

Einschreiben

Eidgenössischer Datenschutz- und
Öffentlichkeitsbeauftragter EDÖB
Feldeggweg 1
3003 Bern

David Rosenthal
lic. iur.
Tel [REDACTED]
[REDACTED]

Zürich, 27. September 2024
50043638.17

EDÖB-A-EAD83401/1: Stellungnahme

Adrian Gautschi
Rechtsanwalt
Tel [REDACTED]
[REDACTED]

Sehr geehrter Herr Lobsiger, sehr geehrte Frau Gysin,
sehr geehrte Damen und Herren

Eingetragen im
Anwaltsregister des
Kantons Zürich

Mit Schreiben vom 26. Juni 2024 hat der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte EDÖB ("**EDÖB**") in der oben genannten Sache unserer Klientin, der Neuen Zürcher Zeitung AG ("**NZZ**"), die Eröffnung einer Untersuchung nach Art. 49 des Bundesgesetzes über den Datenschutz vom 25. September 2020 (DSG, SR 235.1) angezeigt. Ebenfalls hat der EDÖB der NZZ mit diesem Schreiben den Entwurf einer Sachverhaltsfeststellung ("**Sachverhaltsfeststellung EDÖB**") zukommen lassen. Das Schreiben ist der NZZ am 27. Juni 2024 zugegangen.

www.vischer.com

VISCHER AG

Zürich
Schützengasse 1
Postfach
8021 Zürich
Schweiz
Tel +41 58 211 34 00

Basel
Aeschenvorstadt 4
Postfach
4010 Basel
Schweiz
Tel +41 58 211 33 00

Genf
Rue du Cloître 2
Postfach
1204 Genf
Schweiz
Tel +41 58 211 35 00

Der EDÖB ersucht die NZZ, innert 30 Tagen ab Erhalt des Schreibens vom 26. Juni 2024 die Sachverhaltsfeststellung EDÖB auf ihre Korrektheit zu prüfen und allfällige Korrekturen des Sachverhalts unter Einschluss allfälliger neuer rechtlicher Vorbringen mitzuteilen. Diese Frist endete, unter Berücksichtigung des Fristenstillstandes vom 15. Juli 2024 bis und mit dem 15. August 2024 (Art. 22a lit. b des Bundesgesetzes über das Verwaltungsverfahren vom 20. Dezember 1968 [VwVG, SR 172.021]), am 28. August 2024. Mit Schreiben vom 28. August 2024 hat der EDÖB diese Frist freundlicherweise und antragsgemäss bis zum 27. September 2024 erstreckt.

Mit vorliegender Eingabe nehmen wir namens und im Auftrag der NZZ fristgerecht Stellung und stellen die folgenden

ANTRÄGE

- "1. Es habe sich der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte für das Untersuchungsverfahren (Aktenzeichen EDÖB A EAD83401/1) für unzuständig zu erklären und darüber eine anfechtbare Verfügung zu erlassen;

Rechtsanwältin

Notariat im Kanton
Basel-Stadt

VISCHER

2. **Eventualiter zu Ziff. 1** vorstehend sei das Untersuchungsverfahren (Aktenzeichen EDÖB A EAD83401/1) als gegenstandlos geworden abzuschreiben;
3. Es seien der Neuen Zürcher Zeitung AG keine Kosten aufzuerlegen."

INHALTSVERZEICHNIS

I.	KEINE ZUSTÄNDIGKEIT DES EDÖB	4
II.	MASSGEBENDER SACHVERHALT UND KORREKTUREN	5
A.	Der zwischen März und Juli 2023 vorgefallene Sachverhalt	5
B.	Anfragen beim EDÖB im März 2024	8
C.	Was vom Sachverhalt noch übrig bleibt.....	10
III.	MATERIELLES	12
A.	Übersicht.....	12
B.	Keine Informationspflicht nach aDSG	13
C.	Keine Anwendbarkeit von Art. 24 Abs. 4 DSG auf vor dem Inkrafttreten abgeschlossene Sachverhalte.....	13
D.	Keine Verletzung von Art. 24 Abs. 4 DSG	14
1.	Betroffene müssen nur ausnahmsweise informiert werden.....	14
2.	Information der ehemaligen Mitarbeiter ist schon erfolgt – der Weg spielt keine Rolle	15
3.	Heutige Information aller ehemaliger Mitarbeiter ist zu deren Schutz nicht erforderlich	16
E.	Ausnahme nach Art. 24 Abs. 5 DSG gegeben	17
1.	Öffentliche Bekanntmachung ist erfolgt	17
2.	Unverhältnismässigkeit der Information	18
F.	Der EDÖB widerspricht sich selbst	18
IV.	ZU DEN ANTRÄGEN	19
A.	Fehlende Zuständigkeit (Antrag Ziff. 1)	19
B.	Eventualiter Gegenstandslosigkeit (Antrag Ziff. 2)	19
C.	Kosten (Antrag Ziff. 3)	19

BEGRÜNDUNG

I. KEINE ZUSTÄNDIGKEIT DES EDÖB

- 1 Nach Art. 49 Abs. 1 DSG eröffnet der EDÖB von Amtes wegen oder auf Anzeige hin eine Untersuchung, wenn genügend Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte. Bei der vorliegenden Untersuchung will der EDÖB die folgenden Rechtsfragen prüfen (s. Schreiben des EDÖB vom 26. Juni 2024, S. 2):

"1. Sind im vorliegenden Sachverhalt die Voraussetzungen von Art. 24 Abs. 4 DSG erfüllt, sprich ist die Information der Betroffenen zu ihrem Schutz erforderlich?

2. Kann die Information an die betroffene Person eingeschränkt, aufgeschoben oder auf sie verzichtet werden, gestützt auf die gesetzlichen Ausnahmen von Art. 24 Abs. 5 DSG?"

- 2 Mit dem Inkrafttreten des DSG am 1. September 2023 erhielt der EDÖB die Zuständigkeit zur Durchführung von Untersuchungsverfahren i.S.v. Art. 49 DSG. Am 1. September 2023 traten auch Art. 24 Abs. 4 und 5 DSG in Kraft, welche die Grundlage für die vom EDÖB gestellten Rechtsfragen bilden. Das Untersuchungsverfahren richtet sich gemäss Art. 52 Abs. 1 DSG nach dem Bundesgesetz über das Verwaltungsverfahren vom 20. Dezember 1968 (VwVG, SR 172.021). Damit gelten vorliegend die **üblichen verwaltungsrechtlichen Verfahrensgrundsätze**.
- 3 Die rechtlichen Wirkungen eines Erlasses beginnen mit seinem Inkrafttreten. Der **Zeitpunkt des Inkrafttretens** wird grundsätzlich im Erlass selbst festgesetzt (s. ULRICH HÄFELIN/GEORG MÜLLER/FELIX UHLMANN, Allgemeines Verwaltungsrecht, 8. Aufl., Zürich 2020, Rz. 258) – hier im Falle des DSG: **1. September 2023**.
- 4 Somit gilt das Folgende: Rechtsnormen wirken grundsätzlich in die Zukunft. Dies, weil rückwirkendes Recht im Widerspruch zu Rechtssicherheit und Vertrauensschutz steht. Zudem ist eine Rückwirkung von neuem Recht auf bereits Geschehenes mit Blick auf das Legalitätsprinzip problematisch, weil bereits geschehene Sachverhalte in solchen Konstellationen nicht nach dem Recht beurteilt würden, das im Zeitpunkt des Geschehens galt und sich der Handelnde so auch nicht danach ausrichten konnte (s. HÄFELIN/MÜLLER/UHLMANN, a.a.O., Rz. 266). Eine Rückwirkung auf einen vor dem Inkrafttreten des neuen Rechts abgeschlossenen Sachverhalt ist damit im Grundsatz ausgeschlossen (Verbot der echten Rückwirkung; s. HÄFELIN/MÜLLER/UHLMANN, a.a.O., Rz. 268 f.).

- 5 Eine Rückwirkung der Zuständigkeit bzw. der Kompetenz des EDÖB i.S.v. Art. 49 DSG oder der Geltung von Art. 24 Abs. 4 und 5 DSG auf vergangene, abgeschlossene Sachverhalte ist somit weder laut DSG noch mit Blick auf verwaltungsrechtliche Grundsätze vorgesehen oder zulässig. In diesem Sinne finden sich im DSG auch keine Übergangsbestimmungen, welche die verbindlichen verwaltungsrechtlichen Grundsätze ausser Kraft setzen würden.
- 6 Eine Zuständigkeit des EDÖB, wie sie in Art. 49 DSG für die Durchführung von Untersuchungsverfahren vorgesehen ist, gab es im Vorgängererlass des geltenden DSG, d.h. im Bundesgesetz über den Datenschutz vom 19. Juni 1992 (aDSG, AS 1993 1945), nicht. Das Gleiche gilt für eine Verfügungskompetenz im Zusammenhang mit – damals nicht zulässigen – Untersuchungsverfahren (s. Art. 28 f. aDSG). Damit ist eine Begründung der Zuständigkeit des EDÖB auch nach altem Recht ausgeschlossen für den vorliegenden, abgeschlossenen Sachverhalt (zu diesem nachstehend, Rz. 9 ff.).
- 7 Dazu kommt, dass Art. 70 DSG festhält, dass auf Untersuchungen, die im Zeitpunkt des Inkrafttretens des DSG am 1. September 2023 hängig waren, nicht das DSG, sondern das aDSG anwendbar ist. Zwar gilt der vorliegend zur Diskussion stehende Sachverhalt als abgeschlossen (zu diesem nachstehend, Rz. 9 ff.), doch müsste Art. 70 DSG zumindest nach der Logik des EDÖB greifen. In seinem Schreiben vom 26. Juni 2024 spricht der EDÖB von einer informellen Vorabklärung, die er unter Geltung des aDSG durchgeführt habe. Erachtet der EDÖB somit diese Vorabklärung noch nicht als abgeschlossen oder greift er den entsprechenden Sachverhalt wieder auf, indem er im Jahr 2024 wieder aktiv wird, gilt nach Art. 70 DSG weiterhin und ausdrücklich das aDSG. Ein Ermessens- oder Auslegungsspielraum ist nicht ersichtlich. Auch damit fehlt es dem EDÖB an der Zuständigkeit für das vorliegende Untersuchungsverfahren. Denn – wenn schon – handelt es sich um eine Fortsetzung des alten Verfahrens und nicht um die Eröffnung eines neuen.
- 8 Der EDÖB ist folglich mangels gesetzlicher Grundlage weder für die Eröffnung noch für die Führung des vorliegenden Untersuchungsverfahrens kompetent. Somit ist **Antrag Ziff. 1 der NZZ gutzuheissen** und die vorliegende Sache infolge fehlender Zuständigkeit des EDÖB als abgeschlossen zu betrachten. Im Sinne der Verfahrensökonomie ist hierüber eine **selbständig anfechtbare Zwischenverfügung** zu erlassen.

II. MASSGEBENDER SACHVERHALT UND KORREKTUREN

A. Der zwischen März und Juli 2023 vorgefallene Sachverhalt

- 9 Im März 2023 verübte die Ransomware-Gruppe "Play" auf die NZZ einen Cyber-Angriff. Die NZZ informierte die Öffentlichkeit darüber am gleichen Tag (s. Mitteilung der NZZ vom 24. März 2023, "Cyberangriff

auf das Unternehmen NZZ"). Nach dem damaligen Kenntnisstand waren keine Kundendaten betroffen, sondern Daten einer geringen Anzahl an Mitarbeitern. Diese Mitarbeiter wurden unverzüglich informiert (s. Sachverhaltsfeststellung EDÖB, Rz. 6). Über den Vorfall wurde landesweit und darüber hinaus berichtet.

Beweis:

- Mitteilung der NZZ vom 24. März 2023, "Cyberangriff auf das Unternehmen NZZ"

Beilage 1

- 10 Unmittelbar danach und wie in der Sachverhaltsfeststellung EDÖB richtig festgehalten, am 25. März 2023, informierte die NZZ den EDÖB über die Verletzung der Datensicherheit (act. 1; Sachverhaltsfeststellung EDÖB, Rz. 1, 6). Eine entsprechende Information erfolgte durch die NZZ erneut auch gegenüber der Öffentlichkeit (Information der NZZ vom 25. März 2023, "In eigener Sache: Cyberangriff auf das Unternehmen NZZ"). Am 29. März 2023 bestätigte der EDÖB den Eingang der Meldung vom 25. März 2023 (act. 2; Sachverhaltsdarstellung EDÖB, Rz. 1, 6).

Beweis:

- Information der NZZ vom 25. März 2023, "In eigener Sache: Cyberangriff auf das Unternehmen NZZ"

Beilage 2

- 11 Am 22. April 2023 meldete die NZZ dem EDÖB, dass davon auszugehen sei, dass mehr Daten als ursprünglich angenommen exfiltriert worden seien, namentlich Daten von Mitarbeitern, wobei dies insbesondere eine deutsche Tochtergesellschaft betraf. Die NZZ teilte dem EDÖB mit, dass sie deswegen die Berliner Datenschutzbehörde informiert hat; auch die Öffentlichkeit wurde darüber in Kenntnis gesetzt (s. statt vieler der Beitrag von SRF vom 22. April 2023, "Cyberangriff. Hacker erbeuten bei der NZZ offenbar vertrauliche Personendaten"). Die Sachverhaltsdarstellung EDÖB ist hier nicht präzise (Sachverhaltsfeststellung EDÖB, Rz. 7; act. 3). Bezüglich der öffentlichen Information ist die Sachverhaltsfeststellung EDÖB zu ergänzen.

Beweis:

- Beitrag von SRF vom 22. April 2023, "Cyberangriff. Hacker erbeuten bei der NZZ offenbar vertrauliche Personendaten"

Beilage 3

- 12 Mit E-Mails vom 5. und vom 12. Mai 2023 gab die NZZ dem EDÖB eine Aufdatierung über den bekannten Sachverhalt (Sachverhaltsdarstellung EDÖB, Rz. 8; act. 4, 5). Es wurde in der Öffentlichkeit über die Angelegenheit berichtet (s. statt vieler WOZ Die Wochenzeitung vom 4. Mai 2023, "Hackerangriff. Die NZZ im Cyberdilemma"). Die NZZ selber informierte öffentlich und umfassend am 5. Mai 2023 (Sachverhaltsfeststellung EDÖB, Rz. 9). In der Folge wurden die betroffenen (aktuel-

len) Mitarbeiter über die neuen Erkenntnisse umfassend und unverzüglich informiert. Ihnen wurden Hilfestellungen angeboten und die nötigen Informationen und Handlungsempfehlungen gegeben (Sachverhaltsfeststellung EDÖB, Rz. 12; act. 9–11).

Beweis:

- WOZ Die Wochenzeitung vom 4. Mai 2023, "Hackerangriff. Die NZZ im Cyberdilemma"

Beilage 4

- 13 Mit E-Mail vom 23. Juni 2023 schrieb der EDÖB der NZZ, er "entnehme" ihrer E-Mail vom 12. Mai 2023, dass auch die ehemaligen Mitarbeiter informiert worden seien (act. 8). Diese Information war der E-Mail vom 12. Mai 2023 indessen nicht zu entnehmen. Sie muss vom EDÖB hineininterpretiert worden sein. Diesbezüglich ist die Sachverhaltsfeststellung EDÖB zu ergänzen. Der EDÖB hat in dieser Sache mehrfach E-Mails inkorrekt interpretiert oder inkorrekt wiedergegeben, was einen Einfluss auf den Verlauf des Verfahrens hatte.
- 14 Am 28. Juni 2023 kam es zu einem Telefonat zwischen der NZZ und dem EDÖB, in welchem die NZZ erklärte, dass sie nicht alle ca. 4'000 ehemaligen Mitarbeiter informieren werde (act. 9; Sachverhaltsfeststellung EDÖB, Rz. 13). Der EDÖB fand das nicht richtig, die NZZ war anderer Ansicht. Es folgte eine E-Mail vom 29. Juni 2023 des EDÖB an die NZZ, worin der EDÖB davon sprach, dass auch die ehemaligen Mitarbeiter "ein Anrecht" auf eine aktive Information "haben sollten" (act. 12). Die NZZ verstand dies nachvollziehbarerweise als reine Meinungsäußerung des EDÖB. Die Sachverhaltsfeststellung EDÖB (Rz. 13) stellt dies demgegenüber so dar, als habe der EDÖB der NZZ mitgeteilt, sie müsse alle ehemaligen Mitarbeiter informieren. Von "müssen" war jedoch keine Rede, und schon gar nicht gestützt auf das aDSG. Die Sachverhaltsfeststellung EDÖB (Rz. 13) ist daher nicht korrekt und anzupassen.
- 15 Die NZZ wollte sich nicht auf die aus ihrer Sicht völlig unverhältnismässigen Vorstellungen des EDÖB einlassen. Es gab zu diesem Zeitpunkt auch keinerlei datenschutzrechtliche Pflicht, aktuelle oder ehemalige Mitarbeiter proaktiv zu informieren. Eine solche legte der EDÖB auch in keiner Weise dar. So entschied sich die NZZ, am 3. Juli 2023 42 ehemalige Mitarbeiter der NZZ per E-Mail und postalisch zu informieren (act. 13, 17; Sachverhaltsfeststellung EDÖB, Rz. 14). Die Selektion erfolgte risikobasiert und im Hinblick auf die Möglichkeit der betroffenen Personen, allenfalls in relevanter Weise etwas zu ihrem Schutz tun zu können. Selektiert wurden daher jene Personen, von denen mutmasslich Kopien ihrer Ausweise oder Bankkontodaten entwendet wurden. Sie erhielten zusätzlich zur Information ein Merkblatt mit konkreten Handlungsmöglichkeiten zugesendet. Die Sachverhaltsfeststellung EDÖB ist um die zeitlich korrekte Abfolge und diese Punkte zu

ergänzen, weil diese risikobasierte Selektion in rechtlicher Hinsicht von Relevanz ist.

