Schul-IT

Sicherheit überdenken

[02.09.2015] Auch Schulen müssen sich der Gefahr von Cyber-Angriffen stellen. Nicht nur die eingesetzte Software sollte auf dem aktuellen Stand sein, empfiehlt der TÜV Rheinland.

„Bei der IT-Sicherheit sollten Schulen keine Kompromisse machen“, sagt Frank Melber, Experte für Netzwerksicherheit bei TÜV Rheinland. Denn wie das Unternehmen meldet, wächst auch in diesem Bereich die Zahl von Cyber-Angriffen. Schulnetze könnten aufgrund von Schwachstellen durch Botnetze beispielsweise für Propaganda-Zwecke gekapert werden. Ebenso sei denkbar, dass der Schul-Server lahmgelegt wird, um Abiturnoten zu manipulieren. „Schulen, die in Bezug auf Datenschutz und Datensicherheit compliancesicher unterwegs sein möchten, sollten sich auf den Fall professionell beraten lassen, wie sie ihr Netzwerk absichern können“, erklärt Melber. Die eingesetzte Software sollte stets auf dem aktuellen Stand sein. Gleiches gelte für Antivirus-Software-Lösungen. In beiden Fällen müssen laut dem TÜV Rheinland regelmäßig Updates erfolgen. Ebenfalls zu empfehlen sei der professionelle Umgang mit Passwörtern, am besten über einen Passwort-Manager mit einem Master-Kennwort. Auch das WLAN müsse systematisch abgesichert sein. Besteht der Verdacht, dass eine Schule gehackt wurde, sollte sie laut der Meldung professionelle Hilfe beim IT-Zentraldienstleister holen, der die Schulen des jeweiligen Bundeslandes betreut. Dieser wiederum könne sich auch an das Computer Security Incident Response Team des TÜV Rheinland wenden, das Hacker-Angriffe erkennt, stoppt und den Schaden so schnell wie möglich abwende.

(ve)

Stichwörter: Schul-IT, IT-Sicherheit, TÜV Rheinland