# Kriminelle publizieren sensitive Daten aus Schulen

*Erpresser haben das Schulnetzwerk des Kantons Basel-Stadt angegriffen und grosse Mengen an Informationen erbeutet*

DANIEL GERNY, LUKAS MÄDER, SIMON HUWILER

Noten von Schülerinnen und Schülern, Fotos von Ausflügen oder Vorbereitungen für Schullektionen: Solche Informationen aus dem Erziehungsdepartement (ED) des Kantons Basel-Stadt finden sich in den Daten, die die Erpressergruppe mit dem Namen Bianlian am Dienstagabend im Darknet veröffentlicht hat. «Es handelt sich hier um ein grösseres Leak, das vertrauliche und personenbezogene Daten beinhaltet», sagt der Cybersecurity-Experte Marc Ruef. Er hat die Datenstruktur einer groben Analyse unterzogen.

Das Erziehungsdepartement wird seit Wochen von der kriminellen Bande bedrängt. Bemerkt wurde der Angriff bereits Ende Januar, nachdem eine Geldforderung der Erpresser eingegangen war. Das Erziehungsdepartement reichte in der Folge Strafanzeige gegen Unbekannt ein und informierte das Nationale Zentrum für Cybersicherheit (NCSC) des Bundes. Auf die Lösegeldforderung ging das Departement nach eigenen Angaben nicht ein. Diese Aussage ist glaubwürdig, denn solche Erpressergruppen veröffentlichen die von ihnen erbeuteten Daten üblicherweise nur, wenn das Opfer kein Lösegeld bezahlt. Das ED hat die Öffentlichkeit am Mittwoch über die Veröffentlichung der Daten informiert.

*Wie viele Personen vom Datendiebstahl betroffen sind, ist derzeit noch unklar.* KARIN HOFER / NZZ

## E-Mail enthielt Schadsoftware

Brisant ist der Angriff nicht zuletzt deshalb, weil es den Kriminellen gelungen ist, auf die schulische IT-Infrastruktur eines ganzen Kantons zuzugreifen. Der Angriff betrifft nach Angaben des ED das System «EduBS», eine Arbeitsplattform für Lehrpersonen, Schülerinnen und Schüler im Kanton, die getrennt vom kantonalen Datennetz funktioniert.

Von der Veröffentlichung könnten theoretisch mehrere tausend Personen betroffen sein. Basel-Stadt verfügte 2021 über mehr als 3500 Lehrpersonen und rund 17 500 Schülerinnen und Schüler. Wie viele von ihnen tatsächlich betroffen sind, ist aber ebenso unklar wie die Antwort auf die Frage, welche und wie viele Daten wirklich heikel sind. Die Erpresser geben an, eine Datenmenge von 1,2 Terabyte veröffentlicht zu haben. «Die Kompromittierung ist weitreichend und entspricht den Möglichkeiten, die sich die professionalisierten Erpresserbanden erschlossen haben», sagt Ruef.

Die Daten werden derzeit von Spezialisten analysiert, wie Conradin Cramer, Vorsteher des Erziehungsdepartementes, am Mittwoch vor den Medien sagte. Die veröffentlichten Dokumente würden auch heikle Informationen von Lehrpersonen und Schülern enthalten. Laut Cramer könnten das etwa Schulnoten, Absenzen oder Berichte über Abklärungen von einzelnen Schülern sein. Das würden die Namen von Ordnern und Dateien zeigen. Die Daten selbst konnten noch nicht vollständig heruntergeladen werden. «Wir bedauern extrem, was passiert ist», sagte Cramer und sprach von einem höchst unerfreulichen Ereignis. Personen, deren Namen in den Daten auftauchten, würden aktiv informiert.

Bisher haben die Kriminellen 858 Zip-Archive veröffentlicht, wie im Darknet ersichtlich ist. Dabei entspricht eine Zip-Datei anscheinend einem Benutzeraccount des Schulnetzwerks. Die Pfadstrukturen deuten laut Aussagen von Ruef auf Mitarbeiter, Lehrpersonen und Schüler hin. Das ED bestätigt dies. Stichproben zeigten, dass wohl auch Arbeitsplatzrechner kompromittiert worden sind. Die IT-Fachleute des ED gehen dagegen eher davon aus, dass keine solchen Rechner betroffen sind.

Die Kriminellen hätten sich vermutlich über eine E-Mail, die um den Jahreswechsel herum verschickt worden sei und eine Schadsoftware enthalten habe, Zugang zum «EduBS»-Netzwerk verschaffen können, sagte Regierungsrat Cramer. Gewisse technische Fehler hätten den Angriff ermöglicht. In die IT-Systeme der kantonalen Verwaltung konnten sie offenbar nicht eindringen, weil es keine direkte Verbindung gab. Die Rechner des «EduBS»-Netzwerks wurden nicht verschlüsselt.

## Schokoladehersteller attackiert

Der Angriff auf das Basler Erziehungsdepartement ist kein Einzelfall: Der Einsatz von sogenannter Ransomware hat in den letzten Jahren einen grossen Aufschwung erlebt und ist zu einem Milliardengeschäft geworden. Es lässt sich leicht skalieren und birgt für die Cyberkriminellen kaum Risiken. Die Ransomware-Gruppen arbeiten professionell und sind international vernetzt. Es handelt sich um eine Form der organisierten Kriminalität. Die NZZ und CH Media sind in den letzten Wochen ebenfalls Opfer eines Ransomware-Angriffes geworden.

Üblicherweise versuchen solche kriminellen Erpresserbanden die IT-Systeme der Opfer zu verschlüsseln, um sie unbrauchbar zu machen. Für die Entschlüsselung fordern diese Ransomware-Gruppen dann ein Lösegeld (auf Englisch «ransom»). Häufig kopieren die Kriminellen zuvor noch Daten des Opfers, um mit deren Veröffentlichung zu drohen und so zusätzlichen Druck im Hinblick auf eine Lösegeldzahlung aufzubauen.

Die Gruppe Bianlian, die hinter dem Angriff auf das Basler Schulnetzwerk steht, ist seit mindestens Sommer 2022 aktiv und wendet für ihre Erpressungen ebenfalls eine Kombination von Verschlüsselung und Datendiebstahl an. Zu ihren Opfern gehören relativ häufig Schulen und Spitäler, die laut der Sicherheitsfirma Redacted bis im März rund ein Viertel aller Angriffsziele ausmachten. Ein prominentes Schweizer Opfer der Gruppe Bianlian war der Schokoladenhersteller Läderach im letzten September.

> «Es handelt sich hier um ein grösseres Leak, das vertrauliche und personenbezogene Daten beinhaltet.»
>
> **Marc Ruef**
> Cybersecurity-Experte

Interessanterweise hat Bianlian in den letzten Wochen und Monaten die Vorgehensweise verändert. Die Gruppe verzichtet laut Redacted zunehmend darauf, die Daten ihrer Opfer zu verschlüsseln, und versucht stattdessen, ihre Opfer einzig mit der Drohung zu erpressen, brisante Daten zu veröffentlichen.

Die technischen Stärken der kriminellen Gruppe liegen laut Redacted eher beim Eindringen in IT-Systeme und weniger bei der Verschlüsselung der Daten und der Erpressung. Das könnte ein Grund gewesen sein, warum beim Angriff auf das Basler Schulnetzwerk keine Rechner verschlüsselt wurden.