Hacker stellen sensible Daten von Schülern und Lehrerinnen ins Darknet

Hunderte in Basel betroffen Über eine präparierte Mail verschafften sich Cyberkriminelle im Januar Zugang zu einem Server des Erziehungsdepartements. Dies mit dem Ziel, Geld zu erpressen.

Andrea Schuhmacher

Zerknirscht über die Cyberattacke: (Von links) Informationssicherheitsbeauftragter Christian Kern, Regierungsrat Conradin Cramer und Thomas Wenk, Leiter Digitalisierung und Informatik. Foto: Pino Covino

Sie schlich sich während der Weihnachtsferien ins Netzwerk ein. Wochenlang sammelte die bekannte Hackergruppe Bian-Lian Daten von einem Server des Basler Erziehungsdepartements (ED) – bis sie am 25. Januar dann die Behörden vor die Wahl stellte: Zahlt, oder wir stellen die gesammelten Daten ins Darknet. Der Kanton liess sich nicht erpressen – und muss nun die Konsequenzen ausbaden.

Am Dienstagabend machten die Cyberkriminellen ihre Drohung wahr und veröffentlichten vom Edubs.ch-Server geklaute Daten im Umfang von 1,2 Terabyte im Darknet. Wie sich im Verlauf des gestrigen Tages herausstellte, befinden sich darunter sensible Daten von Basler Schülerinnen und Lehrpersonen. Darunter: Lehrberichte, Noten, Absenzen, E-Mail-Korrespondenzen, Abklärungsberichte – und eine Anzahl den Behörden noch unbekannte Daten.

Auf dem Server liegt nämlich auch, was Lehrpersonen und Schülerinnen auf den vom ED zur Verfügung gestellten Laptops abspeichern. Die Chance, dass sich darunter etwa auch heikle Dokumente wie schulpsychologische Berichte befinden, ist relativ gross. Glück im Unglück: Dieser Server ist vom kantonalen Datennetz isoliert.

Kein gezielter Angriff

An einer Medienorientierung erklärten Bildungsdirektor Conradin Cramer, Thomas Wenk (Leiter Digitalisierung und Informatik DIG-IT) und Christian Kern (Informationssicherheitsbeauftragter vom ED) gestern Abend den aktuellen Stand ihrer Ermittlungen. Und zwar erstaunlich ausführlich. Man wolle «Licht ins Darknet» bringen, so Cramer.

Die Erpresser gelangten über eine Phishing-Mail ins System und nützten technische Lücken aus, um an die Daten zu gelangen. Gemäss Wenk griffen die Hacker das ED aber nicht gezielt an. Vielmehr habe die Gruppe massenweise mit Ransomware verseuchte E-Mails verschickt – und eine bis dato unbekannte Person mit einem Edubs.ch-Account öffnete diese nichts ahnend. Ob es sich um eine Lehrperson oder einen Schüler handelt, ist unbekannt. Dass die Hacker die Daten trotzdem zu einem Erpressungsversuch verwendeten, obwohl diese laut Cramer kaum kommerzialisierbar sind, sei dem Ruf der Gruppe geschuldet. «Sie will, dass allen Unternehmen klar wird: Wir machen Ernst und schrecken auch vor Kindern nicht zurück», so der Bildungsdirektor zum möglichen Motiv der Cyberkriminellen.

Die Lösegeldsumme – die Behörden nennen die Höhe nicht – zu zahlen, sei nie ein Thema gewesen. «Es wäre ein Dammbruch mit ungeahnten Folgen, wenn sich der Kanton erpressen lassen würde», sagte Cramer.

Per Whatsapp kontaktiert

Mit den Erpressern verhandeln konnten weder die Basler Staatsanwaltschaft noch das Departement. Die Gruppe ignorierte Kontaktversuche. «Die Kommunikation lief einseitig», informierte Conradin Cramer. Er selbst sei über Whatsapp kontaktiert worden. Er erhielt die Nachricht: «Does your chairman know you had a data breach?» Auf Deutsch: «Weiss Ihr Vorsitzender, dass Sie einen Datendiebstahl hatten?»

Dass die Cyberkriminellen die Behörden nur austricksen wollten, schloss man aus. «Diese Gruppe blufft nicht», sagte Thomas Wenk, der vor seiner Stelle beim ED bei der Stadtpolizei Zürich das Kompetenzzentrum für digitale Ermittlungsdienste leitete. Wenk erklärte, was man über die gestohlenen Daten bisher weiss und was nicht.

Von Anfang an sei es schwierig gewesen, zu wissen, was gestohlen worden sei. Denn die Erpresser entwendeten keine Daten, sie kopierten sie nur. Jetzt, da sie im Darknet auffindbar sind, hätten die IT-Spezialisten vom Kanton und eine zur Hilfe gezogene externe Firma Ordnerstrukturen und sichtbare Verzeichnisse geortet. Aufgrund dieser weiss man zwar Näheres über die Natur der Daten. Bis die Spezialisten an alle Inhalte kommen, ist allerdings unklar, wessen Daten im Darknet öffentlich gemacht wurden.

«Unser Team ist daran, die Listen zu analysieren», sagte Wenk. Da die Verbindung zum Server im Darknet allerdings nicht stabil sei, laufe dieser Prozess nur langsam. Selber lade man allerdings keine Daten aus dem Darknet herunter, stellte Informationssicherheitsbeauftragter Christian Kern klar.

Viele Betroffene

Sobald man Näheres wisse, nehme man mit den Betroffenen Kontakt auf, um das Vorgehen zu besprechen. Dies werde in den kommenden Tagen das ED vor allem beschäftigen, sagte Conradin Cramer. «Eine grosse Zahl von Personen im Kanton Basel-Stadt dürfte betroffen sein.» Im schlimmsten Fall Hunderte.

«Wir bedauern, dass es passiert ist», so Cramer weiter. Vor allem weil es in einer Zeit geschehen ist, in der das ED seine Datensicherheit massiv aufrüstet. «Wir haben viele Bestrebungen unternommen, wurden aber von den Kriminellen überholt – das ist bitter.»

Erpressungen dieser Art sind in der Schweiz keine Seltenheit. Oft gelangen sie aber nicht an die Öffentlichkeit. Zuletzt sorgte der Erpressungsversuch bei den Medienunternehmen NZZ und CH Media für Schlagzeilen. Auch in diesem Fall wurden geklaute Daten ins Darknet gestellt, nachdem sich die Unternehmen geweigert hatten, ein Lösegeld zu zahlen.

Unter anderem betroffen waren Lohnlisten, Lohnausweise, Erfolgsrechnungen, Korrespondenzen mit dem Fiskus, Werberechnungen, vertrauliche Daten für den Erhalt staatlicher Presseförderung und Medienprojekte, bei denen auch Konkurrenzunternehmen wie Ringier und der Tamedia-Konzern im Fokus sind.

Vor rund zwei Jahren traf es den Vergleichsdienst Comparis. In diesem Fall entschieden sich die Eigentümer dazu, einen Teil des geforderten Lösegelds zu zahlen. Zunächst war man fest entschlossen gewesen, nicht auf die Forderungen der Hacker einzugehen. Doch eine Kosten-Nutzen-Abwägung zeigte schlussendlich: Es wäre für das Unternehmen offenbar viel teurer geworden, alle noch verschlüsselten essenziellen Dateien wiederherzustellen.