- 16 Am Tag darauf, mit E-Mail vom 4. Juli 2023, informierte die NZZ den EDÖB über den Versand (act. 13). Aus der beiliegenden E-Mail geht klar hervor, dass die NZZ nur jene ehemaligen Mitarbeiter informierte, die "im Zeitraum zwischen November 2021 und März 2023 Ausweis- und Bankkartenkopien beim HR eingereicht haben". Sie tat also genau das, was sie dem EDÖB angekündigt hatte. Dieser entscheidende Punkt ist in der Sachverhaltsfeststellung EDÖB weggelassen worden. Die Sachverhaltsfeststellung EDÖB ist daher in Rz. 14 dahingehend anzupassen, dass aus dem Schreiben an die Mitarbeitenden, welches dem EDÖB zugestellt wurde, hervorging, dass die NZZ trotz Einwendung des EDÖB daran festhielt, nur diejenigen ehemaligen Mitarbeiter anzuschreiben, bei denen mutmasslich Kopien ihrer Ausweise oder Bankkontodaten entwendet worden sind und nicht alle.
- 17 Dass der EDÖB im Nachgang scheinbar trotzdem davon ausging, dass alle ehemaligen Mitarbeiter informiert wurden (Sachverhaltsfeststellung EDÖB, Rz. 15), ist somit abermals ein Fehler der Sachverhaltsfeststellung EDÖB. Die NZZ vermutet, dass er das Schreiben der NZZ nicht richtig las oder nicht richtig interpretierte (s. schon oben, Rz. 13). Hätte der EDÖB das Schreiben richtig beachtet, wäre ihm klar gewesen, dass die NZZ nicht auf seinen Wunsch einging. Mindestens hätte er Zweifel haben und rückfragen müssen, falls ihm die Sache wirklich wichtig gewesen wäre; die NZZ stand für Rückfragen ausdrücklich zur Verfügung (act. 13). Als es seitens des EDÖB zu keinen Rückfragen kam, der EDÖB seine Untersuchung im Juli 2023 abschloss und auf weitere Schritte verzichtete (Sachverhaltsfeststellung EDÖB, Rz. 1), ging die NZZ davon aus, die Sache sei erledigt. Dies alles ist in der Sachverhaltsfeststellung EDÖB (Rz. 3 und 15) festzuhalten.
- 18 Festzuhalten ist in der Sachverhaltsfeststellung ferner, dass sich **seit Juli 2023 keine neuen Tatsachen ereignet haben**, welche die Eröffnung eines Verfahrens betreffend die Notifikation einer Verletzung der Datensicherheit rechtfertigen würden. Solche werden vom EDÖB auch nicht behauptet.

B. Anfragen beim EDÖB im März 2024

- 19 Am 13. März 2024 gelangte eine Person an den EDÖB mit der Behauptung, dass ein Grossteil der betroffenen Mitarbeiter nicht wisse, dass Daten im Darknet publiziert worden seien. Es handle sich mehrheitlich um Journalisten. Die NZZ habe keine weiteren Schritte unternommen für eine proaktive Information (s. Sachverhaltsfeststellung EDÖB, Rz. 16; act. 14). Diese Behauptungen werden ausdrücklich bestritten.
- 20 Die Behauptung, nicht persönlich angeschriebene ehemalige Mitarbeiter wüssten nicht, dass Daten von ihnen im Darknet stünden, macht auch keinen Sinn. Dies gerade auch vor dem Hintergrund, dass selbst die anzeigende Person offensichtlich Bescheid weiss, wie ihrer Anzeige

zu entnehmen ist (act. 14). Dass die anzeigende Person selbst betroffene Person ist, ist nicht ersichtlich. Sie legt dies nicht dar und behauptet es noch nicht einmal. Daher ist sie rechtlich nicht als betroffene Person zu betrachten und ihr die Information nach Art. 49 Abs. 4 DSGVO zu verweigern. Aus dem Schreiben geht zudem – zumindest in der uns vorliegenden geschwärzten Version – in keiner Weise hervor, dass es sich bei der anzeigenden Person um eine "ehemalig bei der NZZ angestellte Person" handle, wie es der EDÖB in der Sachverhaltsfeststellung EDÖB (Rz. 16) schreibt. Der Sachverhalt ist in dieser Hinsicht gegebenenfalls entsprechend zu korrigieren.

- 21 Über den "Cyberhack bei der NZZ" – einschliesslich der Publikation der hier relevanten Daten im Darknet – ist des Langen und Breiten in den Medien berichtet worden. Ein Journalist der NZZ selbst hat am 17. Februar 2024 so umfassend und schonungslos über den Vorfall und dessen Aufarbeitung berichtet, wie dies noch nie ein Ransomware-Opfer in der Schweiz getan hat.

Beweis:

- NZZ vom 17. Februar 2024, "Kriminelle Hacker greifen die NZZ an und erpressen sie. Das Protokoll einer Krise"

Beilage 5

- 22 Zwei Zitate aus diesem Bericht:

"Die Firma und die Mitarbeiter stehen entblösst da."

"Dass nicht alle Mitarbeiter individuell darüber informiert werden, welche Daten von ihnen im Darknet stehen, stösst weitherum auf Unverständnis."

Die Sachverhaltsfeststellung EDÖB führt mit Ausnahme der Meldung der NZZ vom 5. Mai 2023 (act. 6) keine der zahlreichen Publikationen zum Vorfall auf, weder jene der NZZ selbst noch der anderen Medien (s. oben, Rz. 9 ff. sowie ergänzend und beispielhaft auch: Blick vom 21. bzw. 28. April 2023, "Hacker-Gruppe Play erpresst 'NZZ' – zittern vor Veröffentlichung im Darknet"; Tagesanzeiger vom 3. Mai 2023, "Internetpiraten veröffentlichen Lohnlisten, Erfolgsrechnungen und Passwörter"). Weil diese Publikationen in Bezug auf die Informationslage der betroffenen Personen und damit in rechtlicher Hinsicht entscheidend sind, ist die Sachverhaltsfeststellung EDÖB um diese zu ergänzen.

Beweise:

- Blick vom 21. bzw. 28. April 2023, "Hacker-Gruppe Play erpresst 'NZZ? - zittern vor Veröffentlichung im Darknet'"

Beilage 6

- Tagesanzeiger vom 3. Mai 2023, "Internetpiraten veröffentlichen Lohnlisten, Erfolgsrechnungen und Passwörter"

Beilage 7

- 23 In der Folge erläuterte die NZZ dem EDÖB erneut ihre Risikoabwägung für die selektive Information der betroffenen ehemaligen Mitarbeiter (Sachverhaltsfeststellung EDÖB, Rz. 17; act. 15). Sie wies auch darauf hin, dass zum damaligen Zeitpunkt das alte DSG galt und dieses gar keine Informationspflicht vorsah.
- 24 Mit E-Mail vom 22. April 2024 machte der EDÖB gegenüber der NZZ geltend, bereits unter altem Recht sei sie aufgrund von Art. 4 aDSG zur Information aller Mitarbeiter verpflichtet gewesen (act. 16). Die NZZ wurde gebeten, dem EDÖB bis zum 3. Mai 2024 mitzuteilen, wie die Mitarbeiter informiert worden seien (act. 16). Dies hat die NZZ getan (act. 17). Weder die E-Mail des EDÖB vom 22. April 2024 noch die vorherige enthielt einen Hinweis, dass die NZZ unter dem aktuellen DSG zur Information aller ehemaliger Mitarbeiter verpflichtet sei oder der EDÖB dies verlange.
- 25 Trotzdem wird in der Sachverhaltsfeststellung EDÖB das Gegenteil behauptet, nämlich, dass die NZZ vom EDÖB "aufgefordert" worden sei, alle ehemaligen Mitarbeiter zu informieren (Sachverhaltsfeststellung EDÖB, Rz. 18 sowie S. 1). Weder gab es 2023 oder 2024 eine solche Aufforderung zur Information aller ehemaliger Mitarbeiter, noch hat der EDÖB gegenüber der NZZ je behauptet, das geltende Recht verlange eine solche Information. Daran ändern auch die Aussagen des EDÖB nichts, dass er eine solche Information für angezeigt hielt bzw. hält; der EDÖB verfolgt in Fachkreisen allgemein bekannt seit Jahren eine gefestigte Praxis, von verantwortlichen Stellen wesentlich mehr zu fordern, als das DSG vorsieht.

Beweis:

- Martin Steiger/David Rosenthal, Wie verbindlich ist die Meinung des EDÖB zu Cookies und Künstlicher Intelligenz?, 13. Februar 2024

Beilage 8

- 26 Daher ist in der Sachverhaltsfeststellung EDÖB (Rz. 18 und 20, sowie S. 1) klarzustellen, dass es nie eine Aufforderung des EDÖB gab und auch nie einen Hinweis, wonach geltendes Recht verletzt werde. Diese Klarstellung ist relevant, weil der EDÖB mit der angeblichen Missachtung der nicht existenten Forderung die Eröffnung des vorliegenden Verfahrens begründet (Sachverhaltsfeststellung EDÖB, Rz. 20 und S. 1).

C. Was vom Sachverhalt noch übrig bleibt

- 27 Wie die Sachverhaltsfeststellung EDÖB ausführt, kam es zur Verletzung der Datensicherheit bei der NZZ im März 2023. Sämtliche Vorgänge, die die Datensicherheit, d.h. die Vertraulichkeit, Integrität und Verfügbarkeit von Personendaten beeinträchtigen, gelten als solche (ADRIAN BIERI/JULIAN POWELL, DSG, Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zürich 2023, DSG 5 Bst. h N 2; wir weisen darauf hin, dass es diesen Rechtsbegriff damals noch nicht gab).

- 28 Die Datensicherheitsverletzung umfasst somit den Vorgang des Cyberangriffs auf die NZZ, der die Vertraulichkeit, Integrität und Verfügbarkeit von Personendaten der aktiven und ehemaligen Mitarbeitenden sowie von Kundinnen und Kunden der NZZ durch die Veröffentlichung der Daten im Darknet beeinträchtigt hat. Dieser Vorgang umfasst allerdings nur den Cyberangriff an sich. Dieser wurde mit Veröffentlichung der relevanten Daten im Darknet beendet. Dies geschah am 11. Mai 2023 (NZZ vom 17. Februar 2024, "Kriminelle Hacker greifen die NZZ an und erpressen sie. Das Protokoll einer Krise"; Beilage 5).
- 29 Als Folge der Datensicherheitsverletzung hat die NZZ umfassend informiert. Sie orientierte ohne gesetzliche Pflicht nicht nur den EDÖB, sondern auch Kunden, aktuelle Mitarbeiter und eine Auswahl ehemaliger Mitarbeiter (act. 10, act. 11, act. 13). Die NZZ bot den betroffenen Mitarbeitenden die Möglichkeit, über ein von ihr mandatiertes Anwaltsbüro Auskunft über die sie betreffenden Daten zu erhalten. Hierzu wurde mit hohem Aufwand ein spezielles System betrieben, in welchem entsprechende Abfragen getätigt werden konnten. Die letzten diesbezüglichen Auskunftersuchen gingen dort Ende Juli 2023 ein. Da danach keine Anfragen mehr erfolgten, wurde das System per Ende 2024 aus Kostengründen ausser Betrieb genommen. Selbst aus Sicht der (wirklich) betroffenen Personen ist der Sachverhalt somit abgeschlossen.
- 30 Darüber hinaus hat die NZZ mit der Medienmitteilung vom 11. Mai 2023 bzw. 13. Juli 2023 öffentlich verkündet, dass Personendaten von ehemaligen Mitarbeitenden im Darknet veröffentlicht worden sind. Dies wurde von zahlreichen Medien weiterverbreitet (NZZ vom 11. Mai 2023 bzw. 13. Juli 2023, "Cyberangriff auf das Unternehmen NZZ: Veröffentlichung von NZZ-Daten im Darknet"). Am 17. Februar 2024 berichtete die NZZ nochmals ausführlich über alle Details. Somit wurde auch über die Öffentlichkeit umfassend über die Publikation der Daten im Darknet informiert. Dieser Sachverhalt ist damit ebenfalls abgeschlossen.

Beweis:

- NZZ vom 11. Mai 2023, "Cyberangriff auf das Unternehmen NZZ: Veröffentlichung von NZZ-Daten im Darknet"

Beilage 9

- 31 Bleibt die Frage, was mit den gestohlenen Daten passiert ist. Das weiss der EDÖB offenkundig nicht und hat auch keine Nachforschungen angestellt. Der NZZ sind keinerlei Hinweise bekannt, dass die Daten über deren Diebstahl und Aufschaltung im Darknet hinaus missbraucht worden wären (von einer etwaigen Verwendung durch hiesige Medien abgesehen), geschweige denn jetzt noch eine tatsächliche, realistische Gefahr von ihnen ausgeht: Für die Hacker haben die Daten mit ihrer Veröffentlichung ihren Wert verloren – sie dienten der Erpressung, die nicht funktioniert hat. Ein Interesse, sie für die Nachwelt weiterhin be-

reitzuhalten und damit Platz für Daten weiterer Opfer zu blockieren, haben sie kaum. Selbst wenn sie noch angezeigt werden, nebst Daten aus vielen anderen Raubzügen, ist völlig unklar, ob sie überhaupt in nützlicher Form abrufbar sind. Und selbst Spezialisten gelang es nach ihrer Aufschaltung im Darknet im Mai 2023 nur mit Mühe, eine Kopie zu erstellen – sie brauchten nur schon für den Download der riesigen Datenmenge bereits eine Woche. Der Download selbst genügt zudem nicht für eine Nutzung. Die einzelnen Datensätze müssen aufwändig extrahiert und durchsucht werden; das Darknet ist keine benutzerfreundliche Datenbank, das sich nach Inhalten bestimmter Personen durchsuchen lässt. Das Gegenteil ist der Fall. Selbst die NZZ brauchte erheblichen Aufwand, die Daten durchsuchbar zu machen, um Auskunftsbegehren zu beantworten. Ob sich ausser einigen Journalisten in der Anfangsphase andere Personen die Mühe machten, die Daten nur schon herunterzuladen, mit ungewissem Nutzen, ist zu bezweifeln, scheint aber aufgrund des Gesagten unwahrscheinlich und ist unbelegt. Nach allgemeiner Erfahrung finden Missbräuche – wenn überhaupt – kurz nach Publikation solcher Daten und nicht viele Monate oder Jahre später statt, denn inzwischen sind zahlreiche andere, aktuellere und interessantere Daten publiziert worden. Kurz: Aus dem Umstand der Publikation der Daten im Darknet kann nicht geschlossen werden, dass von ihnen für die betroffenen Personen heute noch – mehr als ein Jahr später – ein relevantes Risiko ausgeht. Ein solches ist jedenfalls durch nichts belegt und reine Spekulation.

- 32 Der EDÖB hat offenbar keine Fälle eines Missbrauchs ermitteln können; die Sachverhaltsfeststellung EDÖB enthält jedenfalls keine Hinweise. In der Sachverhaltsfeststellung EDÖB ist daher festzuhalten, dass keine Anhaltspunkte dafür bestehen, dass es seit dem Diebstahl und der Aufschaltung der Daten der ehemaligen Mitarbeiter zu Missbräuchen gekommen ist oder mit solchen im konkreten Fall vernünftigerweise zu rechnen ist.
- 33 Der für das vorliegende Verfahren relevante Sachverhalt ist also in jeder Hinsicht abgeschlossen.

III. MATERIELLES

A. Übersicht

- 34 Die NZZ war nicht und ist nicht verpflichtet, alle ehemaligen Mitarbeiter über die Verletzung der Datensicherheit zu informieren; ihre bisherige Information genügte. Unter dem aDSG hatte der Gesetzgeber sie nicht vorgesehen (Ziff. B). Das DSG kennt zwar eine solche Pflicht, aber es ist auf unter dem alten Recht abgeschlossene Sachverhalte nicht anwendbar (Ziff. C). Doch selbst, wenn es anwendbar wäre, würde keine solche Pflicht bestehen: Erstens gibt es keine Person, zu deren Schutz eine heutige Information noch erforderlich wäre (Ziff. D). Zweitens wäre die Information, falls sie einst erforderlich gewesen wäre, durch öffentliche Bekanntmachung längst sichergestellt gewesen (Ziff. E.1).

Drittens wäre jede (weitere) Information mit einem unverhältnismässigen Aufwand verbunden (Ziff. E.2).

B. Keine Informationspflicht nach aDSG

- 35 Die Pflicht zur Information über Verletzungen der Datensicherheit wurde erst mit dem revidierten DSG eingeführt. Unter dem aDSG wurde sie nicht geregelt, weder gegenüber dem EDÖB bzw. der betroffenen Person (durch den Verantwortlichen) noch gegenüber dem Verantwortlichen (durch den Auftragsbearbeiter). Je nach Einzelfall war eine Meldepflicht aufgrund des Grundsatzes von Treu und Glauben möglich (ROLAND MATHYS/KENZO THOMANN, in: Blechta/Vasella (Hrsg.), Basler Kommentar Datenschutzgesetz/Öffentlichkeitsgesetz, 4. Aufl., Basel 2024, DSG 24 N 6).
- 36 Schon unter altem Recht ging es dabei immer nur um Fälle, in denen die Information Grundlage konkreter Schutzvorkehrungen vor konkret drohenden Gefahren war, wie etwa die sofortige Sperrung einer gestohlenen Kreditkartennummer (DAVID ROSENTHAL, in: Rosenthal/Jöhri, Handkommentar zum Datenschutzgesetz, Zürich/Basel/Genf 2008, DSG 4 N 16). Die Notwendigkeit solcher Massnahmen stand vorliegend nie zur Diskussion. Nachdem in der Öffentlichkeit bereits breit über die Aufschaltung der Daten im Darknet berichtet worden war, ging selbst die von der NZZ vorgenommene Information der 42 ehemaligen Mitarbeiter über das Erforderliche hinaus.
- 37 Aus dem Grundsatz der Transparenz (Art. 4 [Abs. 4] aDSG), wie der EDÖB dies behauptet hatte (act. 16), wurde eine solche Pflicht jedoch nie hergeleitet, weil dies schon im Ansatz keinen Sinn macht. Die Transparenzpflicht bezüglich des Diebstahls und der Publikation der Daten im Darknet würde als dafür Verantwortliche wenn schon die Hacker treffen, und nicht die NZZ.

