«Basler» Hacker suchen nach Verstärkung

Cyberkriminalität Vor einem Jahr erhielt das Basler Erziehungsdepartement (ED) ein Erpresserschreiben einer unbekannten Hackergruppe. Zu diesem Zeitpunkt ging man bei der Basler Verwaltung davon aus, dass die Cyberkriminellen nur bei einer Person erfolgreich waren. Ein schwerer Irrtum: Insgesamt 1,2 Terabyte Daten von insgesamt 761 Lehr- und Fachpersonen, Schülerinnen und Schülern und Verwaltungsangestellten hatten die Hacker vom Bildungsserver abgegriffen. Als kein Geld floss, wurden die teilweise sensiblen Daten im Mai im Darknet veröffentlicht, also dem versteckten Teil des Internets.

Eine der aktivsten Erpressergruppen weltweit

Bekannt zum Angriff und Erpressungsversuch hat sich die Hackergruppe BianLian, die im Sommer 2022 erstmals aufgetaucht ist. «Sie spekulieren darauf, dass eine Veröffentlichung der Daten schmerzhaft genug sein wird, um eine Zahlung zu erzwingen», sagte Sicherheitsexperte Marc Ruef.

Und offenbar sind die Cyberkriminellen damit erfolgreich. Die renommierte IT-Sicherheitsfirma Palo Alto Networks hat kürzlich einen neuen Forschungsbericht zu BianLian veröffentlicht. Mittlerweile sei BianLian eine der aktivsten und dominierendsten Hackergruppen im Bereich Erpressung. Im vergangenen Mai stellten die Sicherheitsexperten mehr als zwei Dutzend Vorfälle im Zusammenhang mit BianLian fest. Und: Hinweise rund um die Gruppe würden darauf hindeuten, dass BianLian expandiert und neue Entwickler und Entwicklerinnen sowie Mitglieder sucht.

Die Autorinnen und Autoren des Berichts sind auch auf Überschneidungen in der Schadsoftware von BianLian mit einer russischen Cybererpresserbande gestossen. Weiter lassen die Daten vermuten, dass das Erziehungsdepartement war wohl eher ein zufälliges Opfer war: «Diese Gruppe zielt vor allem auf das Gesundheitswesen, die verarbeitende Industrie sowie den professionellen und juristischen Dienstleistungssektor», so die Expertinnen und Experten. Das wäre eine mögliche Erklärung, weshalb die Hacker auf Kontaktaufnahme in Basel gar nicht erst reagierten.

Aufräumarbeiten noch immer nicht abgeschlossen

Beim Erziehungsdepartement ist man auch ein Jahr nach dem Angriff am Aufräumen: «Wir haben die direkt Betroffenen informiert. Die indirekt Betroffenen sind mittlerweile ebenfalls identifiziert», sagt Sprecher Gaudenz Wacker. Nun sei die Information der indirekt Betroffenen angelaufen. Im ersten halben Jahr war ein Team von vier Personen vollumfänglich und ausschliesslich mit der Aufarbeitung beschäftigt. Seit November ist der Aufwand integriert in die regulären Dienstleistungen der IT-Abteilung des Erziehungsdepartements.

Jonas Hoskyn