Sterne am Nachthimmel sind Lichtjahre entfernt, Daten im Darknet zum Greifen nah. Andreas Andrzejewski

Die Stille nach dem Datenklau

Hacker haben sensible Informationen über Abonnentinnen und Angestellte von NZZ und CH Media im Darknet publiziert. Die Unternehmen verharmlosten das Ausmass des Datendiebstahls und informierten Betroffene nicht.

Von Adrienne Fichter, 04.07.2023

Auf den ersten Blick handelte die NZZ vorbildlich.

Der Medienkonzern war gemeinsam mit CH Media im Frühjahr 2023 Opfer einer Cyberattacke der Hackergruppe Play geworden. Die Folgen: ein Abfluss von 530 Gigabyte Daten aus den IT-Unternehmensnetzwerken, die danach im Darknet veröffentlicht wurden.

Die Bande Play schaffte es, tief in das Unternehmensnetzwerk einzudringen, und publizierte darauf paketweise die Dateien. Wer sich einen Überblick über das Ausmass der entwendeten Daten verschaffen wollte, brauchte Geduld: Die Menge an PDFs, E-Mails und Exceldateien war derart gross, dass der Download mehrere Wochen benötigte.

Wie genau die Angreifer an all diese Geschäftsinterna gelangten, ist unklar. Gemäss «Blick» war der Klick auf eine Phishing-E-Mail durch einen Mitarbeiter von CH Media massgebend. Dadurch öffnete sich ein Einfallstor zu den IT-Systemen der NZZ. Denn CH Media ist ein Joint Venture von NZZ und AZ Medien und bezieht IT-Services der NZZ.

Im Darknet landeten die Daten, weil sich die Medienunternehmen weigerten, das geforderte Lösegeld an die Play-Hacker zu bezahlen. Stattdessen benachrichtigte sie das National Cyber Security Centre des Bundes, den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (Edöb) und die Strafverfolgungsbehörden über den Angriff, der sich Ende März ereignet haben soll.

Damit beherzigten die Medienhäuser einen alten Grundsatz der IT-Sicherheit: Lösegeldforderungen von Cyberkriminellen nicht nachkommen. Denn nur so wird deren Geschäftsmodell zerstört und der Markt ausgetrocknet.

Doch NZZ und CH Media zahlten mit der Verweigerung einen hohen Preis: Unter den Daten, die darauf im Darknet auftauchten, befanden sich teilweise kompromittierende persönliche Informationen von Personal und Leserschaft.

Das Schweigen

Die Reaktionen von NZZ und CH Media hinsichtlich der Strafverfolgung bei der Cyberattacke waren also State of the Art.

Die Informationspolitik der NZZ ist hingegen eine Katastrophe.

Das Traditionsunternehmen an der Zürcher Falkenstrasse verlautbarte zwar in zwei Hausmitteilungen und wenigen Artikeln – die aber hinter einer Paywall versteckt waren –, dass Mitarbeiterdaten und Kundinnenindformationen betroffen seien. Doch die vage formulierte Mitteilung erweckte den Anschein, dass «nur» die Daten des aktuellen Personals entwendet worden seien.

Dabei befinden sich unter den geleakten Dateien nicht nur die Lohnausweise, Sozialversicherungsnummern, Bankkontoinformationen, Pensionskassenguthaben sowie die Postadressen von aktuellen Mitarbeitern, sondern auch diejenigen von vielen ehemaligen NZZ-Angestellten.

Das bedeutet: Zahlreiche Journalistinnen, die heute in anderen Schweizer Medienhäusern arbeiten, sind ebenfalls betroffen. Ihre Daten sind bereits seit zwei Monaten im Darknet einsehbar. Informiert wurden sie von der NZZ nie.

Darf die NZZ in diesem Fall schweigen?

Nach dem bestehenden Datenschutzgesetz – das noch bis zum 31. August 2023 gilt – gibt es nach Meinung vieler Privacy-Experten, mit der die Republik gesprochen hat, keine zwingende Informationspflicht bei solchen Sicherheitslecks.

Der eidgenössische Datenschutzbeauftragte Adrian Lobsiger sieht das aber anders: «Wir vertreten schon seit dem Swisscom-Fall 2018 die Ansicht, dass sich die Informationspflicht bis zu einem gewissen Grad aus dem alten Datenschutzgesetz ableitet.» (Lobsiger nimmt damit Bezug auf einen Cyberangriff, der zum Abfluss von 800'000 Swisscom-Kundendaten führte.)