C. Keine Anwendbarkeit von Art. 24 Abs. 4 DSG auf vor dem Inkrafttreten abgeschlossene Sachverhalte

- 38 In vorliegenden Verfahren können nur Pflichten gemäss (neuem) DSG geprüft und durchgesetzt werden, vorliegend also nach Art. 24 Abs. 4 DSG. Das neue DSG gilt jedoch erst seit dem 1. September 2023. Weil das Schweizer Recht ein Rückwirkungsverbot ohne ausdrückliche gesetzliche Regelung nicht kennt (s. oben, Rz. 4), ist es nur auf Sachverhalte anwendbar, die sich ab dem 1. September 2023 zugetragen haben. Zu diesem Zeitpunkt war der hier massgeblich relevante Sachverhalt bereits seit zwei Monaten beendet, nämlich mit der Information der Auswahl an ehemaligen Mitarbeiter am 3. Juli 2023. Sie folgte auf die Information der aktuellen Mitarbeiter und jene der Kunden sowie die diversen öffentlichen Bekanntmachungen (s. oben, Rz. 9 ff., Rz. 15 ff.). Der Vorgang ist damit klarerweise bereits abgeschlossen. Selbst wenn die Information damals nach aDSG hätte umfassender erfolgen sollen (wie der EDÖB geltend macht und was – wie oben (Ziff. II.C)

dargelegt – nicht der Fall ist), ändert das nichts dran, dass dieser Vorgang beendet ist.

- 39 Der EDÖB erklärte seine damalige Untersuchung ebenfalls als im Juli 2023 abgeschlossen (s. oben, Rz. 17). Dass er dies womöglich nur tat, weil er eine E-Mail der NZZ nicht genau las, ändert nichts daran, dass die Untersuchung bei Inkrafttreten des (neuen) DSG längst beendet war. Wenn er nun versucht, diese alte Sache wieder "aufzuwärmen", dann lässt er damit materiell die damalige Untersuchung wieder aufleben und müsste diese – im Einklang mit Art. 70 DSG – konsequenterweise unter dem aDSG durchführen. Anderes wäre nur denkbar, wenn die Untersuchung aufgrund echter neuer Erkenntnisse wieder aufgenommen worden wäre – was vorliegend aber nicht der Fall ist. Auch aus diesem Grund ist das (neue) DSG somit auf den vorliegenden Sachverhalt nicht anwendbar.
- 40 Selbst wenn alle Meldungen und Informationen der NZZ bis und mit Juli 2023 weggedacht werden, könnte der EDÖB das vorliegende Verfahren unter dem (neuen) DSG nur und erst dann führen, wenn er nachweisen kann, dass sich seit dem 1. September 2023 ein relevanter Sachverhalt ereignet hat. Das hat er jedoch nicht im Ansatz getan. Es gibt keinerlei Belege dafür, dass die damals gestohlenen Daten noch irgendwo in vernünftigerweise nutzbarer Form abrufbar sind, sie die ehemaligen Mitarbeiter betreffen, ein konkretes Risiko von Missbräuchen dieser Daten bestehen, geschweige denn, welche konkreten Schutzmassnahmen gegen diese nicht nachgewiesenen Missbrauchsmöglichkeiten welche betroffenen Personen konkret treffen könnten und würden. Die Sachverhaltsfeststellung EDÖB äussert sich schlicht nicht dazu. Der Umstand, dass es bis heute keine Anzeichen von Missbräuchen gibt, zeigt, dass es schon an einem relevanten Sachverhalt für das (neue) DSG fehlt.

D. Keine Verletzung von Art. 24 Abs. 4 DSG

1. Betroffene müssen nur ausnahmsweise informiert werden

- 41 Selbst wenn vorliegend das (neue) DSG zur Anwendung gelangen sollte, was nicht der Fall ist, wäre zu prüfen, ob Art. 24 Abs. 4 DSG im vorliegenden Fall überhaupt verletzt wäre, d.h. die noch nicht direkt und persönlich informierten ehemaligen Mitarbeiter so zu informieren wären.
- 42 Eine Information der Betroffenen muss gemäss Art. 24 Abs. 4 DSG nur aber immerhin erfolgen, falls und wenn ihr Schutz dies erfordert. Hat die Datensicherheitsverletzung ein hohes Risiko für die betroffene Person zur Folge, löst dies grundsätzlich die Meldepflicht nach Art. 24 Abs. 1 DSG gegenüber dem EDÖB aus. Gegenüber der betroffenen Person muss jedoch keine Information erfolgen, wenn dies zu ihrem Schutz nicht erforderlich ist (BSK-MATHYS/THOMANN, DSG 24 N 63). Betroffene müssen insbesondere informiert werden, wenn sie dadurch Vorkehrungen treffen können, um einen weiteren Schaden zu verhüten.

dern (BSK-MATHYS/THOMANN, DSG 24 N 5). Der Zweck der Meldepflicht liegt nämlich nicht primär in der Schaffung von Transparenz, sondern in der Befähigung des Einzelnen, sich nach Möglichkeit selbst vor den Folgen zu schützen oder diese abzumildern (BSK-MATHYS/THOMANN, DSG 24 N 64). Die Meldung an den EDÖB sowie die Information der betroffenen Personen müssen demnach zeitnah bzw. innert nützlicher Frist erfolgen. Denn die von den Betroffenen zu ergreifenden Massnahmen zu ihrem Schutz müssen noch dazu beitragen können, das aus der Verletzung der Datensicherheit hervorgehende Risiko zu beseitigen oder zu vermindern (vgl. OFK-BIERI/POWELL, DSG 24 N 18 m.w.H.). Die Information zum Schutz der betroffenen Personen ist also dann nicht erforderlich, wenn sich die negativen Folgen bereits verwirklicht haben oder wenn die betroffene Person nichts Relevantes (mehr) dagegen ausrichten kann (BSK-MATHYS/THOMANN, DSG 24 N 68).

- 43 Insgesamt gilt, dass die Information der betroffenen Personen nur ausnahmsweise erforderlich sein soll (DAVID ROSENTHAL, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020, Rz. 166, m.w.H.). Wo der Schaden schon angerichtet oder die betroffene Person bereits im Bilde ist oder selbst nichts Relevantes tun kann, besteht keine Informationspflicht (ebd.). Der EDÖB kann nach Art. 24 Abs. 4 DSG zwar eine Information der betroffenen Personen anordnen, doch ist auch dies nur dort möglich, wo überhaupt eine Informationspflicht besteht (BSK-MATHYS/THOMANN, DSG 24 N 70). Er kann die Informationspflicht inhaltlich also nicht ausdehnen, wenn er das selbst für angezeigt erachten würde, wie er dies bisher so vertrat.

2. Information der ehemaligen Mitarbeiter ist schon erfolgt – der Weg spielt keine Rolle

- 44 Vorliegend steht zur Diskussion, ob alle ehemaligen Mitarbeiter der NZZ heute noch, d.h. anderthalb Jahre nach dem Diebstahl und Aufschalten ihrer Daten, von ihr darüber informiert werden müssen.
- 45 Zunächst ist festzuhalten, dass über die breite öffentliche Kommunikation über den Vorfall die ehemaligen Mitarbeiter bereits informiert worden sind, sei es über die Mitteilungen und Berichte der NZZ, sei es über die Berichterstattung anderer Medien (s. oben, Rz. 9 ff.). An dieser Berichterstattung gab es zum damaligen Zeitpunkt kein Vorbeikommen. Es darf also davon ausgegangen werden, dass auch die ehemaligen Mitarbeiter aus der Presse wussten, dass ihre Daten mutmasslich im Darknet gelandet waren. Wer es damals nicht realisierte, erfuhr davon durch spätere Berichterstattungen. Auch die Person, die Anzeige erstattet hat, war offenkundig bestens im Bilde (act. 14). Sie ärgerte sich darüber, dass keine persönliche Information durch die NZZ erfolgte, doch diesen Anspruch sieht Art. 24 Abs. 4 DSG nicht vor. Ist eine betroffene Person im Bilde – auf welchem Weg auch immer – kommt Art. 24 Abs. 4 DSG nicht mehr zum Tragen. Schon aus diesem Grund ist eine (neuerliche) Information aller ehemaliger Mitarbeiter nicht mehr erforderlich.

3. Heutige Information aller ehemaliger Mitarbeiter ist zu deren Schutz nicht erforderlich

- 46 Damit die Pflicht zu einer solchen Information heute noch gegeben wäre, müsste nachgewiesen werden, dass alle ehemaligen Mitarbeiter mit einer solchen Information überhaupt erst in die Lage versetzt würden, in relevanter Weise die negativen Folgen des Diebstahls und der damaligen Aufschaltung ihrer Daten im Darknet zu beseitigen oder zu mildern. Nur dann wäre die Information zu ihrem Schutz erforderlich.
- 47 Es geht dabei nicht um Massnahmen, die einzelne Betroffene gegen einen allfälligen konkreten Missbrauch ihrer Daten ergreifen könnten, sollte es zu solchen kommen (wovon wir bisher nichts wissen, s. oben, Rz. 31 f.). Es geht hier einzig um Massnahmen, die Betroffene *präventiv* ergreifen könnten, würde ihnen die NZZ die gemäss Art. 24 Abs. 4 DSG vorgesehenen Informationen heute zukommen lassen. Dies sind nach Art. 15 Abs. 3 Datenschutzverordnung ("**DSV**") Angaben (i) zur Art der Verletzung, (ii) zu den Folgen, einschliesslich der allfälligen Risiken für sie, (iii) welche Massnahmen die NZZ selbst getroffen hat oder vorgesehen sind, um den Mangel zu beheben oder die Folgen zu mindern und (iv) den Namen und die Kontaktdaten einer Ansprechperson.
- 48 Solche Massnahmen sind vorliegend nicht ersichtlich. Nicht nur ist der Schaden, soweit es ihn gibt, bereits angerichtet. Auch wären die ehemaligen Mitarbeiter mit diesen Informationen nicht besser in der Lage, sich vor etwaigen weiteren Schäden zu schützen, so überhaupt heute noch mit solchen zu rechnen ist (was bestritten wird, s. oben, Rz. 31 f.). Das erstaunt nicht, denn mit Art. 24 Abs. 4 DSG hatte der Gesetzgeber ganz andere Fallkonstellationen im Blick. Es ging dabei um konkrete Schutzvorkehrungen wie die Anpassung von Passwörtern oder die Sperrung von Kreditkarten, die mit einer solchen zeitnahen Information ermöglicht werden sollten. Eine Information anderthalb Jahre nachdem alles bekannt wurde, hatte der Gesetzgeber definitiv nicht im Sinn, und erst recht nicht eine Information nach dem Giesskannenprinzip, wie sie der EDÖB vertritt. Der Gesetzgeber sah das Gegenteil vor: Eine zeitnahe Information, und auch diese nur als Ausnahmefall.
- 49 Nicht einmal das immer wieder zitierte Risiko von Phishing-Angriffen hilft dem EDÖB hier weiter. Denn dieses besteht immer, mit und ohne Datendiebstahl. Dass die hier gestohlenen Daten für solche verwendet werden, ist zudem reine Spekulation, da es in den anderthalb Jahren keinerlei Hinweise auf solche Aktivitäten gab, die über das übliche Mass hinaus gingen oder auf den Datendiebstahl zurückgeführt werden müssten. Hätten die Hacker solche Missbräuche beabsichtigt, wäre es schon längst dazu gekommen. Zudem könnten die ehemaligen Mitarbeiter diesbezüglich höchstens aufgerufen werden, in der elektronischen Kommunikation wachsam zu sein. Dieser Rat gilt allerdings so oder so und kann eine nachträgliche Information, wie sie der EDÖB

will, nicht rechtfertigen. Die Information hätte schlicht keine relevante positive Wirkung.

- 50 Ganz im Gegenteil: Würde heute, mehr als anderthalb Jahre nach dem Cyberangriff, informiert, würde dies in erster Linie für Verunsicherung und Angst sorgen. Nicht wenige würden sie vermutlich sogar für einen Phishing-Versuch halten. Selbst wenn der EDÖB 2023 Recht gehabt hätte, und eine Information aller ehemaligen Mitarbeiter angezeigt gewesen wäre (was die NZZ bestreitet), wäre es schlicht unsinnig und kontraproduktiv, dies jetzt nachzuholen. Darum verlangen andere Datenschutzaufsichtsbehörden solches auch nicht.
- 51 Jene ehemaligen Mitarbeiter, die womöglich tatsächlich etwas zu ihrem Schutz tun konnten, sind längst informiert und sogar mit konkreten Empfehlungen versorgt worden (s. oben, Rz. 15). Selbst in diesen Fällen stellt sich die Frage, ob diese damalige Information selbst nach dem (neuen) DSG tatsächlich erforderlich gewesen wäre. Die NZZ wollte jedoch auf Nummer sicher gehen.

E. Ausnahme nach Art. 24 Abs. 5 DSG gegeben

1. Öffentliche Bekanntmachung ist erfolgt

- 52 Nach Art. 24 Abs. 5 Bst. c DSG ist eine Information der betroffenen Person nicht erforderlich, wenn deren Information durch eine öffentliche Bekanntmachung "in vergleichbarer Weise" sichergestellt ist. Es ist somit nicht zwingend, jede betroffene Person individuell zu erreichen. Vielmehr reicht es aus, dass die öffentliche Bekanntmachung mindestens ähnlich wirksam ist, wie eine individuelle Notifikation. Über welchen Kanal eine solche öffentliche Bekanntmachung stattzufinden hat, ist nicht vorgegeben, sondern hängt von den Eigenschaften der betroffenen Personengruppen ab (OFK-BIERI/POWELL, DSG 24 N 23; BSK-MATHYS/THOMANN, DSG 24 N 93 f.). Wenn es sich bei den betroffenen Personen um Angestellte und Kunden einer bestimmten Zeitung handelt, ist genau diese Zeitung als Kanal für eine solche Bekanntmachung prädestiniert.
- 53 Genau dies ist vorliegend nicht nur ein Mal, sondern mehrere Male geschehen. Wir verweisen auf die öffentlichen Verlautbarungen der NZZ auch speziell an die ehemaligen Mitarbeitenden auf ihrer Website, der Berichterstattung in der NZZ und in den zahlreichen anderen Medien, und zuletzt im ausführlichen Beitrag der NZZ vom 17. Februar 2024. Da es sich bei den ehemaligen Mitarbeitern mehrheitlich um Journalisten handelt, ist erst recht davon auszugehen, dass sie diese Berichte und Verlautbarungen zur Kenntnis genommen haben und daher hinreichend im Bilde sind.
- 54 Damit ist die Ausnahme von Art. 24 Abs. 5 Bst. c DSG gegeben, und es müssen die ehemaligen Mitarbeiter bereits aus diesem Grund nicht mehr informiert werden.

2. Unverhältnismässigkeit der Information

- 55 Eine Information der betroffenen Personen ist ebenfalls nicht erforderlich, wenn die Information gemäss Art. 24 Abs. 5 Bst. b DSG unmöglich ist oder einen unverhältnismässigen Aufwand erfordert. Von einem unverhältnismässigen Aufwand ist z.B. auszugehen, wenn eine grosse Anzahl betroffener Personen individuell informiert werden müsste, wobei die dadurch entstehenden Kosten im Verhältnis zum Informationsgewinn für die einzelnen Personen unverhältnismässig wären (Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941, S. 7065; BSK-MATHYS/THOMANN, DSG 24 N 90).
- 56 Vorliegend müssten ca. 4'000 ehemalige Mitarbeitende individuell informiert werden (s. Sachverhaltsfeststellung EDÖB, Rz. 13). Bei vielen fehlen aktuelle Kontaktangaben. Sie müssten in einem enormen Aufwand aufgearbeitet werden. Müsste nur schon bei der Hälfte je eine halbe Stunde dafür verwendet werden, würde dies einen personellen Aufwand von 25 Personenwochen bzw. rund ein halbes Personenjahr benötigen. Den ehemaligen Mitarbeitenden könnte jedoch nicht mehr mitgeteilt werden als bisher (und als ihnen bekannt sein wird), nämlich dass Personendaten 2023 gestohlen und im Darknet aufgeschaltet wurden. Wie zuvor ausgeführt wurde, können die Betroffenen sich mit dieser heutigen Information sich nicht wirklich besser oder anders schützen, als sie das bisher konnten, weshalb eine individuelle Information angesichts des fehlenden Nutzens für die Betroffenen einen unverhältnismässigen Aufwand darstellt.
- 57 Damit fällt eine Informationspflicht auch nach Art. 24 Abs. 5 Bst. b DSG ausser Betracht.

F. Der EDÖB widerspricht sich selbst

- 58 Mit seiner bisherigen Beurteilung im Fall der NZZ widerspricht der EDÖB sich selbst.
- 59 In seinen Schlussberichten zum Ransomware-Angriff auf das Unternehmen Xplain, bei dem im Mai 2023 Personendaten der Bundesverwaltung im Darknet publiziert wurden, führte er zunächst aus, dass im aDSG keine ausdrückliche Bestimmung zur Meldung bestehe. Da der EDÖB über den Ransomware-Vorfall informiert wurde, könne offenbleiben, ob sich eine Meldepflicht nach Treu und Glauben und der allgemeinen Informationspflicht ergeben hätte (Schlussbericht und Empfehlungen vom 25. April 2024 des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) in Sachen BAZG aufgrund Ransomware-Vorfall, Rz. 106; Schlussbericht und Empfehlungen vom 25. April 2024 des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) in Sachen fedpol aufgrund Ransomware-Vorfall, Rz. 143). Gemäss dem Schlussbericht in Sachen BAZG informierte dieses zudem nur diejenigen Personen "direkt und aktiv", "die nach dem risikobasier-

ten Ansatz als mit 'erhöhtem Risiko' beurteilt wurden" (Schlussbericht und Empfehlungen vom 25. April 2024 des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) in Sachen BAZG aufgrund Ransomware-Vorfall, Rz. 49; in diesem Zusammenhang informierte auch das Bundesamt für Justiz gem. einer Information auf der Website nur "besonders betroffene Personen" direkt, s. Bundesamt für Justiz vom 7. September 2023, "Information zum Datenabfluss bei Xplain"). Zusammen mit einer Information der involvierten Stellen und einem auf der Website publizierten Kontaktformular für Rückfragen erachtete der EDÖB die "Informationspflichten" als "nach Treu und Glauben wahrgenommen" (Schlussbericht und Empfehlungen vom 25. April 2024 des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten [EDÖB] in Sachen BAZG aufgrund Ransomware-Vorfall, Rz. 107). Der EDÖB verlangte gemäss Bericht also keine individuelle Information aller Betroffenen, deren Personendaten in den Leaks auch noch enthalten waren.

