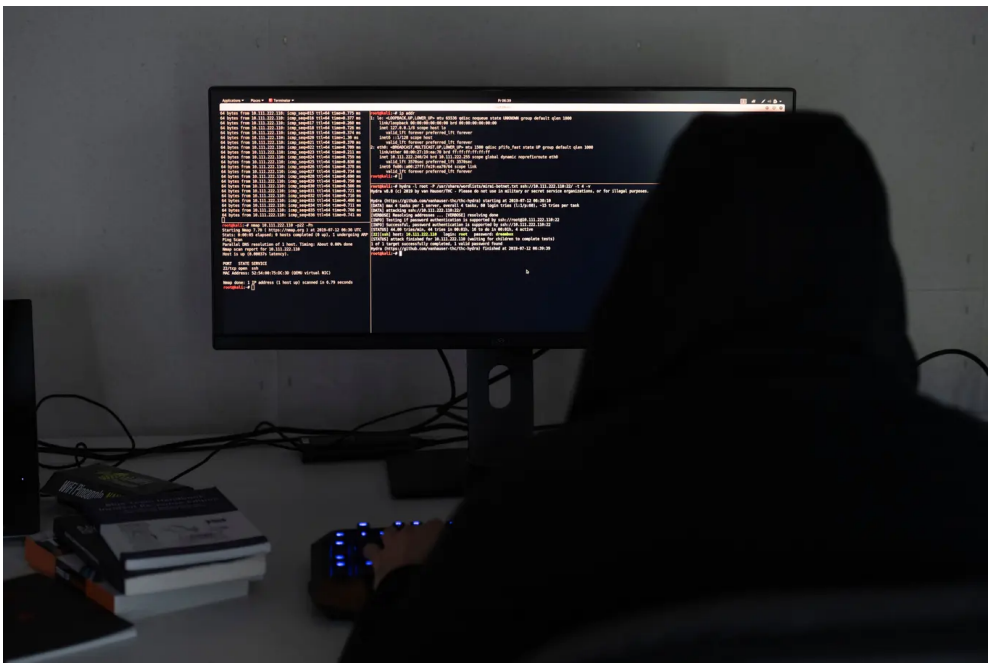
Neue Zürcher Zeitung

Dass die Universität Zürich von Hackern attackiert wird, dürfte kein Zufall sein. Aber was wollen die Angreifer?

Bildungseinrichtungen werden seit der Corona-Pandemie immer häufiger Opfer von Hackern. Worauf haben es die Kriminellen mit ihrem Cyberangriff auf die Hochschule abgesehen? Wir haben Experten befragt.

Fabian Vogt

03.02.2023, 18.46 Uhr



Hackerangriffe auf Unternehmen nehmen stetig zu. Besonders Bildungseinrichtungen sind immer stärker im Fokus von Angreifern.

Str / Keystone

Die Verantwortlichen der Universität Zürich sind besorgt. «Kein Kommentar», heisst es am Freitag zur Cyberattacke, die die Hochschule in diesen Tagen stark fordert. Man befinde sich mitten in der Abwehr der Angriffe und könne aus

taktischen Gründen nicht mehr sagen als in einer Mitteilung vom Vortag. Laut dieser versuchen Hacker momentan, in die Systeme der Universität einzudringen. Zu welchem Zweck und wer dahintersteckt, ist derzeit nicht klar. Ein Studenten-Jux dürfte es aber kaum sein. Dafür scheint der Angriff zu gut organisiert.

«Es sieht relativ ernst aus», sagte Kurt Bodenmüller, Medienbeauftragter der UZH, am Donnerstag. Die Angriffe würden auf verschiedene Arten stattfinden. Es gebe Distributed-Denial-of-Service-Angriffe (DDoS) – eine geballte Vielzahl an Attacken, die das System zum Kollaps führen sollen. Aber auch gezielte Angriffe auf einzelne Accounts finden statt. Mitarbeiter und Studenten wurden aufgefordert, sämtliche Passwörter zu den Uni-Systemen zu ändern.

Auch wer hinter der Attacke steckt und aus welchem Grund, ist noch unklar. Die Zürcher Kantonspolizei ermittelt, will sich aber nicht weiter zum Vorfall äussern.

Seit Corona haben Hacker mehr Möglichkeiten

Dass die Universität Zürich Opfer eines Cyberangriffs geworden ist, liegt im Trend: Vergangenes Jahr war der Bildungs- und Forschungssektor weltweit die am häufigsten angegriffene Branche. Das geht aus einer Studie des Sicherheitsanbieters Check Point hervor, der Softwarelösungen zum Schutz von Unternehmen anbietet. Durchschnittlich 2314 Angriffe pro Organisation und Woche wurden laut ihren Daten verzeichnet, ein Anstieg um 43 Prozent gegenüber dem Vorjahr. In der Schweiz waren andere Branchen letztes Jahr noch stärker im Fokus, etwa die

Fertigungsindustrie oder die Finanzbranche, aber das könnte sich bald ändern.

