Diese Daten wurden den Schulen gestohlen

Alles zum Hackerangriff auf Basel Am Dienstag haben Cyberkriminelle massenweise heikle Dokumente von Basler Lehrpersonen und Schülern ins Darknet gestellt. Die wichtigsten Fragen und Antworten.

Dina Sambar, Leif Simonsen, Julia Konstantinidis und **Simon Erlanger**

Immer mehr Institutionen, Gemeinden und Firmen sind Erpressungsversuchen durch Hackerangriffe ausgesetzt. Symbolfoto: AFP

— Wie sensibel sind die Daten, die gehackt wurden?
Thomas Wenk, Leiter Digitalisierung und Informatik beim Erziehungsdepartement (ED), geht davon aus, dass auch sensible Daten unter den gestohlenen Dateien sind. Wenn zum Beispiel ein Lehrer eine Gefährdungsmeldung zu einem Schüler an die Kesb gemacht und diese auf dem Home-Laufwerk des gehackten edubs.ch-Servers gespeichert hat, «ist dieses Dokument nun veröffentlicht worden». Gleiches gelte für möglicherweise sensible Dokumente, die etwa an Lehrer geschickt und abgelegt wurden, beispielsweise ein Bericht der Jugendstaatsanwaltschaft.

Die «Basler Zeitung» hat Einblick in das Verzeichnis der Dateien (nicht in die Dateien selbst). Geht man davon aus, dass die Dateinamen auf die Inhalte schliessen lassen, sind in den gehackten Informationen neben Schulmaterial, Zeugnissen und Lernberichten tatsächlich Dokumente zu Gefährdungsmeldungen zu finden. Auch persönliche Dokumente mit Namen wie Hypothekarvertrag oder Vorsorgeausweis sind auf der Liste.

Unter den Betroffenen sind laut dem ED vor allem Lehr- und Fachpersonen sowie Schülerinnen und Schüler.

— Wie gross ist die Gefahr, dass diese Daten bald für alle im Internet einsehbar sind und missbraucht werden?
Die Wahrscheinlichkeit sei gross, dass die Daten im Internet auftauchen oder missbraucht werden, sagt Martin Lutz, Cybersecurity-Experte beim Unternehmen Axians, das von Arlesheim aus weltweit in der Cybersicherheit tätig ist: «Dafür braucht es nur eine einzige Person weltweit, die diese Daten auf ihren Rechner lädt und dann im Internet veröffentlicht.» Da der Tor-Browser jedoch sehr langsam sei und die Datenmenge jeweils gross, werde dieser Vorgang schätzungsweise ein bis zwei Wochen dauern.

— Darf man die geklauten Daten des ED anschauen?
Eigentlich nicht. Allerdings handelt es sich juristisch um eine Grauzone. So dürfen Journalisten aufgrund des sogenannten Medienprivilegs solche Daten unter bestimmten Umständen eben doch lesen. Sonst wäre die publizistische Auswertung der Datenlecks von Wikileaks und Panama Papers nicht möglich gewesen. Ob Normalverbraucher die ED-Daten lesen dürfen, ist juristisch unklar. Klar ist aber: Sie dürfen diese weder kopieren noch herunterladen oder sonst irgendwie davon Gebrauch machen. Generell handelt es sich um einen Bereich des Datenschutzes, der noch der Rechtsprechung harrt.

— Wie geht das Erziehungsdepartement nun weiter vor?
Die betroffenen Personen werden vom ED direkt benachrichtig, sobald die Analysen zum Datendiebstahl fertig sind: «Sie werden die Möglichkeit erhalten, einzusehen, welche ihrer Daten sich nach aktuellem Kenntnisstand im Darknet befinden», schreibt das ED. Zudem wird eine Hotline aufgeschaltet, bei der sich besorgte Personen melden können. Bei der Anzahl der direkt betroffenen Personen handelt es sich laut Thomas Wenk um eine im sehr tiefen vierstelligen Bereich.

Man habe damit begonnen, die Dateien zu durchforsten, so Wenk. In seiner Abteilung sind seit dem Angriff rund zehn Personen regelmässig mit dem Fall beschäftigt. Die Direktbetroffenen könne man aufgrund der Dateinamen ermitteln. «Aus Datenschutzgründen öffnen wir die Dateien nicht.» Eruierbar seien daher nur Personen, deren Namen eindeutig in publizierten Verzeichnissen erscheinen. Dass man alle Dateien abschliessend ermitteln könne, ist laut Wenk unmöglich.

— Wie schützt sich das Erziehungsdepartement in Zukunft besser?
Der Angriff hat gemäss ED zu einem Zeitpunkt stattgefunden, in dem das Departement daran war, eine grundlegend neue zentrale IT-Infrastruktur aufzubauen. «Dieser Prozess konnte diesen Angriff noch nicht verhindern, da die neue Infrastruktur zu diesem Zeitpunkt noch nicht in Betrieb war», schreibt das ED. Der Aufbau des neuen Systems sei unmittelbar nach Bekanntwerden des Datenklaus im Januar beschleunigt worden, damit Angriffe künftig besser erkannt und verhindert werden könnten.

Doch auch mit dem besten System sei man nicht zu hundert Prozent vor Hackerangriffen gefeit. «Man muss damit leben und lernen, damit umzugehen», sagt der Leiter Digitalisierung und Informatik beim ED.