Beweis:

- Bundesamt für Justiz vom 7. September 2023, "Information zum Datenabfluss bei Xplain"

Beilage 10

- 60 Diesen risikobasierten Ansatz verfolgte auch die NZZ, die überdies jene ehemaligen Mitarbeiter mit einem aus ihrer Sicht erhöhten Risiko eines Missbrauchs persönlich informierte. Weshalb der EDÖB nun von der NZZ auch die persönliche Information aller anderen der 4'000 ehemaligen Mitarbeiter verlangt, während der EDÖB dies im oben genannten Fall nicht als nötig erachtete, ist nicht nachvollziehbar. Die Haltung, dass die NZZ alle ehemaligen Mitarbeiter informieren sollte, vertrat er dabei bereits unter dem aDSG.

IV. ZU DEN ANTRÄGEN

A. Fehlende Zuständigkeit (Antrag Ziff. 1)

- 61 Wie die NZZ gezeigt hat, fehlt es dem EDÖB für das vorliegende Untersuchungsverfahren an der Zuständigkeit. Hierüber ist mit einer anfechtbaren Verfügung zu entscheiden.

B. Eventualiter Gegenstandslosigkeit (Antrag Ziff. 2)

- 62 Sollte der EDÖB wider Erwarten und entgegen der Verfahrensökonomie nicht selbständig über Antrag 1 entscheiden, ist das vorliegende Untersuchungsverfahren als gegenstandslos geworden abzuschreiben.

C. Kosten (Antrag Ziff. 3)

- 63 Entsprechend dem Ausgang des Verfahrens sind der NZZ keine Kosten aufzuerlegen.

VISCHER

Aufgrund obiger Ausführungen ersuchen wir Sie, sehr geehrter Herr Lobsiger, sehr geehrte Damen und Herren, um antragsgemässen Entscheid.

Mit freundlichen Grüssen



David Rosenthal



Adrian Gautschi

Beweismittel gemäss separatem Verzeichnis

**Beweismittelverzeichnis zur Stellungnahme
vom 27. September 2024
EDÖB / NZZ**

Beilagenverzeichnis

Beilage 1	Mitteilung der NZZ vom 24. März 2023, "Cyberangriff auf das Unternehmen NZZ"
Beilage 2	Information der NZZ vom 25. März 2023, "In eigener Sache: Cyberangriff auf das Unternehmen NZZ"
Beilage 3	Beitrag von SRF vom 22. April 2023, "Cyberangriff. Hacker erbeuten bei der NZZ offenbar vertrauliche Personendaten"
Beilage 4	WOZ Die Wochenzeitung vom 4. Mai 2023, "Hackerangriff. Die NZZ im Cyberdilemma"
Beilage 5	NZZ vom 17. Februar 2024, "Kriminelle Hacker greifen die NZZ an und erpressen sie. Das Protokoll einer Krise"
Beilage 6	Blick vom 21. bzw. 28. April 2023, "Hacker-Gruppe Play erpresst 'NZZ? - zittern vor Veröffentlichung im Darknet"
Beilage 7	Tagesanzeiger vom 3. Mai 2023, "Internetpiraten veröffentlichen Lohnlisten, Erfolgsrechnungen und Passwörter"
Beilage 8	Martin Steiger/David Rosenthal, Wie verbindlich ist die Meinung des EDÖB zu Cookies und Künstlicher Intelligenz?, 13. Februar 2024
Beilage 9	NZZ vom 11. Mai 2023, "Cyberangriff auf das Unternehmen NZZ: Veröffentlichung von NZZ-Daten im Darknet"
Beilage 10	Bundesamt für Justiz vom 7. September 2023, "Information zum Datenabfluss bei Xplain"

NZZ

24. März 2023

Cyberangriff auf das Unternehmen NZZ

Aufgrund eines Cyberangriffs durch Ransomware stehen zurzeit einige Systeme und Services des Unternehmens NZZ nicht zur Verfügung.

Der Angriff konnte frühzeitig erkannt und isoliert werden. Aktuell wird er von der NZZ IT zusammen mit externen Spezialisten und Experten des NCSC und der KAPO Zürich analysiert.

Weitere Informationen:

NZZ-Unternehmenskommunikation

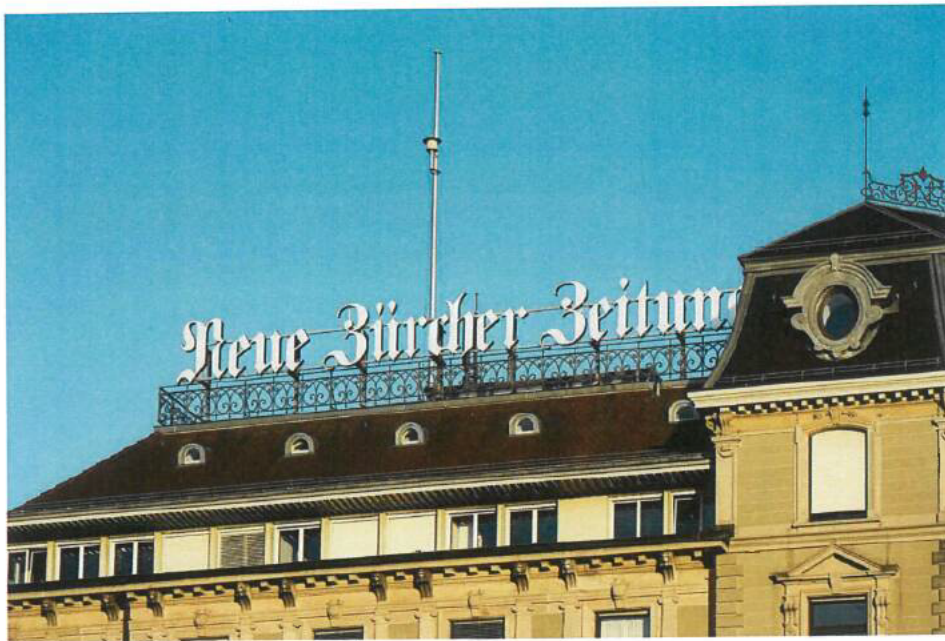
+41 44 258 17 72, unternehmenskommunikation@nzz.ch (<mailto:unternehmenskommunikation@nzz.ch>)

Service

NZZ

In eigener Sache: Cyberangriff auf das Unternehmen NZZ

25.03.2023, 05:15 Uhr ⌚ 1 min



Die heutige NZZ-Ausgabe erscheint aufgrund eines Cyberangriffs in leicht reduziertem Umfang.

Goran Basic

%%. Aufgrund eines Cyberangriffs durch Ransomware stehen zurzeit einige Systeme und Services des Unternehmens NZZ nicht zur Verfügung. Der Angriff konnte frühzeitig erkannt werden. Aktuell wird er von der NZZ IT zusammen mit externen Spezialisten und Experten des Nationalen Zentrums für Cybersicherheit (NCSC) und der Kantonspolizei Zürich analysiert. Infolgedessen erscheint die heutige Zeitung in leicht reduziertem Umfang. Davon betroffen ist auch das E-Paper, das nur eingeschränkt nutzbar ist. Wir bedauern dies ausserordentlich.

Wir setzen alles daran, dass Sie, geschätzte Leserinnen und Leser, so bald wie möglich wieder von unserem gewohnten Angebot profitieren können. Unser volles Angebot können Sie weiterhin unter [nzz.ch](https://www.nzz.ch) und in der NZZ-App nutzen.

Neueste Artikel >



KURZMELDUNGEN

News aus Zürich: Tigermücken breiten sich in Quartieren aus – Bevölkerung soll bei Bekämpfung helfen

Aktualisiert vor 2 Stunden



INTERAKTIV

Neukunden zahlen für Gas so viel wie zuletzt im Herbst 2023 – Zahlen zur Energieversorgung in Deutschland, täglich aktualisiert

Aktualisiert vor 2 Stunden ⌚ 9 min





Mini Cooper SE: Elektrischer Fahrspass mit minimalistischem Design

vor 2 Stunden ⌚ 4 min



KURZMELDUNGEN

Deutschland: Scholz und Pistorius stellen Iris-T-System in Dienst +++ Bürgergeld steigt 2025 nicht weiter an

Aktualisiert vor 3 Stunden



KURZMELDUNGEN

Deutschland: 9-Euro-Ticket sorgte für verspätete Züge statt weniger Autoverkehr

Aktualisiert vor 3 Stunden



Gegen die Puschkinisierung des Angriffskriegs – Michail Schischkin ist seine Heimat Russland fremd geworden. Die russische Literatur aber lässt er sich nicht nehmen

04.09.2024 ⌚ 3 min



Für Sie empfohlen >



Mini Cooper SE: Elektrischer Fahrspass mit minimalistischem Design

vor 2 Stunden ⌚ 4 min



Pro

Killer gegen Normalos – wie Gefangenendeals zum neuen Geschäftsmodell werden

04.09.2024 ⌚ 7 min



NZZ AKZENT

Indiens wahrer König ist ein Bollywood-Star

04.09.2024 🔊 18 min



DIE NEUSTEN ENTWICKLUNGEN

Migrationskrise in Europa: Mindestens zwölf Tote bei Kentern eines Flüchtlingsboots im Ärmelkanal

03.09.2024



Tinkturen der Arnika hemmen Entzündungen und lindern Schmerzen – doch der Heilpflanze droht das Aus

03.09.2024 ⌚ 3 min





75 Jahre Currywurst: Sie braucht nicht viel, riecht nach ehrlicher Arbeit, Wirtschaftswunder und der alten BRD

04.09.2024 ⌚ 4 min



Eigenartige Differenz bei Schweizer Wachstumszahlen: Warum Cristiano Ronaldo und Simone Biles das BIP der Schweiz erhöhen

04.09.2024 ⌚ 4 min



INTERVIEW

«Biodiversität dem Klima zu opfern, ist verrückt», sagt der Naturschutzbiologe

03.09.2024 ⌚ 8 min



Copyright © Neue Zürcher Zeitung AG. Alle Rechte vorbehalten. Eine Weiterverarbeitung, Wiederveröffentlichung oder dauerhafte Speicherung zu gewerblichen oder anderen Zwecken ohne vorherige ausdrückliche Erlaubnis von Neue Zürcher Zeitung ist nicht gestattet.

News > Schweiz >

Cyberangriff

Hacker erbeuten bei der NZZ offenbar vertrauliche Personaldaten

Samstag, 22.04.2023, 12:28 Uhr

TEILEN

Ein Cyberangriff auf den Verlag der Neuen Zürcher Zeitung (NZZ) vor einem Monat ist gravierender als bisher angenommen.

Die Hackergruppe hat dem Unternehmen zufolge vermutlich vertrauliche Daten von Mitarbeitenden erbeutet und droht mit der Publikation im Internet.

Nach Medienberichten verlangen die Hacker von der NZZ ein Lösegeld.



Archiv: Hacker-Angriff auf NZZ und CH Media

03:10 min, aus Rendez-vous vom 28.03.2023.

Bild: KEYSTONE/Christian Beutler

Eine Gruppe unter dem Namen «Play» habe sich zu dem Cyberangriff bekannt und im Darknet angekündigt, im Besitz der Daten zu sein. Dies teilte die NZZ der Nachrichtenagentur Keystone-SDA am Samstag auf Anfrage mit. Das Unternehmen bestätigte entsprechende Medienberichte. Es bestehe die Möglichkeit, dass die Daten ab Montag veröffentlicht würden.

Cyberattacke mit Ransomware

Die Hacker wollen laut eigenen Angaben Daten etwa zu Löhnen, Projekten und Mitarbeitenden publizieren. Sie nennen den 24. April als Datum. Nach Informationen von Keystone-SDA forderten die Hacker von der NZZ ein Lösegeld. Das Unternehmen äusserte sich nicht dazu.

Ausmass des Angriffs noch unbekannt

Wie gross das Ausmass des Diebstahls ist, sei Gegenstand von Abklärungen, schrieb die NZZ. Das Unternehmen arbeitet bei dem Vorfall mit den zuständigen Behörden, der Polizei und eigenen Cybersicherheitsexperten zusammen.



Die Hackergruppe hat offenbar Personaldaten gestohlen und will sie in den kommenden Tagen veröffentlichen. (Bild vom NZZ-Standort nahe dem Opernhaus Zürich)

KEYSTONE/WALTER BIERI

Die gemeinsamen IT-Systeme der Verlage NZZ und CH Media waren am 24. März von Cyberkriminellen angegriffen worden. In der Folge mussten die drei Titel Aargauer Zeitung, Luzerner Zeitung und St. Galler Tagblatt vorübergehend auf die unterschiedlichen Regionalteile, sogenannte Splitausgaben, verzichten. Die NZZ erschien an einzelnen Tagen ebenfalls reduziert. Inzwischen erscheinen die Zeitungen wieder wie gewohnt.

SRF 4 News, 22.04.2023, 14 Uhr ; sda/spic;fla

Mehr zum Thema



Zwei Wochen nach Cyberangriff

Cyberangriff: NZZ muss System für Zeitungsproduktion abschalten

08.04.2023

Mit Audio



Cyberattacke hat weiter Folgen

«NZZ will Lösegeldforderung wohl nicht nachkommen»

06.04.2023

Mit Audio



Im Fokus von Hackern

NZZ kämpft noch immer mit Cyberangriff

28.03.2023

Mit Video



Cyberangriff auf NZZ

Hackerangriff trifft verschiedene Systeme der NZZ und CH Media

24.03.2023

Mit Audio

TEILEN



Jederzeit top informiert!

Erhalten Sie alle News-Highlights direkt per Browser-Push und bleiben Sie immer auf dem Laufenden, **Mehr**

AKTIVIEREN

Meistgelesene Artikel



Krise bei Berner Inselgruppe
«Die Lage beim Berner Inselspital ist dramatisch»

Über
«Si

Suchen

Home

News

Sport

Meteo

Kultur

Dok

Wissen

[Play SRF Mediathek](#)

[Audio & Podcasts](#)

[Play Suisse](#)

[TV-Programm](#)

[Radio-Programm](#)

[Archiv](#)

[Verkehr](#)

[Kids](#)

[SRF school](#)

[Newsletter](#)

[Hallo SRF!](#)

[Über SRF](#)

[Radio SRF 1](#)

[Radio SRF 2 Kultur](#)

[Radio SRF 3](#)

[Radio SRF 4 News](#)

[Radio SRF Musikwelle](#)

[Radio SRF Virus](#)

[Radio Swiss Classic](#)

[Radio Swiss Jazz](#)

[Radio Swiss Pop](#)

[SRF Apps](#)

[Korrekturen](#)

[Hilfe](#)

[Medien](#)

[Datenschutzerklärung](#)

[Themenliste](#)

[Jobs](#)

[Kontakt](#)

[Impressum](#)

[Datenschutz-Einstellungen](#)

Nutzungsbedingungen



SRF Schweizer Radio und Fernsehen,
Zweigniederlassung der Schweizerischen Radio- und Fernsehgesellschaft

RTS

RSI

RTR

SWI

3SAT

Nr. 18 – 4. Mai 2023

Hackerangriff**Die NZZ im Cyberdilemma**

Die Hacker:innenbande Play ist in die Computer der NZZ-Mediengruppe und von CH Media eingedrungen und hat Daten gestohlen. Am Mittwoch veröffentlichte sie eine erste Tranche. Wer steckt hinter dem Angriff?

Von Thomas Schwendener

Die Informatikabteilung der NZZ blickt auf turbulente Wochen zurück. Am 27. März wurden das Zürcher Medienhaus sowie der Verlag CH Media von einem Cyberangriff heimgesucht: Kriminelle verschlüsselten Systeme der beiden Unternehmen mit sogenannter Ransomware. Obwohl die NZZ mitteilte, der Angriff habe frühzeitig erkannt und isoliert werden können, erschienen verschiedene gedruckte Ausgaben in reduziertem Umfang. Erst vier Wochen nach dem Angriff wurden die Regionalbünde der «Aargauer Zeitung», der «Luzerner Zeitung» und des «St. Galler Tagblatts» wieder vollständig ausgeliefert.

Die Titel von CH Media erlitten gewissermassen einen Kollateralschaden: Das Aarauer Medienhaus bezieht IT-Dienstleistungen der NZZ-Mediengruppe und hat mit Andreas Bossecker denselben Informatik- und Technologiechef. Dieser dürfte auch heute noch schlecht schlafen: So fielen am letzten Donnerstag die Websites der beiden Medienkonzerne komplett aus. Rund eine halbe Stunde war statt Artikeln bloss eine Fehlermeldung zu sehen. Die NZZ beeilte sich, auf eine «technische Ursache» hinzuweisen: Man arbeite intern an den Systemen, der Ausfall habe mit dem Cyberangriff nichts mehr zu tun.

Doch die Geschichte ist längst nicht ausgestanden. Ransomwarebanden verschlüsseln nicht nur die Systeme ihrer Opfer, sondern stehlen auch deren Daten – und drohen mit einer Veröffentlichung, sollte kein Lösegeld fliessen. So auch die Bande Play, die sich zum Angriff auf die Schweizer Medienhäuser bekannt hat. Die Gruppe behauptet, vertrauliche Informationen, Projektangaben, Inhaltslisten und Auskünfte über Mitarbeitende erbeutet zu haben. Am Mittwoch sind erste Daten im Darknet aufgetaucht, einem Bereich

des Internets, der nur mit speziellen Browsern zugänglich ist und nicht von Suchmaschinen wie Google durchforstet wird.