«Vor zwei Jahren gab es einen massiven Anstieg von Cyberangriffen auf den Bildungssektor», sagt Alvaro Amato, bei Check Point zuständig für die Schweiz. Auslöser sei die Corona-Pandemie gewesen: «Auf einmal durften die Studenten nicht mehr in die Klassenräume. Es brauchte sofortige Lösungen, um den Unterricht fortzuführen, vielerorts wechselte man ins Internet.» Dabei sei aber teilweise vielleicht der Sicherheitsaspekt vernachlässigt worden: «Wenn Studenten beispielsweise nicht mehr im Klassenzimmer sitzen, sondern miteinander über Slack, Skype und andere Tools kommunizieren, haben Hacker auf einmal viel mehr Möglichkeiten, um das Unternehmen anzugreifen.»

Lösegeld, Identitätsklau oder Betriebsspionage

Solche Angriffe simuliert Urs Rufer, CEO von Terreactive, regelmässig. Das Aargauer Unternehmen prüft einerseits die Systeme seiner Kunden auf Schwachstellen und wehrt andererseits echte Angriffe ab. Einen bestimmten Modus Operandi gebe es dabei nicht, zu unterschiedlich seien die Vorgehensweisen der Hacker. «Einige haben es auf Geld abgesehen. Die versuchen dann beispielsweise, mit Ransomware-Angriffen Systeme lahmzulegen. Etwa, indem sie gewisse Daten verschlüsseln und erst wieder freigeben, nachdem ein Lösegeld bezahlt worden ist.»

Anderen Hackern würde es darum gehen, vertrauliche Informationen – zum Beispiel Pläne für ein neues Produkt – zu stehlen, um diese einer konkurrenzierenden Firma zu

verkaufen. Oder, was auch in einer Uni der Fall sein könnte, Datenbanken mit Adressen und anderen Informationen über die Mitarbeiter zu kopieren, um deren Identitäten dann im Darknet zu verkaufen, wo falsche Pässe oder Identitätskarten ausgestellt werden.

Glücklicherweise sei es oftmals so, dass die Verteidiger die Angreifer in die Schranken weisen könnten, sagt Rufer. Aber auch dies werde zunehmend schwieriger, da die Hacker immer ausgefeilter und koordinierter attackieren würden.

Angriffe simulieren, um für den Ernstfall gewappnet zu sein

Rufer empfiehlt Organisationen einen Drei-Punkte-Plan, um sich zu schützen: «Die Infrastruktur gilt es aktuell zu halten, das heisst, immer alle Updates zu installieren und es Angreifern durch 2-Faktor-Authentifizierung und andere Massnahmen so schwer wie möglich zu machen, in die Systeme zu gelangen.» Als Zweites müssten die Mitarbeiter stetig geschult werden, sagt Rufer: «Auch wenn heute die meisten wissen, nicht auf jede Mail zu klicken, gibt es im Bereich Social Engineering ständig neue Angriffsmethoden.» Als Drittes empfiehlt der Experte jeder Organisation, den Notfall zu üben. «Wer bereits durchgespielt hat, Opfer einer Ransomware-Attacke geworden zu sein, wird im Ernstfall wesentlich effizienter reagieren können.» Mit dem Ernstfall muss sich auch die ETH Zürich immer öfter befassen. «Wir mussten in den vergangenen zirka fünf Jahren leider einen kontinuierlichen Anstieg von Attacken unterschiedlicher Art feststellen», sagt Sprecherin Marion Schihin. So würde man täglich «unzählige Phishing-Mails» verzeichnen, von denen «wir die allermeisten mit unseren Filtersystemen abfangen».

Es bestehe ein regelmässiger Austausch mit der Universität Zürich und anderen Schweizer Hochschulen zum Thema IT-Sicherheit, sagt Schihin. Im gegenwärtigen Fall sei die ETH Zürich von der UZH informiert worden, so dass die ETH umgehend ihre eigenen Systeme gezielt habe prüfen können. Bis jetzt gebe es keinerlei Hinweise darauf, dass auch die ETH betroffen sei.

Falls die Uni Zürich den Angriff erfolgreich abwehrt, werden darum auch die Verantwortlichen der ETH ruhiger schlafen. Ob das gelungen ist, will die Hochschule nächste Woche kommunizieren.