Kanton Zürich
Bildungsdirektion
Mittelschul- und Berufsbildungsamt
Digital Service Center Sek II

Kontakt: Bettina Irnhauser, Verantwortliche für Informationssicherheit und Datenschutz Sek II, Ausstellungsstrasse 80, 8090 Zürich
bettina.irnhauser@mba.zh.ch

16. Mai 2025

Personenbezogene Auswertung von Logdaten - Ablauf und Vorgehen seitens DSC Sek II

Bevor es zu einer personenbezogenen Auswertung von Logdaten kommt, muss ein Ereignis stattgefunden haben. Ein Ereignis kann z.B. eine Meldung vom System zu einer Unregelmässigkeit, oder ein Verdachtsfall durch z.B. Meldung der Schulleitung via Ticket sein.

Mögliche Erkennung von Sicherheitsvorfällen beim DSC Sek II durch:

- Verdachtsfälle werden vom System gemeldet.
- Standardauswertung durch Routine Systemchecks.
- Informationen und Meldung zu Sicherheitsvorfall vom AFI an das DSC Sek II.
- Meldung der Schule via Ticket-System OTRS oder ServiceNow (neue IKT-Grundversorgung) zu einem möglichen Sicherheitsvorfalls (Verdachtsfall).

Je nach sicherheitskritischem Stand können Sofortmassnahmen, wie eine Isolation von einem PC/Laptop in die Wege geleitet werden. Sofortmassnahmen sind notwendig, wenn eine unmittelbare Gefahr für Personendaten, die Schule oder die Infrastruktur besteht.

Als nächster Schritt ist eine Analyse der erhaltenen Informationen und Daten durchzuführen. Bei einem Verdachtsfall wird folgendes Vorgehen seitens DSC Sek II gewählt.

- Abteilungsinterne Abstimmung im DSC Sek II für das weitere Vorgehen.
- Je nach Verdachtsfall, Einbezug der benötigten Bereiche und Fachspezialisten der Systeme z. B. Bereich Support und Operation, Application Service, …
- Dabei wird der Kreis der involvierten Personen möglichst klein gehalten.
- Analyse des genauen Sachverhalts inkl. Auslöser durch Spezialisten.
- Bei Bedarf personenbezogene Auswertung durchführen.

Nach einer allgemeinen Analyse ist die Notwendigkeit von personenbezogenen Auswertungen zu prüfen. Eine personenbezogene Auswertung wird erst in einem begründeten Verdachtsfall durchgeführt. Die Entscheidung wird situationsbedingt teamintern im DSC Sek II getroffen. Die betroffene Person wird über eine personenbezogene Auswertung vom DSC Sek II informiert. Es gilt die Unschuldsvermutung, solange das Gegenteil nicht bewiesen ist.

Die Schulleitungen werden nicht informiert, falls eine personenbezogene Auswertung einer Mitarbeiterin oder eines Mitarbeiters der Schule durchgeführt wird. Wenn sich der Verdacht erhärtet, wird die Schulleitung involviert. Eine Erhärtung des Verdachts tritt ein, wenn die Analysen z.B. eine Anstellungsrelevanz haben.

Falls ein erheblicher Schaden entsteht oder das Ereignis eine strafrechtliche Relevanz hat, wird das Mittelschul- und Berufsbildungsamt Strafanzeige erstatten.