Die Dynamik in den Medien

Die NZZ steht unter Druck: Liess das Unternehmen zu Beginn kurz und knapp verlauten, man habe die Sache im Griff, hiess es später in einer Mitteilung an die Mitarbeitenden, es seien mehr Daten erbeutet worden als vorerst vermutet. In der Beute der Kriminellen befänden sich wohl auch vertrauliche Informationen, zitierte der «Blick» aus dem Memo.

Der Angriff sorgt für eine Berichterstattung wie sonst kaum ein Cybervorfall in der Schweiz. Auf der Darknetsite von Play heisst es an die Opfer gerichtet: «Journalisten und andere werden Ihre Dokumente durchforsten und darin Ungereimtheiten oder Verstösse finden.»

Play hatte das Datum für die Veröffentlichung der Informationen mehrfach verschoben. Das deutet auf laufende Verhandlungen hin. Ob derzeit Gespräche stattfinden, wollte die NZZ auf Anfrage nicht mitteilen.

Die am Mittwoch veröffentlichten Daten umfassen E-Mails, Budgets, Infos über Mitarbeiter:innen und Protokolle der Vertriebsorganisation von CH Media, so etwa jenes einer Verwaltungsratssitzung, in der es um GAV-Verhandlungen und Auflageentwicklung geht.* Falls keine Reaktion erfolge, würden die gesamten Daten publiziert, wird gedroht. Der Umfang dessen, was Play tatsächlich erbeutet hat, bleibt vorerst unklar. Dieses Vorgehen ist von Ransomwarebanden bekannt: Play will den Druck auf die Medienhäuser erhöhen.

Diese befinden sich in einer Zwickmühle. Entweder sie riskieren eine unfreiwillige Nabelschau – wobei sie kaum wissen dürften, welche Daten genau entwendet wurden –, oder sie bezahlen und unterstützen damit das Geschäft der kriminellen Bande, die sich mit dem Geld neue Ressourcen für ihre Feldzüge beschaffen kann. Zahlungsbereite Opfer werden zudem oftmals erneut von Ransomwarebanden heimgesucht. Laut der Cybersecurityfirma Cybereason wurden 2022 rund achtzig Prozent der Zahlungswilligen ein zweites Mal attackiert, die Hälfte davon von denselben Angreifern. Das Nationale Zentrum für Cybersicherheit (NCSC) rät darum dringend davon ab, Lösegeld zu bezahlen.

Zwanzig Milliarden Dollar pro Jahr

Die Angreifer:innen sind keine Robin-Hood-Hacker:innen in schwarzen Kapuzenpullovern. Es geht ihnen nur um den Profit. Die Aktivitäten von Play wurden im Juni 2022 erstmals dokumentiert. Nach Anfängen in Lateinamerika hat die Bande Firmen, Behörden und Organisationen vorwiegend in den USA und Europa angegriffen, um Geld zu erpressen. Play verfolgt dabei offenbar sehr ähnliche Angriffsmethoden wie die berühmte Gruppe Hive, deren Infrastruktur Ende Januar in einer koordinierten Polizeiaktion ausgehoben wurde. Die Bande, die auch hinter einem Angriff auf das Autohandelshaus Emil Frey AG steckte, hatte laut dem FBI bis Ende 2022 rund hundert Millionen US-Dollar erbeutet. Viele der Hive-Hacker:innen dürften inzwischen zu anderen Banden gewechselt haben.

Securityexperten entdeckten bei Play ähnliche Filenamen, Tools und Taktiken wie bei Hive, aber sie fanden auch Parallelen zu anderen Banden. Die Gruppen klar zu identifizieren, ist kaum möglich. Die grossen Cybercrimebanden ähneln Firmen, sie beschäftigen eigenes Personal für Softwareentwicklung, Personalrekrutierung, Finanztransaktionen, aber auch für die Betreuung von Partnern, die Operationen für sie ausführen. Dabei ist ein unübersichtliches Geflecht entstanden, das die Ermittlungsbehörden vor grosse Probleme stellt, zumal sich die Gruppen auflösen und neu zusammensetzen, um der Strafverfolgung zu entgehen.

Die Schäden, die weltweit mit Ransomware angerichtet wurden, überstiegen laut Cybereason letztes Jahr die Summe von zwanzig Milliarden US-Dollar. Auch Play hat bereits viele Opfer gefordert. Die bislang verheerendste Operation führte die Bande gegen die US-Stadt Oakland durch. Diese wurde am 10. Februar so hart getroffen, dass die Regierung einige Tage darauf den lokalen Ausnahmezustand ausrief. Die gesamten IT-Systeme mit Ausnahme der Notrufaktionen und der Finanzverwaltung waren lahmgelegt: Öffentliche Computer, Scanner, Drucker, WLAN, Telefondienste und Behördendienste waren während Tagen nicht erreichbar.

Eine Meldepflicht für Cybervorfälle

Auch in der Schweiz war Play schon aktiv: Ende 2022 veröffentlichte die Bande nach dem Hack einer deutschen Hotelkette Rechnungen, Identitätskarten und Buchungen von Gästen in Schweizer Hotels. Erst im Februar verschlüsselte Play die Systeme von Energie Pool Schweiz. Danach veröffentlichte sie sensible Informationen des Dienstleistungsunternehmens im Darknet.

Ransomwareangriffe stehen hierzulande auf der Tagesordnung. Das hat auch die Politik auf den Plan gerufen. Der Nationalrat hat bereits einer Meldepflicht für Cyberangriffe auf kritische Infrastruktur wie Strom- und Wasserversorgung oder Notfalldienste zugestimmt. Laut dem NCSC werden nicht nur die Angriffe zu oft verschwiegen und einfach Lösegeld gezahlt, auch mangelt es an Sicherheitsmassnahmen. Das NCSC wird derzeit zum Bundesamt ausgebaut.

Ob das reicht, ist fraglich, denn die Verteidigung sieht sich hochgerüsteten und finanzstarken Banden gegenüber, die ständig nach Schwachstellen in den Systemen suchen. Auch die NZZ-Gruppe hatte im letzten Jahresbericht verkündet, dass sie Cybersicherheit zum Topthema mache, Mitarbeitende schule und eine interne Sicherheitsplattform lanciert habe. Der Geschäftsbericht erschien zwei Wochen vor dem Ransomwarevorfall.

Thomas Schwendener ist Redaktor des Fachmagazins «Inside IT».

* Wegen einer superprovisorischen Verfügung des Handelsgerichts Kanton Aargau wurde dieser Satz am Montag, 8. Mai 2023, eingeschwärzt. Nach Vergleichsverhandlungen zwischen CH Media und der WOZ vor dem Handelsgericht Aarau vom 13. Juni 2023, darf die im Zusammenhang mit der superprovisorischen Massnahme zensierte Passage nun wieder veröffentlicht werden.

NZZ

Kriminelle Hacker greifen die NZZ an und erpressen sie. Das Protokoll einer Krise

Im März vor einem Jahr wird die NZZ Opfer eines Cyberangriffs. Die Folgen beschäftigen das Medienhaus über Wochen und Monate. Dabei hat der Verlag noch Glück.

Lukas Mäder

17.02.2024, 05.30 Uhr ⌚ 17 min



Illustration Simon Tanner / NZZ

Der Cyberangriff auf die NZZ ist eine Geschichte, wie sie sich täglich ereignet. In der Schweiz, in Europa, irgendwo auf der Welt. Überall greifen Kriminelle Unternehmen an und erpressen sie. Bei diesen Ransomware-Angriffen dringen die Erpresser in die Rechner der Opfer ein, stehlen Daten, legen Computer lahm

und drohen damit, vertrauliche Informationen zu veröffentlichen. Diese Art der Angriffe nimmt seit einigen Jahren stark zu.

Die NZZ wurde im vergangenen Frühjahr Opfer eines solchen Angriffs und hat sich dazu entschieden, die Hintergründe publik zu machen. Dass die meisten angegriffenen Unternehmen schweigen, spielt den Erpressern in die Hände. Ein Angriff gilt als Versagen. Dabei kann es jeden treffen. Die NZZ ist überzeugt, dass die Lehren aus dem eigenen Cyberangriff anderen Firmen helfen können, sich vor Ransomware-Banden zu schützen.

Journalisten schreiben üblicherweise nicht über das eigene Unternehmen. Dass der Autor hier eine Ausnahme macht, liegt an der besonderen Ausgangslage. Er konnte den Cyberangriff so nahe mitverfolgen, wie das bei einer externen Firma nicht möglich wäre. Die Geschäftsleitung hat dem Autor von Beginn an einen umfassenden Einblick in das Geschehen gewährt.

Entstanden ist das seltene Protokoll eines Schweizer Unternehmens im Ausnahmezustand. Es zeigt, wie die NZZ den Kampf gegen eine gut organisierte Cybermafia führt – einen Kampf, den sie nicht gewinnen kann.

Teil 1: Der Angriff – «kalte Fischstäbchen zum Znacht»

Freitagmorgen, 24. März: Es geht ums Ganze

Als die Kriminellen zuschlagen, herrscht auf der Redaktion normaler Alltag. Die Journalisten schreiben ihre Artikel im Redaktionssystem und können sie publizieren. Die Laptops funktionieren normal. Auch bei den E-Mails und mit der Website nzz.ch gibt es keine Probleme. Zwar erzählt man sich auf den Gängen von einem Cyberangriff, aber zu spüren ist davon nichts.

Ganz anders ist die Situation auf der anderen Seite der Falkenstrasse: In den Räumen der IT-Abteilung herrscht der Ausnahmezustand. Seit 8 Uhr morgens hat sich der Krisenstab im sogenannten «War Room» eingefunden: Ein ganzer Stock ist freigeräumt für den CEO, den Rechtsdienst, die Kommunikationsabteilung und die IT-Mitarbeiter.

Bei der Kaffeemaschine stehen Cola- und Rivella-Flaschen, daneben liegen Gipfeli. Die Stimmung ist angespannt, aber konzentriert. Allen ist klar, dass es ums Ganze geht. Höchste Priorität hat es, ein weiteres Ausbreiten der Schadsoftware zu verhindern – und die Produktion der gedruckten Zeitung sicherzustellen.

Was den Anwesenden nicht klar ist: wie lange der Cyberangriff sie noch auf Trab halten wird.

Am Freitagmittag vermelden die ersten Medien den Angriff. Betroffen ist nicht nur die NZZ, sondern auch das Verlagshaus CH Media, an welchem die NZZ beteiligt ist. CH Media bezieht den Grossteil der IT-Dienstleistungen von der NZZ.

Zu CH Media gehören die «Luzerner Zeitung», die «Aargauer Zeitung» und das «St. Galler Tagblatt» sowie mehrere Radio- und Fernsehstationen. Dort sind die Auswirkungen des Angriffs sofort spürbar. Beim Ostschweizer Radiosender FM1 hat die Redaktion zum Beispiel keinen Zugriff mehr auf die Musikdatenbank.

Freitagnachmittag, 24. März: Der Krisenstab stochert im Nebel

In den ersten Stunden muss sich der Krisenstab einen Überblick verschaffen: Welche Systeme sind betroffen? Haben die Kriminellen Daten gestohlen? Kann die gedruckte Ausgabe der NZZ morgen erscheinen?

Klar ist: Die Angreifer haben in der Nacht auf den 24. März zahlreiche IT-Systeme verschlüsselt und unbrauchbar gemacht. Eingeschränkt ist bei der NZZ etwa die automatische Produktion der gedruckten Zeitung. Besonders schmerzhaft: Die sogenannten «Domain Controller» des NZZ-Netzwerks sind ebenfalls verschlüsselt. Sie sind das Herzstück eines IT-Netzwerks. Alle Rechner der Firma melden sich dort an. Die Benutzer des IT-Netzwerks werden dort verwaltet. Ohne «Domain Controller» läuft nichts.

Was hinzukommt: Keiner weiss am Freitagnachmittag, ob der Angriff bereits vorüber ist. Haben sich die Kriminellen im Netzwerk eingenistet und warten nur darauf, in der Nacht erneut zuzuschlagen? Es braucht zusätzliche

Sicherheitsmassnahmen für den Fall, dass die Angreifer zurückkommen.

Völlig unvorbereitet ist der Krisenstab nicht. Die NZZ hat in den Monaten vor dem Angriff ein sogenanntes Playbook erstellt: ein rund 30-seitiges Handbuch, in dem die Abläufe, die Zuständigkeiten und die Kontaktinformationen für den Krisenfall festgehalten sind. Das Kapitel zum Cybervorfall wurde zuletzt am 9. März aktualisiert, zwei Wochen vor dem Ransomware-Angriff. Eigentlich war für den Frühsommer eine Übung geplant. Jetzt kam der Ernstfall früher.

Das Dokument hilft dennoch: Die Krisenorganisation ist klar. Zur Unterstützung bietet die NZZ die externe IT-Sicherheitsfirma Oneconsult auf. Die NZZ hat mit der Firma einen Servicevertrag für einen solchen Notfall abgeschlossen. Das zahlt sich jetzt aus. Die Kantonspolizei Zürich und das Nationale Zentrum für Cybersicherheit werden informiert und schicken Leute vor Ort.

Die IT-Experten haben schon bald jene Server im Internet identifiziert, über welche die Kriminellen ihren Angriff steuern. Sie stehen in Litauen und in Russland. Diese Informationen sind wichtig für die Ermittlungen der Polizei. Sie sagen jedoch nichts darüber aus, woher die Angreifer tatsächlich stammen.

Von der Erpresserbande ist nur der Name bekannt: Play. Auf den infizierten Servern hat sie eine Textdatei mit einer knappen Nachricht hinterlassen. Sie enthält den Namen der Gruppe und zwei Kontaktmöglichkeiten, eine E-Mail-Adresse und einen Link

ins Darknet, jenen anonymisierten Teil des Internets, den Cyberkriminelle gerne nutzen.

Aufgetaucht ist die Ransomware-Gruppe Play im Sommer 2022. Zu den ersten prominenten Opfern gehörten die Justizbehörde von Córdoba in Argentinien, die deutsche Hotelkette H Hotels und die österreichische Nachrichtenagentur APA. Anfang 2023 hat sich Play bereits als eine der aktivsten Ransomware-Gruppen weltweit etabliert.

Ransomware-Banden gehen fast immer gleich vor: Die Kriminellen dringen in die IT-Systeme des Opfers ein. Von dort laden sie vertrauliche Daten herunter, bevor sie die Server verschlüsseln – und damit unbrauchbar machen. Für die Entschlüsselung fordern die Angreifer ein Lösegeld, auf Englisch «ransom». Zusätzlich drohen die Erpresser damit, die internen Informationen des Opfers im Internet zu veröffentlichen.

Hinter den Angriffen stecken professionell organisierte Banden. Sie erbeuten mit ihren Angriffen mehrere hundert Millionen Franken im Jahr. Woher die Mitglieder von Play stammen, ist nicht klar. Es gibt jedoch Verbindungen zum russischen Ökosystem von Cyberkriminellen. Deswegen müssen die Personen, die hinter dem Angriff auf die NZZ stecken, aber nicht unbedingt aus Russland kommen.

Freitagabend, 24. März: Die NZZ will nicht bezahlen

Der Krisenstab der NZZ will auf die Lösegeldforderung der Kriminellen nicht eingehen. Die Nachricht im Darknet, die

sogenannte «Ransom Note», bleibt unberührt. Dort würde die geforderte Summe stehen. Doch die Befürchtung ist, dass beim Aufrufen des Links ein Countdown ausgelöst wird.

Für den CEO der NZZ, Felix Graf, ist klar: Die NZZ bezahlt falls irgendwie möglich kein Lösegeld. Aber in diesen ersten Stunden des Angriffs ist noch alles offen. Der Cyberangriff könnte zu einer existenziellen Bedrohung für das Unternehmen werden. Entsprechend ist vorgesorgt: Ein Händler steht bereit, um nötigenfalls rasch das Lösegeld in einer Kryptowährung überweisen zu können.

Einen Datenverlust verursacht die Verschlüsselung der Server nicht. Die NZZ hat Sicherheitskopien. Die Verantwortlichen sind sogar optimistisch, was den Datendiebstahl betrifft. Sie gehen davon aus, dass die Angreifer keine grossen Datenmengen entwendet haben. Die Log-Dateien deuten auf einen Datenabfluss von rund 5 Gigabyte hin. Die Mitarbeiterdaten sollen zudem nur in verschlüsselter Form gespeichert und für die Erpresser deshalb wertlos sein.

Diese Beurteilung hält sich über Wochen. Sie wird sich als Fehleinschätzung mit Folgen herausstellen.

Freitagnacht, 24. März: Die Angreifer kommen zurück

Es ist etwa 21 Uhr, als die Kriminellen wieder aktiv werden. Die Zeitungsproduktion bei NZZ und CH Media ist noch in vollem Gange. Den Angreifern gelingt es, weitere Server zu verschlüsseln. Erst gegen Mitternacht kappen die

Verantwortlichen die Verbindung ins Internet. Die Angreifer sind damit ausgeschlossen.

Die NZZ hat seit Anfang 2022 einen Vertrag mit einem SOC-Dienstleister. Die Abkürzung SOC steht für «Security Operations Center»: eine rund um die Uhr besetzte Zentrale, welche im Ernstfall rasch reagieren und Alarm schlagen kann.

Im Fall der NZZ hat dies allerdings nicht wunschgemäss funktioniert. Bereits in der Nacht auf Donnerstag bemerkten die Sicherheitssysteme verdächtige Aktivitäten im IT-Netzwerk. Daraufhin sperrten die Mitarbeiter des externen SOC einige betroffene Accounts, jedoch vermutlich nicht alle. Die zuständigen Personen bei der NZZ wurden zwar informiert, aber niemand löste einen Alarm aus. Möglicherweise hätte ein rascheres und beherzteres Eingreifen Schlimmeres verhindern können.

Nach dem erneuten Angriff in der Nacht auf Samstag fassen die Verantwortlichen einen Plan: Jeden Abend um 21 Uhr wird die Verbindung von NZZ und CH Media ins Internet getrennt. Die Angreifer, die meist nachts aktiv sind, können dann nichts mehr ausrichten.