Der Datenschutzbeauftragte selbst verfährt bereits jetzt nach neuem Datenschutzrecht, das ab dem 1. September verbindlich für alle in der Schweiz gilt. Und dieses sieht je nach Vorfall eine Kommunikation an alle Betroffenen vor. Insbesondere wenn der Datenverlust «Risiken für die betroffenen Personen mit sich bringt» und sie dadurch «Massnahmen ergreifen müssen, um sich davor zu schützen», wie Lobsiger auf Anfrage schreibt.

Die NZZ-Gruppe teilte dem Datenschutzbeauftragten am 12. Mai 2023 mit, dass neben Hausmitteilungen eine «erneute separate Information» über das Ausmass des Vorfalls an alle betroffenen Mitarbeiterinnen erfolgen würde. Allerdings gilt das nicht für die Abonnenten. Obwohl die Postadressen von einem Teil der NZZ-Leserschaft ins Darknet gelangt sind.

Der Datenschutzbeauftragte forderte daraufhin, dass die NZZ-Abonnentinnen ebenfalls einzeln benachrichtigt werden sollen, da die allgemeine Information via Artikel und Mitteilung nicht ausreiche. In den Datensätzen im Darknet finden sich gemäss Swissinfo.ch auch E-Mail- und Postadressen von 425'000 Auslandschweizerinnen, die zum Abonnentenstamm des Schweizer Magazins «Schweizer Revue» gehören, das in einer Druckerei hergestellt wird, die zu CH Media gehört.

Die Republik wies Lobsiger vor zwei Wochen darauf hin, dass auch betroffene Ex-Mitarbeiter der NZZ keine Post von ihrer früheren Arbeitgeberin erhalten haben. Daraufhin setzte sein Team für den 28. Juni ein Treffen mit der NZZ an. Lobsiger sagt dazu: «Wir sind der Ansicht, dass auch ehemalige Mitarbeitende ein Anrecht auf aktive Information haben. Die Modalitäten einer solchen Information sind aber momentan noch Gegenstand von Diskussionen mit der NZZ.»

Warum kommuniziert das Medienunternehmen so zögerlich? Der NZZ sei es wichtig gewesen, zunächst ihre heutigen Beschäftigten über das Datenleak und den Inhalt der im Darknet veröffentlichten Daten zu informieren, sagt Mediensprecherin Karin Heim auf Anfrage. Benachrichtigt wurde lediglich ehemaliges Personal, dessen Bank- und Ausweiskopien von den Hackern veröffentlicht worden sind.

Wie hat CH Media die Kommunikationspolitik gehandhabt?

Der Konzern hält fest, dass alle vom Leak betroffenen Gruppen im Bilde seien: «Wir haben unsere Mitarbeitenden, unsere ehemaligen Mitarbeitenden sowie unsere Kundinnen und Kunden zeitnah, wiederholt und breitflächig über das Datenleak und den Inhalt der betroffenen Daten informiert. Überdies haben wir eine Anlaufstelle eingerichtet für individuelle Anfragen.»

Doch das stimmt nur teilweise. Zwar haben CH-Media-Leser einen entsprechenden Infobrief erhalten. Doch die Republik befragte neun ehemalige CH-Media-Mitarbeiterinnen, deren Lohn- und Sozialversicherungsausweise sowie Arbeitszeugnisse im Darknet vorhanden sind: Niemand hat von seiner ehemaligen Arbeitgeberin je etwas gehört.

Es drohen Identitätsdiebstahl und Phishing-Attacken

Die Risiken für alle Betroffenen des Hacks sind nicht zu unterschätzen. Die persönliche AHV-Nummer beispielsweise ist eine Zahl, die das ganze Leben unverändert bleibt. Eine Änderung auf eine neue AHV-Nummer ist nicht möglich.

Die Sozialbehörden finden das erstaunlicherweise nicht problematisch.

Harald Sohns, Mediensprecher des Bundesamts für Sozialversicherungen, begründet dies so: «Eine Person mit kriminellen Absichten kann mit meiner AHV-Nummer nicht mehr anrichten, als wenn sie nur meinen Namen kennt, denn die AHV-Nummer gilt nicht als Identitätsnachweis.»

Das ist arg beschönigend. Erstens wird die AHV-Nummer als persönliches Merkmal eine Rolle spielen bei der künftigen E-ID oder beim Adressdienstgesetz, was von Organisationen wie der Digitalen Gesellschaft stark kritisiert wird.

Und zweitens ist jede personenbezogene, amtliche Information im Darknet eine zu viel. Kriminelle könnten sich aus dem Fundus bedienen und eine umfassende Datenbank mit der wichtigsten Sozialversicherungskennzahl sowie der zugehörigen Postadresse, dem Geburtsdatum und allenfalls auch Mobilnummern erstellen. Dieses Hintergrundwissen über eine einzelne Person dient Hackern für potenziellen Identitätsdiebstahl. Es handelt sich um Informationen, die bei Hotlines oft als Identifizierung von Kundinnen angegeben werden. Die AHV-Nummer wird beispielsweise in der Korrespondenz bei der kantonalen Steuerbehörde und der Sozialversicherungsanstalt sehr wohl auch als identifizierendes Merkmal verlangt.