— Hat sich das ED richtig entschieden, kein Geld zu bezahlen?
Das Nationale Zentrum für Cybersicherheit (NCSC) im Eidgenössischen Finanzdepartement sagt, dass Basel-Stadt richtig reagiert habe: «Der Kanton hat die Strafverfolgungsbehörden miteinbezogen und kein Lösegeld bezahlt.» Das NCSC rät genau zu diesem Vorgehen. Die Veröffentlichung der Daten möge für Einzelne schlimm sein, sagt Martin Lutz: «Doch hätte das ED bezahlt, wäre die Schweiz als Angriffsziel noch interessanter geworden. Indem man die Zahlung verweigert, macht man das Geschäftsmodell dieser Hackergruppen kaputt.»

> **«Staatliche Stellen in der Schweiz sind in der Regel besser abgesichert als die meisten Unternehmen.»**
>
> **Martin Lutz**
> Cybersecurity-Experte

— Was können einzelne Betroffene jetzt tun?
«Ehrlich gesagt, fällt mir nichts ein, was man tun könnte», sagt Cybersecurity-Experte Lutz. Sind die Daten erst im Internet, sei es fast unmöglich, sie dort wieder herauszuholen.

— Hätte der Angriff verhindert werden können?
Martin Lutz fehlen die Informationen, um eine Beurteilung zu diesem Vorfall abzugeben: «Grundsätzlich können viele Angriffe verhindert werden.» Allerdings sei das äusserst schwierig. «Wenn die Hacker ein grösseres Budget und Zeit für den Angriff haben, ist die Wahrscheinlichkeit gross, dass sie das auch schaffen.»

— Wie sicher sind die anderen Daten, die beim Kanton gespeichert sind?
Der Chef der Basler Finanzkontrolle (Fiko), Daniel Dubois, sagt: «Die jüngsten Angriffe auf Medienhäuser und jetzt auf das Erziehungsdepartement zeigen: Heute ist es unerlässlich, in die IT-Sicherheit zu investieren.» Die Finanzkontrolle hat den Kanton mehrere Jahre für seine Nachlässigkeiten in diesem Bereich kritisiert. Im Tätigkeitsbericht von 2022 schreibt die Fiko: «Die Prüfung der Informatikprozesse ergab, dass die vorgegebenen Standardprozesse nicht eingehalten werden.» Auch fehle ein Monitoring in den Systemen, um Angriffe von Hackern sofort zu identifizieren, damit schnell darauf reagiert werden könne. Dubois hält der IT Basel-Stadt aber zugute, dass diesbezüglich «stetig Fortschritte» gemacht würden. Immerhin: Das nun gehackte Netzwerk des Erziehungsdepartements (Edubs) ist abgekoppelt von den anderen IT-Netzwerken des Kantons.

Für jenes Netzwerk, mit dem die Verwaltungsstellen arbeiten, wurde gemäss Mario Magnanelli, Leiter IT Basel-Stadt, ein Drei-Stufen-Schutzsystem erarbeitet: Es wird zwischen Daten unterschieden, die einen Grundschutz, einen erhöhten Schutz oder einen sehr hohen Schutz benötigen. Entsprechend würden die Sicherheitsvorkehrungen, etwa eine Zwei-Stufen-Authentifizierung, eingestellt und die Daten nicht auf denselben Systemen gespeichert.

Ausserdem sei man dabei, ein kantonales «Security Operation Center» aufzubauen. «An dieser zentralen Stelle werden Infos rund um die Datensicherheit gesammelt und versucht, Verdächtiges zu entdecken», sagt Magnanelli. Wenn sich etwa jemand 15-mal vergeblich in ein Konto einzuloggen versuche, werde diesem Fall nachgegangen.

— Sind Kantone durch die zunehmenden Cyberangriffe besonders gefährdet?
Nein, sagen die Experten des NCSC: «Die kantonalen Behörden sind gleich gefährdet wie Unternehmen.» In der Schweiz liege die Cybersicherheit in der Eigenverantwortung von Unternehmen und Behörden. «Das Sicherheitsniveau reicht von sehr gut bis verbesserungsfähig», sagen die Cybersicherheitsleute.

Laut Martin Lutz sind «staatliche Stellen in der Schweiz in der Regel besser abgesichert als die meisten Unternehmen. Doch eine hundertprozentige Sicherheit gibt es nicht.»

— Wer steht hinter der Hackergruppe Bian Lian?
Die Hackergruppe, welche hinter dem Datendiebstahl und der anschliessenden Erpressung steckt, nennt sich Bian Lian. Der Begriff entstammt der klassischen chinesischen Oper und bezeichnet eine Art der Maskenkunst, bei der die maskierten Bühnenkünstler blitzschnell zwischen diversen Masken und Rollen wechseln. Entsprechend digital maskiert und schwer fassbar sind auch die Hacker von Bian Lian. Ihre Identität und ihre Herkunft sind bis heute unbekannt. Aktiv sind sie vor allem in Westeuropa, Australien, Indien und den USA.

In den USA sind rund zwei Drittel der Opfer lokalisiert. Bei den Datendiebstählen und Erpressungen stehen zusehends auch lokale Verwaltungen und Kommunen im Fokus. So wurde etwa im März die Stadt Waynesboro in Virginia durch Bian Lian attackiert. Auch Polizeistationen waren betroffen.

ANZEIGE