Für den Betrieb der Redaktion bedeutet das: Die Produktion der gedruckten Zeitung wird vorgezogen und muss bis 21 Uhr abgeschlossen sein. Der Nachtdienst in Übersee hat keinen Zugriff auf Agenturmeldungen oder Bilder. Diese Einschränkungen sind für die Betroffenen mühsam. Aber sie

bewähren sich. In den kommenden Tagen und Nächten sind keine Aktivitäten der Kriminellen mehr zu beobachten.

Sonntag, 26. März: Die grosse Geduld der Angreifer

Die externen Sicherheitsexperten arbeiten mit Hochdruck daran, das Einfallstor der Kriminellen zu finden. Diese Information ist wichtig, um eine allfällige Lücke im IT-System schliessen zu können.

Am Sonntagnachmittag findet ein Mitarbeiter der Firma Oneconsult den entscheidenden Eintrag in der Protokolldatei eines Servers. Die Entdeckung offenbart das Vorgehen der Angreifer – und ihre Geduld.

In den frühen Morgenstunden des 4. März, um 4.04 Uhr, melden sich die Kriminellen erstmals im Netzwerk an – also fast drei Wochen vor der Entdeckung. Sie richten auf dem Server eine Hintertüre ein. Nach einer halben Stunde sind sie wieder weg.

Dass sich die Angreifer am Server anmelden können, liegt an mangelhaften Sicherheitsvorkehrungen. Das Log-in, das die Kriminellen verwenden, gehört dem Mitarbeiter eines externen Softwarelieferanten. Dessen Zugang ist nicht durch einen zweiten Faktor geschützt, also zum Beispiel durch einen SMS-Code, der zusätzlich zum Passwort eingegeben werden muss. Auf dem Server war zudem eine ungenügende Sicherheitssoftware installiert, die keinen Alarm auslöste. Sie hätte bald ersetzt werden sollen.

Wie die Kriminellen ursprünglich an Benutzername und Passwort des externen Mitarbeiters gelangen konnten, ist unklar. Möglicherweise ist dieser auf einen sogenannten Phishing-Angriff hereingefallen und hat seine Kombination von E-Mail-Adresse und Passwort auf einer gefälschten Seite eingegeben.

Zusätzlich bitter ist: Der Vertrag mit dem IT-Lieferanten war bereits gekündigt. Der Zugang wurde nicht mehr benötigt, und der Account hätte gelöscht werden sollen. Doch diese Meldung ging intern irgendwo verloren.

Der eigentliche Ransomware-Angriff startet drei Wochen nach dem ersten Eindringen: am Donnerstag, dem 23. März, um 0.16 Uhr. Die Kriminellen beginnen, vom Lieferantenaccount des Servers aus das IT-Netzwerk zu erkunden.

Warum es diese mehrwöchige Pause gab, ist nicht klar. Die Kriminellen waren möglicherweise mit anderen Angriffen beschäftigt oder mussten sich vorbereiten. Die Hintertüre von Anfang März kann auch von einem sogenannten «Initial Access Broker» eingerichtet worden sein. Das sind professionelle Händler von Hintertüren: Sie suchen nach schlecht gesicherten Systemen, richten dort einen versteckten Zugang ein und verkaufen diesen dann an andere Kriminelle weiter – zum Beispiel an Ransomware-Gruppen wie Play.

Bei ihrem Angriff an diesem frühen Donnerstagmorgen finden die Kriminellen von Play im Arbeitsspeicher eines Servers das Passwort eines Administrators. Dieser hatte sich nicht abgemeldet. Mit diesen Zugangsdaten gelingt es den Angreifern

eine gute Stunde später, sich am zentralen «Domain Controller» anzumelden, dem Herz des IT-Netzwerks. Von dort aus können sich die Angreifer im gesamten Netzwerk ausbreiten.

In der zweiten Nacht, am Freitag, dem 24. März, kurz nach Mitternacht, machen sich die Angreifer daran, auf mehreren Systemen die Sicherheitssoftware zu deaktivieren. Das gibt ihnen freie Bahn, um ausgehend vom «Domain Controller» über 200 IT-Systeme im Netz von NZZ und CH Media zu verschlüsseln.

Um ihre Spuren zu verwischen, löschen die Angreifer zuvor auf mehreren Servern die Log-Dateien. Der genaue Weg der Kriminellen durch das IT-Netzwerk lässt sich deshalb nicht mehr rekonstruieren.

Sonntagabend, 26. März: Die IT-Mitarbeiter im Dauereinsatz

Am Sonntagnachmittag hat sich die Krisenbewältigung eingespielt. Jeder weiss, was er zu tun hat. Der Notbetrieb läuft stabil. Und allen ist klar, dass der Angriff sie noch lange beschäftigen wird.

Neben der Kaffeemaschine liegen Süssigkeiten. Zucker und Adrenalin sind der Treibstoff, welcher die IT-Mitarbeiter seit Freitagmorgen auf Trab hält. Sie sind praktisch ununterbrochen im Einsatz und gehen nur für einige Stunden zum Schlafen nach Hause.

Die Leidtragenden sind ihre Angehörigen. Ein IT-Mitarbeiter hat eine gut dreimonatige Tochter zu Hause. Er hat sie seit vier Tagen nicht mehr gesehen, wie er sagt. «Gestern Abend habe ich um 22 Uhr zu Hause nur noch kalte Fischstäbchen gegessen.»

Teil 2: Der Wiederaufbau – «Wir sitzen auf einem Vulkan, der jederzeit ausbrechen kann»

Dienstag, 28. März: Die Systeme drohen auszufallen

Der Ransomware-Angriff hinterlässt in der IT-Landschaft ein Bild der Verwüstung. Bernd Hornig ist für die IT-Infrastruktur verantwortlich und ein Mann der klaren Worte. Er vergleicht den Zustand der IT-Systeme mit einem zerbombten Hochhaus.

«Einzelne Etagen sind komplett zerstört und einige Treppen eingestürzt. Der Lift ist ausgefallen, und an mehreren Stellen ist Feuer ausgebrochen», sagt Hornig. Er schätzt, dass am Freitagmorgen nach dem Angriff noch etwa 50 bis 60 Prozent der IT-Systeme funktionstüchtig waren. Der Rest ist ausgefallen.

Diese Ruine ist die rote Zone. Der Betrieb der NZZ läuft zum grössten Teil noch immer dort, insbesondere die Produktion der gedruckten Zeitung. Einige Anwendungen sind behelfsmässig geflickt. Andere funktionieren gar nicht. So können die Mitarbeiter zum Beispiel die Sitzungszimmer nicht online reservieren und nicht drucken.

Eigentlich möchte Hornig in der roten Zone möglichst wenig reparieren. Jede Arbeitsstunde, die seine Mitarbeiter in die rote Zone investieren, fehlt beim Aufbau der grünen Zone. Und auf dieser liegt der Fokus.

In der grünen Zone bauen die IT-Mitarbeiter die Systeme von Grund auf neu auf. Daten, die von der roten Zone übernommen werden, durchlaufen zuerst eine Prüfung. Dieses Vorgehen soll sicherstellen, dass die Kriminellen keine Hintertüre hinterlassen haben und so später zurückkommen können.

Die Zeit für den Aufbau drängt. Weil sich die alten Systeme aus Sicherheitsgründen nicht mehr synchronisieren, kommt es irgendwann zu Funktionseinschränkungen, wie Hornig sagt. Das Hochhaus, um bei seinem Bild zu bleiben, droht einzustürzen. «Die Uhr tickt.»

Deshalb arbeitet die IT-Abteilung noch immer im Krisenmodus. «Was wir jetzt machen, ist normalerweise ein Projekt von anderthalb Jahren», sagt Hornig. Und obwohl die Zeit drängt, muss er Pausen für seine Leute organisieren. «Einige der Mitarbeiter sind seit Tagen ununterbrochen am Arbeiten», sagt Hornig. Dass es jetzt nur noch zehn Arbeitsstunden am Tag sind, ist bereits ein Fortschritt. Einige kommen an den Anschlag.

Mittwochabend, 29. März: Der eingeschränkte Betrieb

Es folgt eine Zeit des Improvisierens. Jeden Abend um 18 Uhr treffen sich die Bereichsleiter der NZZ zum Video-Call. Sie

tauschen sich über die zahlreichen Hindernisse und Stolpersteine aus, mit denen sie jeden Tag konfrontiert sind.

Die Buchhaltung kann zum Beispiel keine Rechnungen direkt aus dem Buchhaltungssystem heraus bezahlen. Einige Zahlungen muss sie direkt über das Online-Banking verbuchen. Für die Übertragung von Arbeitszeiten und Spesen ins zentrale SAP-System fehlt die Schnittstelle. Auf den Redaktionen ist für die Printausgabe weiterhin Handarbeit gefragt. Die Produzenten müssen die Texte aus dem Online-System, das problemlos läuft, ins Layout der Zeitung kopieren.

Die grösste Einschränkung gibt es bei den Zeitungen von CH Media. Statt wie üblich sechzehn Regionalausgaben erscheinen nur die drei Ausgaben von «Luzerner Zeitung», «Aargauer Zeitung» und «St. Galler Tagblatt». Grund dafür ist der Ausfall der automatischen Seitenplanung, welche für die aufwendige Platzierung der Inserate nötig ist. Das entsprechende IT-System wurde beim Angriff lahmgelegt.

Immerhin weicht langsam die Unsicherheit, ob die Angreifer noch einmal zurückkommen. Seit dem Wochenende gibt es in der roten Zone zwar noch einige Fehlalarme. Aber ein Lebenszeichen der Angreifer registrieren die Systeme nicht.

Karfreitag, 7. April: Der grosse Wechsel gelingt

Die heikle Umstellung auf die grüne Zone, der «Switch», findet am Osterwochenende statt, zwei Wochen nach dem Angriff. Das Osterdatum ist ein Glücksfall: Die Feiertage geben den

Beteiligten mehr Zeit für die kritische Operation. Es fällt keine Ausgabe der Zeitung aus, und die IT-Mitarbeiter müssen keine Nachtschicht einlegen.

Die Verantwortlichen haben von Gründonnerstag um 23 Uhr bis am frühen Nachmittag des Ostermontags Zeit, bis die Produktion der Dienstagsausgabe anläuft. Einzige Einschränkung für die Leserschaft: Die Samstagsausgabe der NZZ und die Osterausgabe der «NZZ am Sonntag» werden bereits am Donnerstag vorproduziert. Aktualität gibt es nur online.

Der definitive Entscheid zum Sprung fällt am Freitagmorgen im kleinen Kreis mit dem CEO Graf. «Wir haben uns tief in die Augen geschaut und gesagt: Lasst es uns wagen!», so schildert es ein Beteiligter.

Der Wechsel muss gelingen. Ein Zurück gibt es nicht. Ist das zentrale Verzeichnis des IT-Netzwerks, die «Active Directory», erst einmal mit der grünen Zone verbunden, muss die rote Zone aufgegeben werden. Insgesamt stehen rund 35 Personen im Einsatz, interne IT-Mitarbeiter und externe Spezialisten.

Um etwa 11 Uhr am Karfreitag kommt der heikle Moment: Der «Domain Controller» der NZZ wechselt in die grüne Zone. Alles geht gut. Komplikationen gibt es keine. Dann erfolgt der Aufbau des restlichen IT-Netzwerks. Am Samstag folgt das gleiche Vorgehen für das Netzwerk von CH Media. Und der Ostersonntag ist für Tests reserviert.

Der Wechsel gelingt. Am Ostermontag kann die Redaktion die Zeitungsproduktion wie geplant aufnehmen. Und Bernd Hornig ändert den Namen des Kanals auf der internen Chat-Plattform von «Cyber Restore Weekend» auf «Cyber Restore Marathon». Die Arbeit der IT ist noch lange nicht zu Ende.

Teil 3: Das Datenleck – «Wir müssen vom Schlimmsten ausgehen»

Mittwoch, 12. April: Die Erpresser erhöhen den Druck

Nach der erfolgreichen Umstellung der IT-Systeme stellt sich eine gewisse Erleichterung ein. Der CEO Graf zeigt sich am Dienstag nach Ostern insgesamt zufrieden mit der Bewältigung des Cyberangriffs. Doch die Zeit des Verschnaufens ist kurz. Bereits am Mittwoch geht die Erpressung weiter.

Am 12. April schaltet die kriminelle Gruppe Play auf ihrer Leak-Site im Darknet eine Ankündigung auf. Man werde interne Unternehmensdaten, die beim Angriff gestohlen wurden, veröffentlichen: vertrauliche Personendaten, Informationen über Projekte und Löhne. Publikationsdatum: 2023-04-24. Die Uhr tickt.

Ransomware-Angriffe haben meist zwei Stufen. Im ersten Teil der Erpressung steht das Opfer unter Druck, weil seine IT-Systeme stillstehen und die Daten verschlüsselt sind. Das kann Produktionsausfälle oder einen Datenverlust bedeuten.

Im zweiten Teil drohen die Angreifer damit, alle internen Daten zu publizieren, die sie beim Angriff entwendet haben. Die Veröffentlichung von vertraulichen Informationen bedeutet einen Reputationsschaden und kann die Kunden, die Mitarbeiter und das Geschäft schädigen. Der Druck auf das Opfer steigt.

Die Öffentlichkeit ist Teil der Erpressung. Das Vorgehen der Kriminellen funktioniert nur, wenn der Angriff und der Datendiebstahl publik werden. Das Opfer muss am Pranger stehen. Deswegen haben die Erpresserbanden im Darknet ihre eigenen Websites eingerichtet, sogenannte Leak-Sites. Dort veröffentlichen sie die Namen der Opfer und deren Daten.

Im Fall der NZZ wird die Ankündigung der Kriminellen am Montag, dem 17. April, publik. Der «Blick» vermeldet, dass die kriminelle Gruppe Play mit der Veröffentlichung der Daten drohe. Zahlreiche Medien nehmen die Nachricht auf.

Die Verantwortlichen der NZZ sind zu diesem Zeitpunkt weiterhin optimistisch. Die Unternehmenskommunikation spricht noch immer von «geringen Datenmengen», die abgeflossen seien. Ein Trugschluss, wie sich später herausstellen wird.

Dienstagnachmittag, 18. April: Das Video als Beweis

Nun kommt es zu Verhandlungen. Bisher hatte die Geschäftsleitung die Lösegeldforderung der Erpresser ignoriert. Niemand hatte die sogenannte «Ransom Note», das Erpresserschreiben im Darknet, aufgerufen.

Nach der Drohung nimmt die Kantonspolizei Zürich Kontakt zu den Kriminellen auf. Sie übernimmt die Verhandlungsführung. Dabei geht es nicht darum, das geforderte Lösegeld herunterzuhandeln. Diese Aufgabe übernimmt die Kantonspolizei nicht. Zudem ist die Geschäftsleitung noch immer der Meinung, dass die NZZ kein Lösegeld bezahlen soll.

Das Ziel der Polizei ist es, aus den Verhandlungen Hinweise für die Ermittlungen zu erhalten. Sie will die Kriminellen möglichst lange hinhalten und dazu verleiten, Spuren zu hinterlassen. Das können zum Beispiel IP-Adressen oder Krypto-Wallets sein.

In die Verhandlungen ist die NZZ nicht involviert. Sie bekommt den Verlauf des Chats mit den Kriminellen nicht zu sehen. Der Krisenstab erhält nur zusammenfassende Infos. Zum Beispiel, wenn die Kriminellen einen Aufschub gewähren und den Publikationstermin verschieben. Das geschieht mehrmals.

Die Polizei verlangt von den Erpressern den Beweis, dass sie tatsächlich im Besitz vertraulicher Daten sind. Am Nachmittag des 18. April erhält der CEO Graf deswegen einen Anruf. Die Kriminellen haben ein Video übermittelt. Es macht die letzte Hoffnung auf ein glimpfliches Ende zunichte.

Die Aufnahme zeigt vier Minuten lang, welche Daten die Erpresser nach eigenen Angaben entwendet haben. Zu sehen sind Ordner und Dateien der NZZ. Die Kriminellen öffnen einzelne Dateien, um zu beweisen, dass diese nicht verschlüsselt sind. Die Erpresser bluffen nicht. Sie sind tatsächlich im Besitz

sensibler Daten. 800 Gigabyte sollen es sein – ein Vielfaches der bisher angenommenen Datenmenge.

Montagsmorgen, 24. April, 9.30 Uhr: Keine Antworten

Die Einladung zur Mitarbeiterinformation kommt kurzfristig. Ursprünglich hatten die Erpresser angekündigt, an diesem Montag erstmals Daten zu veröffentlichen. Die Geschäftsleitung will deshalb die drängendsten Fragen beantworten. Doch die Verhandler haben einen Aufschub erwirkt. Die Veranstaltung findet trotzdem statt. Sie markiert einen Wendepunkt.

Bisher konnten die Verantwortlichen handeln. Sie konnten die Angreifer im Netzwerk bekämpfen und die neue IT-Umgebung aufbauen. Die Spekulationen in den Medien hielten sich in Grenzen. Die Verantwortlichen waren überzeugt, dass nur eine geringe Menge von Daten abgeflossen sei.

Am 24. April ändert sich das. Nun muss sich die Geschäftsleitung rechtfertigen, vor allem gegen innen. Denn ab sofort sind alle Mitarbeiter direkt betroffen.

Als Felix Graf an diesem Montag vor die Kamera tritt, gibt er ein zerknirschtes Bild ab. Die Hoffnung, mit einem blauen Auge davongekommen zu sein, ist verflogen. Im Video-Stream gesteht er ein: «Wir müssen vom Schlimmsten ausgehen.» In den nächsten Tagen könnten persönliche Daten, Personaldaten und Finanzdaten im Darknet auftauchen.

Wie schwierig das Informieren der Belegschaft ist, wird in der Fragerunde klar. Die Verantwortlichen haben auf die meisten Fragen der verunsicherten Mitarbeiter keine Antwort. Noch immer wissen sie nicht, welche Daten tatsächlich abgeflossen sind. Erklären, wie es dazu kommen konnte, ist schwierig. Garantieren, dass es nicht wieder vorkommt, kann niemand.

Graf tut, was er in dieser Situation tun kann: Er bedauert die Vorkommnisse und entschuldigt sich dafür, dass persönliche Daten abgeflossen sind.