Ausserdem können solche Informationen für personalisierte Phishing-Angriffe genutzt werden. Ein mögliches Szenario: Eine böswillige Hackerin erstellt eine Fake-Website des Bundesamts für Sozialversicherungen oder der Sozialversicherungsanstalt des Kantons Zürich und versendet eine E-Mail an ein potenzielles Opfer mit Angabe der persönlichen AHV-Nummer. Die ahnungslose Person nimmt im schlimmsten Fall an, es handle sich beim Absender wirklich um eine offizielle Stelle – schliesslich ist diese im Besitz einer persönlichen Kennzahl, die sich nicht einfach so ergoogeln lässt.

Und zu schlechter Letzt: In den im Darknet veröffentlichten Dokumenten von NZZ und CH Media finden sich auch arbeitsrechtliche Auseinandersetzungen mit Angestellten und Kadermitgliedern sowie E-Mail-Verläufe mit wüsten Beschimpfungen – alles Informationen für potenzielle Erpressungen. So kann Journalistinnen, über die heikles Material vorhanden ist, bei missliebiger Berichterstattung gedroht werden.

Ein problematischer Präzedenzfall

Zwar informierte CH Media Betroffene umfassender als die NZZ-Gruppe. Weniger vorbildlich verhielt sich der Verlag, als es um die Berichterstattung über den Datendiebstahl ging.

CH Media versuchte nämlich, die Publikationen rund um das Datenleak einzuschränken, und schuf vor knapp zwei Monaten einen problematischen Präzedenzfall: Das Unternehmen erwirkte mittels einer superprovisorischen Verfügung, dass Medien wie das Branchenportal «Inside-IT» und die Wochenzeitung WOZ in ihren Artikeln zum Thema mehrere Abschnitte schwärzen oder löschen mussten. Die Leserschaft durfte nicht

erfahren, welche gravierenden Folgen die Cyberattacke auf CH Media und NZZ hatte.

«Inside IT» und WOZ wehrten sich vor Gericht erfolgreich gegen die Zensur. In einem Vergleich einigten sich die Medienhäuser darauf, dass die Artikel wieder unzensiert veröffentlicht werden dürfen – unter der Bedingung, dass die Medienhäuser die aus dem Darknet heruntergeladenen Datensätze danach löschen würden.

Der Vergleich ist ein gutes Signal für die Medienbranche. Denn er bedeutet: Investigativjournalistinnen sollen im Darknet recherchieren können, etwa um zu verifizieren, ob eine Sicherheitslücke entgegen anderslautenden Aussagen von Unternehmen und Bundesorganen effektiv ausgenutzt wurde, oder um herauszufinden, wie viele Daten gestohlen wurden.

Das ist wichtig. Gemäss den Rechercheerfahrungen der Republik werden solche Vorkommnisse von attackierten Firmen und Institutionen stets heruntergespielt oder ganz geleugnet. Und selbstverständlich ist es Praxis, solche Datensätze nach Beendigung einer Recherche zu löschen.

Bleibt zu hoffen, dass das Unternehmen NZZ nach der Intervention des Datenschutzbeauftragten ihre Kommunikationspolitik verbessert und dass auch CH Media ihr ehemaliges Personal individuell informiert.

Datenklau: Was Betroffene tun können

Ob nun Abonnenten oder ehemalige Journalistinnen der NZZ: Allen Betroffenen sei geraten, noch vorsichtiger im Umgang mit dubiosen E-Mails und SMS zu sein, keine Links anzuklicken und im Zweifelsfall eingehende Nachrichten gleich zu löschen. Schliesslich werden die Cyberangriffe gemäss Meldung des National Cyber Security Centre immer perfider und raffinierter. Letzte Woche vermeldete das Kompetenzzentrum ein Rekordhoch von Meldungen.

Ausserdem wird empfohlen, mit Hotlines von Telecomkonzernen und weiteren Unternehmen zusätzliche Sicherheitsfragen zu vereinbaren für die Authentifizierung am Telefon, zum Beispiel ein gesprochenes Passwort. Denn oftmals werden lediglich die Postadresse und das Geburtsdatum verlangt.

Ehemalige Mitarbeitende können sich via datenschutz@nzz.ch an die NZZ wenden, um herauszufinden, ob sie vom Datendiebstahl betroffen sind.