«Gehen von vielen Betroffnen aus»

Kanton kann das Ausmass des grossen Hackerangriffs zurzeit noch nicht vollständig abschätzen.

Jonas Hoskyn und Daniel Schurter (watson)

Erziehungsdirektor Conradin Cramer und die IT-Verantwortlichen seines Departements informierten zum Hackerangriff. Bild: Kenneth Nars

Stundenpläne, Zeugnisse, Absenzen, aber auch hochsensible Daten wie Abklärungsberichte: Noch ist erst ansatzweise geklärt, was der grosse Datensatz umfasst, den Cyberkriminelle vom Basler Erziehungsdepartement erbeutet und nach einem gescheiterten Erpressungsversuch nun veröffentlicht haben. Klar ist aber: Es sind auch vertrauliche Daten darunter. Und: «Wir gehen davon aus, dass eine grosse Zahl von Personen im Kanton Basel-Stadt betroffen ist», wie Erziehungsdirektor Conradin Cramer in einer ersten Einschätzung sagte.

1,2 Terabyte aufgeteilt in 858 Pakete haben die Erpresser im Darknet, also dem versteckten Teil des Internets, veröffentlicht. Zutritt verschafften sich die Cyberkriminellen vermutlich mit der sogenannten Phishing-Methode, bei der mit einem präparierten E-Mail versucht wird, Zugangsdaten zu erschleichen. Aktuell gehen die Verantwortlichen beim Erziehungsdepartement davon aus, dass die Täter via einen Computer, der sowohl privat als auch geschäftlich genutzt wird, eingedrungen sind. Solche benutzen beispielsweise Lehrpersonen.

Im schlimmsten Fall sind 858 Computer betroffen

Dadurch hatten die Hacker Zugriff auf das Netzwerk «eduBS» und breiteten sich dort via Sicherheitslücken aus. Das Netzwerk steht den Basler Lehrpersonen und Schülerinnen und Schülern zur Verfügung und ist vom kantonalen Datennetz isoliert. Entsprechend ist offenbar nur das Erziehungsdepartement vom Hackerangriff betroffen.

Die betroffenen Arbeitsgeräte werden auf dem Server gespiegelt, also als Kopie gespeichert. Diese Daten konnten die Hacker offenbar abgreifen. «Stichproben zeigen, dass hier die Desktop- und Datei-Ordner von einzelnen Personen erbeutet wurden», sagt IT-Sicherheitsexperte Marc Ruef. Pro Computer eine Zip-Datei: Im schlimmsten Fall würde das bedeuten, dass fast 900 Benutzer betroffen sind. Je nach Art der erbeuteten Dateien sind das ein Vielfaches an betroffenen Personen.

> «Wir wollen möglichst schnell informieren, sobald wir Genaueres wissen.»
>
> **Conradin Cramer**
> Erziehungsdirektor BS

Stattgefunden hat der Angriff vermutlich um die Weihnachtsferien. Bemerkt wurden die Hacker erst, als sie sich Ende Januar mit dem Erpresserschreiben beim Kanton gemeldet haben. Entsprechend muss man davon ausgehen, dass sie zu diesem Zeitpunkt ihre Möglichkeiten ausgeschöpft haben.

Hacker kontaktierten Cramer auf dem Handy

Recherchen zeigen, dass hinter dem Angriff die Hackergruppe «BianLian» steckt. Diese ist erstmals im Juli 2022 in Erscheinung getreten. Zu Beginn operierte die Bande mit einem zweistufigen Erpressungssystem. In einem ersten Schritt wurden Daten auf dem gehackten Server verschlüsselt und deren Entschlüsselung an eine Geldforderung geknüpft. Anschliessend drohte man mit der Veröffentlichung der erbeuteten Daten. «Sie spekulieren darauf, dass eine Veröffentlichung der Daten schmerzhaft genug sein wird, um eine Zahlung durch die Opfer zu erzwingen», sagt Ruef.

Bis im März wurden weltweit über 100 Angriffe der Gruppe bekannt, darunter auch einer beim Schokolade-Unternehmen Läderach. Anfang Jahr veröffentliche eine Cybersicherheitsfirma eine Entschlüsselungssoftware gegen «BianLian». Seither fokussiert sich die Gruppe auf die Erpressung durch Veröffentlichung.

Wie hoch die Forderungen gegenüber dem Erziehungsdepartement und damit dem Kanton Basel-Stadt waren, ist nicht bekannt. Klar ist: Eine Zahlung war nie ein Thema: «Es ist einheitliche Politik des Kantons, dass man sich nicht erpressbar macht», sagt Cramer. Auf Kontaktversuche habe die Gruppe nicht reagiert. Stattdessen erhielt Cramer einen Anruf aus Amerika und eine Whatsapp-Nachricht in englischer Sprache, übersetzt: «Weiss Ihr Vorsitzender, das Sie einen Datendiebstahl hatten?»

Das Erziehungsdepartement hat im Januar bei der Staatsanwaltschaft Anzeige gegen Unbekannt erstattet und weitere Behörden und Stellen informiert, darunter den Datenschutzbeauftragten des Kantons und das Nationale Zentrum für Cybersicherheit. Zu den Ermittlungen gibt die Staatsanwaltschaft wie üblich keine Auskunft, teilt aber mit, «dass sich der Angriff, bezogen auf die Datenmenge, im oberen Mittelfeld der uns bekannten Fälle in Basel-Stadt bewegt».

Gleichzeitig sind die Behörden am Analysieren, wer von dem Hackerangriff betroffen ist. Cramer sagt: «Wir wollen möglichst schnell informieren. Sobald wir Genaueres wissen, werden wir die betroffenen Personen direkt kontaktieren.»