Mittwoch, 3. Mai: Erste Tranche der Daten ist online

Das Medienecho ist gross, als die Erpresser am 3. Mai einen Teil der Daten publizieren. Der «Tages-Anzeiger» etwa titelt «Internetpiraten veröffentlichen Lohnlisten und Erfolgsrechnungen» und schreibt von sensiblen Daten. Doch eigentlich ist der erste Teil der Daten weniger brisant als befürchtet. Es handelt sich um Dokumente der Zustellorganisation von CH Media.

Dennoch geht CH Media juristisch gegen einzelne Medien vor, die über die Daten berichten. Eine superprovisorische Verfügung zwingt «Inside IT», die «Wochenzeitung» und «Zentralplus», Passagen aus ihren Artikeln zu löschen, in denen es sehr oberflächlich um die publizierten Dokumente geht. Doch die Löschung ist nur vorübergehend. Vor Gericht zieht CH Media das entsprechende Begehren – weil wenig aussichtsreich – zurück und willigt in einen Vergleich ein. Vermutlich ging es aber sowieso darum, ein Signal an die Öffentlichkeit zu senden.

Mit der Publikation der Daten steht die grosse Frage im Raum: War das schon alles? Ransomware-Gruppen veröffentlichen die Daten ihrer Opfer häufig in Tranchen. Sie wollen so Druck aufbauen, damit die Geschädigten vielleicht doch noch bezahlen. Auch im Fall der NZZ drohen die Erpresser damit, alle paar Tage kleinere Datenpakete zu veröffentlichen. Doch nichts geschieht.

Die Verhandlungen der Polizei scheinen im Sand zu verlaufen. Ganz leise keimt die Hoffnung auf: Vielleicht haben die Erpresser ihr Interesse verloren, weil kein Geld zu holen ist. Vielleicht haben sie sich einfach dem nächsten Opfer zugewandt.

Doch die kriminelle Logik funktioniert anders: Wer nicht bezahlt, soll den Schmerz spüren. Das Opfer soll leiden.

Donnerstag, 11. Mai: Alles steht jetzt im Darknet

Der Rest der Daten kommt auf einen Schlag. Am 11. Mai stehen auf der Leak-Site von Play 752 Archivdateien. Insgesamt sind es rund 500 Gigabyte an Daten. Tausende von Dokumenten aus dem Innern der NZZ mit privaten Informationen und vertraulichen Details. Die Firma und ihre Mitarbeiter stehen entblösst da.

Mit der Veröffentlichung der Daten wird der Ransomware-Angriff für die Geschäftsleitung definitiv zu einer kommunikativen und juristischen Angelegenheit. Die technische Bewältigung des Vorfalls ist in den Hintergrund getreten.

Stattdessen geht es jetzt um die Abwicklung des Datenlecks in seiner schieren Grösse. Und die ist aufwendig.

Was die Kriminellen genau publiziert haben, wissen die Verantwortlichen noch gar nicht, als sie am Montag nach der Publikation die Mitarbeiter informieren. Die Datenmenge ist so gross und die Verbindung ins Darknet so langsam, dass es Zeit braucht, die Dokumente erst herunterzuladen und sie dann zu erfassen. Die Verantwortlichen rechnen allein dafür mit einer Woche.

Die Geschäftsleitung ist nun zunehmend mit Kritik aus der Belegschaft konfrontiert. Dass nicht alle Mitarbeiter individuell darüber informiert werden, welche Daten von ihnen im Darknet stehen, stösst weitherum auf Unverständnis. Wer annehmen muss, dass weitere heikle Daten – zum Beispiel persönliche medizinische Informationen – bei den Angreifern gelandet sind, kann sich an die Anlaufstelle eines Anwaltsbüros wenden. Aus Kapazitätsgründen, sagt Graf. Eine pauschale finanzielle Entschädigung der Mitarbeiter für den Datenverlust lehnt er ab.

Mit der Publikation der Daten geben die Kriminellen ihr letztes Druckmittel aus der Hand. Für sie ist der Angriff abgeschlossen. Beim Opfer gibt es jetzt nichts mehr zu holen. Sie ziehen weiter zur nächsten Firma.

Ganz anders für die Betroffenen: Die privaten Informationen aus ihrem Leben stehen nun öffentlich im Darknet. Jeder kann sie einsehen. Und Cyberkriminelle können diese Informationen

verwenden, um zum Beispiel gezielte Phishing-Angriffe durchzuführen.

Der Cyberangriff auf die NZZ, der im März vor einem Jahr begann, hat kein Ende. Technisch sind die Systeme der NZZ wiederhergestellt. Die Entschädigung mit der Versicherung ist geregelt. Die Blösse aber, entstanden durch die Datenpublikation, die bleibt. Das lässt sich nicht ungeschehen machen. Die Opfer müssen damit leben.

Passend zum Artikel



Wohnadressen des Bundesrates und lahmgelegte Websites: 2023 war ein erfolgreiches Jahr – für Hacker

27.12.2023 ⌚ 5 min



Pro

Globale Hackergruppen: Der Kampf gegen Cyberkriminelle kann erfolgreich sein. Wie bei der Mafia

24.07.2023 ⌚ 10 min



Wenn die Benzinversorgung ausfällt und das Spital stillsteht: Warum Ransomware-Angriffe so gefährlich sind

11.12.2022 ⌚ 7 min



Mehr von Lukas Mäder (mdr) >



KOMMENTAR Pro

von Lukas Mäder

Die Feinde der USA versuchen, die Präsidentschaftswahl zu beeinflussen. Doch dieses Mal ist das Land vorbereitet

10.09.2024 ⌚ 3 min



Pro

Verhaftung des Telegram-Chefs und Terror von Solingen: Die Staaten agieren hilflos im Umgang mit sozialen Netzwerken

04.09.2024 ⌚ 5 min



Pro

Iran mischt sich in die US-Wahlen ein. Das Land baut seit Jahren seine Hacker-Fähigkeiten aus und ist zu einer Gefahr für den Westen geworden

28.08.2024 ⌚ 5 min





Spyware liest Nachrichten auf dem Handy mit oder hört Gespräche ab. Google will das verhindern. Zu Besuch bei einem der besten Spyware-Jäger der Welt

23.08.2024 ⌚ 9 min



Pro

China, Iran, Russland: Eine Allianz der Skrupellosen will die US-Wahlen manipulieren

15.08.2024 ⌚ 8 min



Mehr zum Thema Cyberangriff >



Elon Musk ist dafür, Nancy Pelosi dagegen: Kalifornien plant ein KI-Gesetz, das die Tech-Szene entzweit

11.09.2024 ⌚ 6 min

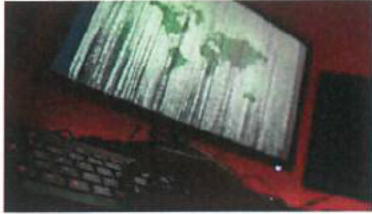


Pro

Iran mischt sich in die US-Wahlen ein. Das Land baut seit Jahren seine Hacker-Fähigkeiten aus und ist zu einer Gefahr für den Westen geworden

28.08.2024 ⌚ 5 min





US-Geheimdienste: Iran steckt hinter Hackerangriffen auf Wahlkampfteams

20.08.2024 ⌚ 2 min



Der Batteriehersteller Varta ist dank Porsche gerettet, doch die Aktionäre erleiden einen Totalverlust

19.08.2024 ⌚ 4 min



Pro

China, Iran, Russland: Eine Allianz der Skrupellosen will die US-Wahlen manipulieren

15.08.2024 ⌚ 8 min



Trump macht Iran für den Hackerangriff auf seine Kampagne verantwortlich

13.08.2024 ⌚ 3 min



Weitere Themen

Ransomware

Darknet

Für Sie empfohlen >



Landtagswahlen in Brandenburg: Ein linkes Bündnis hätte eine Mehrheit – die neuesten Umfragen

16.09.2024 ⌚ 2 min



DATENANALYSE

Harris ist so populär wie seit Jahren nicht mehr, doch das Rennen bleibt offen – die wichtigsten Grafiken zur US-Wahl 2024

17.09.2024 ⌚ 4 min



KURZMELDUNGEN

Kultur: Musikproduzent Roli Mosimann gestorben +++ Rockband Jane's Addiction bricht nach Bühnenzoff Tournee ab +++ Michael Jacksons Bruder Tito gestorben

Aktualisiert 17.09.2024



Er sperrt sie in einen Käfig, nimmt ihr den Pass ab, filmt und fesselt sie – bis die junge Frau die Flucht ergreift

Aktualisiert 17.09.2024 ⌚ 8 min





Die ZSC Lions und ihr Traum von der Dynastie – hat sich der Champion seinen Erfolgshunger bewahrt?

17.09.2024 ⌚ 5 min



Pro

Kosovo unter Spannung: Wenn es hart auf hart kommt, sind die Schweizer Friedenstruppen ganz vorne dabei

17.09.2024 ⌚ 7 min



Eine Mitmach-Sendung über die AfD steht in der Kritik

17.09.2024 ⌚ 3 min



Zürcher Regierungsrat erhöht den Eigenmietwert: Wohneigentümer bezahlen ab 2026 mehr Steuern

17.09.2024 ⌚ 3 min



Copyright © Neue Zürcher Zeitung AG. Alle Rechte vorbehalten. Eine Weiterverarbeitung, Wiederveröffentlichung oder dauerhafte Speicherung zu gewerblichen oder anderen Zwecken ohne vorherige ausdrückliche Erlaubnis von Neue Zürcher Zeitung ist nicht gestattet.

Home > Digital > **Hack-Angriff: Ransomware-Gruppe Play erpresst NZZ und CH Media**

Hacker-Gruppe Play erpresst «NZZ» – zittern vor Veröffentlichung im Darknet

«Mehr vertrauliche Daten gestohlen als angenommen»

Die Nervosität bei «NZZ» und CH Media steigt. Die beiden Verlage werden von der Hacker-Gruppe Play erpresst. Nun ist klar: Der Schaden ist grösser als vermutet. Die Hacker haben mehrmals gedroht, das Material zu veröffentlichen. Neuster Termin: Mittwoch, 3. Mai.

Publiziert: 21.04.2023 um 20:00 Uhr

Aktualisiert: 28.04.2023 um 08:44 Uhr



Thomas Benkö

Journalist & AI Innovation Lead

Kurz vor dem Wochenende hat «NZZ»-CEO Felix Graf ein neues Memo an die Belegschaft verschickt. Es liegt Blick vor. Die Worte tönen ein bisschen dramatischer als noch zu Beginn der Woche.

«Wie wir Euch bereits informiert haben, hat sich die Ransomware-Gruppe Play zum Cyberangriff auf die «NZZ» bekannt. Sie hat im Darknet angekündigt, im Besitz von Daten zu sein, und es besteht die Möglichkeit, dass sie diese ab Montag veröffentlicht», steht im Rund-E-Mail.

Update: Die Hackergruppe hat die Veröffentlichung inzwischen um mehrere Tage auf Mittwoch, 3. Mai, geschoben.

Und weiter: «Die Ermittlungen haben inzwischen ergeben, dass die Angreifer mehr Daten gestohlen haben, als zunächst angenommen. Darunter sind vermutlich auch vertrauliche Daten. Wie gross das Ausmass ist und welche Daten konkret betroffen sind, ist weiterhin Gegenstand der laufenden Abklärungen.»

Lohnlisten erbeutet?

Laut im Darknet veröffentlichten Infos der Gruppe Play, sollen unter den erbeuteten Daten folgende Dokumente sein:

- Private und persönliche vertrauliche Daten
- Projekte
- Lohnlisten
- Mitarbeiterinformationen

Die «NZZ» bittet die Mitarbeiter «dringlichst» am Montag selber keine Daten aus dem Darknet zu laden: «Die Gefahr ist gross, dass Schadsoftware und andere Viren heruntergeladen werden und die Aufbauarbeit der letzten Wochen gefährdet oder sogar zerstört wird.»

Seit dem 24. März kämpft die «NZZ» mit den Folgen des Hacks. Die Zeitungsproduktion stand an gewissen Tagen auf der Kippe, das ePaper funktioniert nicht und Mitarbeiter durften ihre Laptops nicht mehr benutzen.

Fast noch schlimmer erwischte es CH Media. Der Aargauer Verlag bezieht verschiedene IT-Services von der «NZZ»-Mediengruppe. Die Computersysteme sind miteinander vernetzt. Viele Regionalzeitungen von «Aargauer Zeitung» über das «St. Galler Tagblatt» bis zur «Luzerner Zeitung» erscheinen seit dem Hack mit einem verminderten Umfang bei der Regionalberichterstattung.

Auch CH Media informierte die Mitarbeiter am Anfang Woche über den Hack. Im internen Schreiben ist davon die Rede, dass die «Neuorganisation der ICT-Plattform nach wie vor im Gang ist» und dass man «sämtliche Marktauswirkungen bald bereinigen lassen» könne.

Was ist ein Ransomware-Angriff

Ein Ransomware-Angriff ist eine Art von Cyberangriff, bei dem ein Angreifer Schadsoftware auf einem Computer oder einem Netzwerk installiert, um die Daten des Opfers zu verschlüsseln oder zu sperren (auch Verschlüsselungstrojaner genannt). Der Angreifer fordert dann ein Lösegeld von den Opfern, um die Freigabe der verschlüsselten Daten zu ermöglichen. Oftmals drohen die Angreifer

Bekennerschreiben aus dem Darkweb

Was die Hacker genau bezweckten, ist unklar. Meistens geht es bei Ransomware-Angriffen aber darum, vom Opfer Geld zu erpressen.

Falls keine Zahlung eingehe, will Play die erbeuteten Daten am 24. April veröffentlichen – genau einen Monat nach dem Hack. Welche Summe die Hacker von den Verlagen erpressen, ist nicht bekannt. Die Geld-Verhandlungen könnte aber der Grund sein, warum der Veröffentlichungstermin immer wieder geschoben wird.

Nicht das erste Schweizer Opfer

Laut dem Branchenportal «Inside IT» (<https://www.inside-it.ch/ransomware-bande-play-bekennt-sich-zu-angriff-auf-nzz-und-ch-media-20230417>) ist es nicht der erste Angriff von Play auf eine Schweizer Firma. Das letzte bekannt gewordene Opfer sei im Februar Energie Pool Schweiz gewesen. Auch die Hotelkette H Hotels sei ins Visier der Kriminellen geraten. Damals hatte Play ernst gemacht und im Darkweb Dokumente wie Rechnungen, Identitätskarten und Buchungen von Hotelgästen veröffentlicht.

Phishingmail als Einfallstor?

Laut dem US-Sicherheitsdienstleister Avertium (<https://explore.avertium.com/resource/an-in-depth-look-at-play-ransomware>) ist die Play-Gruppe seit Juni 2022 aktiv. Damals gab es einen Angriff auf die Justizverwaltung der argentinischen Millionenstadt Cordoba. Die Angestellten konnten ihre Computer nicht mehr benutzen – und mussten auf Stift und Papier ausweichen.

Laut Avertium sei es Play bei Angriffen im Jahr 2022 gelungen, unter anderem eine Schwachstelle bei ungepatchten Exchange-Servern auszunutzen.

Im aktuellen Fall sei der Angriff aber profaner: Laut Insidern habe ein Mitarbeiter von CH-Media auf ein Phishingmail geklickt. Danach hatten die Angreifer Zugriff und konnten sich bis in die NZZ-Systeme durcharbeiten.

Anm. d. Red.: Dieser Artikel stammt vom 17. April und wurde am 28. April mit zusätzlichen Informationen ergänzt.



[Startseite](#) | [Schweiz](#) | Hackerangriff auf Medienhäuser: Internetpiraten veröffentlichen Lohnlisten, Erfolgsrechnungen und F

Hackerangriff auf Medienhäuser

Internetpiraten veröffentlichen Lohnlisten, Erfolgsrechnungen und Passwörter

Bei ihrem Cyberangriff auf die Medienunternehmen NZZ und CH Media haben Kriminelle auch sensible Daten erbeutet. Diese haben sie nun ins Darknet gestellt.



Philippe Reichen aus Lausanne

Publiziert: 03.05.2023, 16:25

Profitieren Sie von **47% Rabatt**: 1 Jahr ohne Werbung für 189.00 99.00

Nur für kurze Zeit





Wegen des Hackerangriffs erschien die NZZ zeitweise in reduziertem Umfang und die Regionalzeitungen von CH Media als Einheitsausgaben.
Foto: Christian Beutler (Keystone)



Jetzt abonnieren und von der Vorlesefunktion profitieren.

Abo abschliessen

Login

[BotTalk](#)

Die Hackergruppe Play hat ihre Drohung wahr gemacht und am Mittwoch die bei den Medienunternehmen NZZ und CH Media geklauten Daten ins Darknet gestellt. Eine erste Auswertung der Dokumente zeigt: Die Internetkriminellen entwendeten 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. Zudem enthält der gestohlene Datensatz Angaben über Kickbacks, die in vergangenen Jahren an Partnerunternehmen zurückgeflossen waren. Im Darknet sind zudem diverse Dateiordner abrufbar, die keine Informationen enthalten. Das deutet darauf hin, dass die Piraten wohl darauf hoffen, deren Inhalte auf Anfrage individuell verkaufen zu können.

**«Wir werden
konsequent gegen die
Weiterverbreitung von
widerrechtlich
veröffentlichten Daten
vorgehen.»**

aus einer Medienmitteilung von
CH Media

CH Media bestätigte am Mittwochvormittag in einer Medienmitteilung die Veröffentlichung von Daten: Bei einem Cyberangriff durch Ransomware auf die IT-Infrastruktur der NZZ-Mediengruppe seien Unternehmensdaten von CH Media gestohlen und in der Nacht auf Mittwoch widerrechtlich im Darknet veröffentlicht worden, schreibt das Medienunternehmen. NZZ-Sprecherin Karin Heim verweist ihrerseits darauf, dass nur CH Media betroffen sei und man bisher «keine Veröffentlichung von NZZ-Daten feststellen» konnte. «In Abstimmung mit den Behörden und aufgrund der rollenden Entwicklung», mache man derzeit keine detaillierteren Angaben.

