Hardware-**Firewall und Webfilter** ist der Schutz vor Schadsoftware, Bedrohungen und unsachgemäße Inhalte bestmöglich zu gewährleisten.
- Eine **Datensicherung** jener Systeme, welche für den Schulalltag erforderlich sind, hat am jeweiligen Standort zu erfolgen.

Neue Vorgaben bei Beschaffungen im Bereich IT-Infrastruktur

Die IT-Infrastruktur und Vorgaben zur IT-Sicherheit sind vom pädagogischen Auftrag separat zu betrachten. Deren technische Ausgestaltung liegt im Entscheidungsbereich des Schulerhalters.

Vorgaben der Bildungsdirektionen zur Konzeption und Konfiguration der Architektur und Topologie des Systems sind im Sinne der Umsetzung österreichweit einheitlicher Mindeststandards jedenfalls einzuhalten. Dies vereinfacht im Fall eines IT-Sicherheitsvorfalls die notwendigen Maßnahmen zur Schadensabwehr.

Insbesondere für die folgenden Beschaffungen ist die **Zustimmung des für die IT-Systembetreuung zuständigen Referats** gemäß dessen Vorgaben einzuholen:

- **Serverhardware sowie USV-Anlagen**
- **Netzwerkkomponenten** wie Switches, Accesspoints, Firewalls
- **Infrastructure as a Service (IaaS)**
- über den Leistungszeitraum eines Jahres hinausgehende **Werkverträge zur Betreuung der IT-Infrastruktur** (z.B. Säule-3-Budget) sowie über ein Jahr hinausgehende **IT-Dienstleistungsverträge**, die mit Unternehmen geschlossen werden, wie z.B. insbesondere Providerdienstleistungen oder Wartungsverträge.

Kleinbeschaffungen, wie etwa Tastaturen oder Monitore erfordern nicht die Einbeziehung der Bildungsdirektion.

Vorgehensweise bei IT-Security-Vorfall

Ein Sicherheitsvorfall liegt vor, wenn unautorisierte Zugriff auf ein IT-System erfolgte oder die Informationssicherheit (also Vertraulichkeit, Verfügbarkeit und/oder Integrität) von Daten, Services, Systemen oder Anwendungen beeinträchtigt ist.

In Falle eines solchen Sicherheitsvorfalls sind jedenfalls das **für die IT-Systembetreuung zuständige Referat und der/die Datenschutzbeauftragte umgehend** zu informieren.

Wien, 13. Oktober 2024
Für den Bundesminister:
Mag. Martin Netzer, MBA

Beilagen:

- Vorgaben zur IT-Dokumentation
- Vorgaben zum IT-Sicherheitskonzept

Elektronisch gefertigt