Die Analysen laufen

Bei CH Media ist man daran, den Datenklau zu analysieren. «Erste Analysen zeigen, dass es sich um Daten unserer Zustellorganisationen handelt», schreibt das Unternehmen in einer Medienmitteilung. Kundendaten seien gemäss ersten Erkenntnissen nicht betroffen. Man setze «alles daran, die Daten der Kunden, Mitarbeitenden und unseres Unternehmens zu schützen» und werde «auch konsequent gegen die Weiterverbreitung und unrechtmässige Bearbeitung von widerrechtlich veröffentlichten Daten vorgehen», teilt CH Media mit.

Recherchen dieser Zeitung ergeben ein anderes Bild. Im Datenleck sind mutmasslich die Namen und Adressen Tausender Zeitungsabonnenten enthalten, auch solche der Zeitungen «Blick», «SonntagsZeitung» und «NZZ am Sonntag».

Das Medienunternehmen hat den Cyberangriff gemäss eigenen Angaben am 24. März 2023 entdeckt. Angegriffen wurden die gemeinsamen IT-Systeme von NZZ und CH Media. Bei den beiden Schweizer Medienhäusern hat man ursprünglich darauf gehofft, dass die Erpresser bluffen und nicht sonderlich viele Daten erbeuten konnten, deren Veröffentlichung die Verlage in Schwierigkeiten bringen würde. Nach ersten Erkenntnissen sei keine grosse Datenmenge abgeflossen, teilten die NZZ und CH Media Mitte April mit.

Doch später verschärfte sich offenbar die Situation: «Die Ermittlungen haben inzwischen ergeben, dass die Angreifer mehr Daten gestohlen haben als zunächst angenommen», zitierte der «Blick» aus einem Schreiben von NZZ-CEO Felix Graf an die Mitarbeitenden.

Wegen des Angriffs musste das Ostschweizer Radio FM1 eine Woche lang aus Zürich statt aus St. Gallen senden. Einige NZZ-Ausgaben erschienen mit leicht reduziertem Umfang. Deutlich gravierender traf es CH Media: Die «Aargauer Zeitung», die «Luzerner Zeitung» und das «St. Galler Tagblatt» konnten längere Zeit nur als Einheitsausgaben erscheinen – ohne unterschiedliche Regionalteile.

NEWSLETTER

Der Morgen Der perfekte Start in den Tag mit News und Geschichten aus der Schweiz und der Welt.

Weitere Newsletter

Einloggen

Philippe Reichen war bis 2024 Westschweizkorrespondent mit Sitz in Lausanne. Er hat an den Universitäten in Zürich und Freiburg im Breisgau Geschichte, Philosophie und Allgemeines Staatsrecht studiert. Mehr Infos
✕ @PhilippeReichen

Fehler gefunden? Jetzt melden.

22 Kommentare

Wie verbindlich ist die Meinung des zu Cookies und Künstlicher Intelligenz?

Beilage 8

EDÖB
VISCHER

13. Februar 2024, Rechtsanwalt Martin Steiger



Der EDÖB ist die schweizerische Datenschutz-Aufsichtsbehörde. Fachpersonen kritisieren immer wieder, dass die geäußerte Meinung über das geltende Datenschutzrecht hinausgeht, zum Beispiel zur Einwilligung für Cookies oder zur Transparenz bei Künstlicher Intelligenz.

Wie verbindlich ist die Meinung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten?

Für die «Datenschutz Plaudereien» diskutierte ich in einem Podcast-Gespräch mit David Rosenthal diese und weitere Fragen, unter anderem:

Wie verbindlich ist die Meinung des EDÖB jenseits des geltenden Datenschutzrechts?

Was sind die positiven Folgen, was die negativen Folgen für den Datenschutz?

Wie funktioniert die Diskussion zwischen Behörden und Praxis beim Datenschutz in der Schweiz?

Was bedeutet die Meinung einer Datenschutz-Aufsichtsbehörde in der Europäischen Union, zum Beispiel in Deutschland?

Wieso ist nicht mit einer gerichtlichen Klärung der diskutierten Fragen zu rechnen?



 podigee

DAT224 EDÖB: Wie verbindlich ist die Meinun...

«Es ist falsch»: David Rosenthal und Martin Steig...

Episode
abspielen 19:48

Abonnieren Teilen

Transkript: Gespräch mit David Rosenthal

Das nachfolgende Transkript wurde mit dem AI-Dienst CastMagic automatisiert erstellt und nur einige besonders grobe Fehler wurden von Hand korrigiert. Es gilt deshalb das gesprochene Wort, denn das Transkript enthält Fehler.

Martin Steiger: Guten Tag, mein Name ist Martin Steiger. In den heutigen «Datenschutz Plaudereien» freue ich mich, einmal mehr David Rosenthal als Spezialgast begrüßen zu dürfen. Das heutige Thema, über das wir reden wollen. Was ist die Bedeutung, wenn sich eine Aufsichtsbehörde im Datenschutzbereich, in der Schweiz der EDÖB, zu bestimmten Themen äussert? Bevor ich David das Wort gebe, möchte ich erst einen Einstieg geben, weil das Thema mindestens einen bestimmten Grund hat. David und ich wurden kürzlich von einem Journalisten angefragt, wie es mit den Rechten betroffener Personen bei Künstlicher Intelligenz in der Schweiz ist. Auch EDÖB wurde angefragt. Es wurde herausgestellt, als wir die Texte zum Gegenlesen bekamen, Zitate werden in der Schweiz meist autorisiert, dass David und ich recht ähnlich geantwortet haben, aber ziemlich anders als EDÖB.

Der EDÖB geht da sehr weit. Er gab auch eine Medienmitteilung heraus. Geltendes Datenschutzgesetz ist auf KI direkt anwendbar. Das war der eine Anlass. Und der andere Anlass war, ich glaube, sich hat EDÖB einen Leitfaden zu den TOM publiziert, also zu den technischen und organisatorischen Massnahmen, letztlich zur Umset-

zung des Datenschutzrechts. Und dort gibt es auch einen Absatz zu Cookies auf Websites. Und dort vertritt EDÖB eigentlich eine Position, wie man sie bis jetzt nur aus der EU kannte.

David, wie gehen wir damit um? Der EDÖB äussert eine Meinung. Er sagt zwar, es sei nicht verbindlich, aber er ist ja die Aufsichtsbehörde. Wenn er etwas veröffentlicht, gilt das ja schon irgendwie.

David Rosenthal: Das ist in der Schweiz eine sehr spannende Situation. Im Ausland, wo wir in der EU wären, wäre es unklar. Dann würden alle nur das zitieren und sagen, das sei praktisch Gesetz. Das ist in der Schweiz nicht so. Das hat vielleicht damit zu tun, dass wir häufig so Veranstaltungen wie jetzt machen, in denen wir sagen, dass das, was EDÖB sagt, eine Meinung ist. Vor allem in Fachkreisen ist es weit etabliert, dass es eine Meinung von mehreren ist. Daran darf und kann man widersprechen. Und sie ist auch nicht verbindlich und auch nicht zwingend richtig. Und sie kann auch sogar so sein. Das stört mich manchmal in diesem Zusammenhang. Es können auch Positionen sein, die zwar aus bestimmten Ecken wünschbar wären, aber die nicht vom Gesetz gedeckt sind. Das ist eher eine rechtspolitische Äusserung, kein knallhartes Gesetz, wie man sich das bei einer anderen Aufsichtsbehörde gewöhnt ist. Das ist in der Schweiz eine spezielle Situation.

Martin Steiger: Aber jetzt sagst Du, das ist nicht das Gesetz. Zum Beispiel schreibt der EDÖB im Zusammenhang mit den TOM, dass die wichtigsten Vorgaben des Datenschutzgesetzes wiedergegeben werden. Das ist das Thema der Verhältnismässigkeit, der Erkennbarkeit, der Zweckbestimmtheit. Muss man einwilligen, ja oder nein? Das hat eine Auswirkung. Letztlich hat es die Auswirkung, dass ich mir als Verantwortlicher sage, dass ich zwar anderer Meinung bin, und dass Rosenthal oder Steiger sagen, das sei anders. Der Beobachter hat beim KI-Thema getitelt, die Fachleute streiten sich. Der EDÖB wünscht sich eine gerichtliche Erklärung. Als Verantwortlicher sage ich mir aber doch: Ja, der EDÖB untersucht mich am Schluss, der EDÖB verfügt.

David Rosenthal: Das ist richtig. Das finde ich auch schade. Es ist durchaus so, wenn man mit ihm selbst spricht ... Der EDÖB ist eine Funktion, aber auch, wenn man mit dem Leiter spricht, sagt er sehr häufig, er leiste einen Diskussionsbeitrag. Da macht er sich kleiner als das, was, wie du zu recht sagst, die Leute können sehen, es ist eine Behörde, es ist Bern. Die sagen, es sei so. Das ist das Problem.

Du hast natürlich recht, der, der nicht genau Bescheid weiss, wird das für bare Münzen nehmen. Dann passiert etwas, das der Gesetzgeber nicht vorgesehen hat. Ich glaube nicht, dass es zur Verfügung je gekommen wird. Das sehen wir in der Schweiz sowieso ganz selten. Sondern, dass man das dann einfach stillschweigend so macht. Und dass das natürlich dann eine Wirkung hat, die eigentlich nicht vom Gesetzgeber gewollt ist, finde ich persönlich nicht richtig und nicht gut.

Martin Steiger: Das fällt tatsächlich auf. Wenn man es beim TOM-Leitfaden anschaut und dort ausdrücklich die Cookie-Thematik. Dort wird ausdrücklich Artikel 7 Absatz 3 DSG genannt. Wir hatten auch schon ein Podcast-Gespräch darüber geführt, auch unter dem Aufhänger Cookie-Banner. Auch das kommt als Beispiel mit den datenschutzfreundlichen Voreinstellungen. Da kommt ein ganz konkretes Beispiel. Wenn man Cookies auf einer Website sammelt, müsse für alle Cookies, die nicht notwendig seien, die aktive Einwilligung eingeholt wer-

den. Sie müssen standardmässig deaktiviert sein. Für mich ist das eigentlich 1:1 die ePrivacy-Richtlinie, nationale Umsetzung in EU-Mitgliedstaaten und dann vielleicht noch in DSGVO. Das passt doch nicht.

David Rosenthal: Es ist falsch. Es gibt ein anderes Beispiel, das wir seit Jahren kennen. Es gibt immer wieder Situationen, in letzter Zeit ein bisschen weniger, in denen EDÖB behauptet hat, für die Bearbeitung besonders schützenswerter Personendaten, also Gesundheitsdaten und solche Geschichten, brauche es eine Einwilligung. Im Gesetz steht genau das nicht. Es heisst, es braucht eine Rechtfertigungsgrund, also nicht zwingend eine Einwilligung, wenn ich sie einem Dritten weitergeben möchte. Das ist einfach eine falsche Aussage.

Da frage ich mich manchmal, was die Motivation dahinter ist. Man kann es nicht so oder anders verstehen. Es ist einfach nicht so. Aber ich erkläre mir das normalerweise damit, dass man damit etwas erreichen will. Es ist eher eine politische Aussage, was aber ein rechtsstaatliches Problem ist. Er ist eine Behörde und hat eine bestimmte Glaubwürdigkeit, die er mit seinem Amt mitbekommt. Da wäre er meiner Meinung nach verpflichtet, sich an diese Regeln zu halten. Dann kann man sagen, es wäre sinnvoll und es würde erwarten, dass man weitergeht.

Es gibt auch in der Schweiz viele Firmen, die sagen, wir wollen, weil es eine Erwartungshaltung gibt, bei Cookies, sagen, ja, du musst eine Einwilligung geben. Das kann man ja machen, aber dann ist es vielleicht ein Good Practice oder etwas Übergesetzliches oder etwas, was ich aus ethischen Überlegungen sonst mache, aber es ist nicht das Recht. Es ist keine Pflicht. Diese Vermischung zwischen so ein bisschen, wie ich es gerne hätte, und wie ich es hart vom Gesetzgeber vorgesehen habe, sehen wir im Datenschutz häufig. Es gibt sie, muss man gerechterweise sagen, auch in der EU. Also in der EU, wo ich zum Teil in diesen Bereichen schon strengere Regelungen habe, dann gehen sie ja noch weiter. Dort sagen sie ja, der Datenschutz gelte selbst dann, wenn gar keine Personendaten vorliegen. Das heisst, sie definieren dann einfach Personendaten viel breiter, als wir oder der EDÖB in der Schweiz das machen würde.

Also es gibt halt immer so ein bisschen eine «Race to the Top», das Ganze auszuweiten und auszudehnen. Und das ist halt einfach nicht das, was der Gesetzgeber will. Und da bin ich der Meinung, man kann darüber streiten, inhaltlich, was man gut und richtig fände, aber wir haben das Gesetz, sondern das muss man sich halten. Und die Leute sind dann äusserst verwirrt. In der Cloud-Diskussion haben wir das Gleiche. Auch nicht nur vom EDÖB. Andere Datenschutzbehörden behaupten Dinge, die es auf keine Kuhhaut gehen. Aber es ist eine Behörde. Dagegen anzukämpfen ist bei einem Publikum, das das nicht selbst verstehen kann, weil es nicht in der Fachmaterie ist, extrem schwierig. Es braucht viel Energie, die an anderen Orten verloren geht. Meistens bringen Diskussionen gar nichts.

Martin Steiger: Du hast das Gesetz erwähnt, das DSG. Das ist noch recht jung. Da sind ja politische Entscheidungen im Parlament getroffen worden. Man hätte ein Referendum ergreifen können. Jetzt bringt der EDÖB ein Wunschkonzert, zum Beispiel einen Anspruch auf Datenminimierung. Also auch da in diesem TOM-Leitfaden. Man darf immer noch das absolute Minimum an Personendaten bearbeiten. Da haben wir doch einen rechten Gap.

David Rosenthal: Ja, ja. Das zieht sich natürlich überall durch. Man kann nicht gegen alles angehen. Es gibt ja Bereiche, wo, wenn Dinge da sind, man eine Diskussion führen kann, die fruchtbar ist, wo man verschiedene Positionen hat. In gewissen Situationen sind die Dinge natürlich anders. Aber dann ist die Frage, wer die Diskussion führt. Und wo passiert sie überall? Eigentlich haben wir in der Schweiz eine Aufsichtsbehörde, die sich selber eher zurückhält. Wenn man ihn fragt, was er tun muss. Er sagt zum Beispiel nicht sehr viel zum Thema KI. Er hat wesentlich nur ein Statement gemacht, damit auch etwas gesagt wurde.

Das ist eine ambivalente Situation, weil er eigentlich kein «Soft Law» machen will, aber einzelne Statements macht, die sehr weit gehen. Da müssen wir das hinterfragen. Das hat in der Schweiz zum Glück Tradition. Und er ist, und das muss ich ihm auch hoch anrechnen. Wenn ich ihm jetzt auch offen widerspreche an gewissen Orten, ich habe das auch schriftlich gemacht, schon sehr deutsch und deutlich, er nimmt es dann auch sportlich und nimmt es dann nicht in diesem Sinne persönlich. Also er ist durchaus für diese Diskussion da, was andere nicht wären. Die Schwierigkeit ist für den Rechtsanwender und die Rechtsanwenderin, also die, die dann irgendwie etwas Praktisches machen. Und da muss man halt sagen, du kannst es einfach nicht alles für bare Münzen nehmen, was hier kommt. Und das finde ich schade, weil das sollte es eigentlich nicht sein.

Martin Steiger: Das mit der Diskussion, David, kann ich bestätigen. Der EDÖB, die Person und die Behörde, die Leute, die dort arbeiten, sind sehr offen und diskussionsfreudig. Bei den Kantonen war es unterschiedlich, aber auch dort von der Tendenz her. Was die KI-Thematik betrifft, hat er im Titel im Wesentlichen gesagt, das Datenschutzrecht sei auf KI direkt anwendbar. Das war auf den ersten Blick etwas trivial. Ich habe aber von Leuten aus der Verwaltung, die dort Datenschutz machen, gehört, sie seien wirklich froh gewesen über Statement, weil das hätte sie gestärkt. Weil das sei offenbar nicht so selbstverständlich gewesen, das einfach so als Nebenbemerkung.

David Rosenthal: Ich glaube, es hat zum Teil in seinen Äusserungen. Das hat vielleicht auch damit zu tun, dass er als Behörde, und sie sind nicht gross, sie haben nicht viele Leute, also mit sehr wenigen Personen müssen sie eine Riesenaufgabe machen. Ich sagte immer, wenn wir das Geld investieren könnten in ein neues Gesetz oder in mehr Leute beim EDÖB, würden wir viel mehr für den Datenschutz machen, als dass alle Leute ihn mit Bearbeitungsverzeichnissen zuspammen und andere Dinge machen. Das ist natürlich nicht so en vogue. Aber das hat auch zur Folge, dass er viele Themen gar nicht so genau kennt. Die Cookie-Thematik, du erlebst es ja selbst auch. Selbst unter den Profis gibt es viele, die gar nicht so recht verstehen, wie das genau läuft. Es ist ziemlich kompliziert. Man sieht viele Dinge.

Ich denke nicht, dass es böse will, dass er sagt, man müsse das so und so machen. Er hat gewisse Ambitionen, die über den Datenschutz hinausgehen. Er hat Fälle gemacht, wo er Konsumentenschutz recht durchbringt. Er sagt, die Gerichte können wir zurückbinden. Wenn sie das machen, so be it, es gibt mehrere solche Fälle. Das ist ein Ort, an dem man die Differenzierung nicht kennt. Er tut damit nicht viel. Warum sollte EDÖB Top-Experte in KI-Themen sein, wenn er es ja selber an vielen Orten vielleicht gar nicht einsetzen darf und sich dann dazu äussert? Deshalb nimmt man aus diesem Grund gewisse Aussagen nicht für bare Münze nehmen darf.

Wenn man zu ihm kommt und sagt, Adrian Lobsiger, es sei in dem und dem Fall so und so ist, reagiert er. Man kann mit ihm reden und er sagt, das stimme eigentlich. Das müsste man noch anders sehen. Dass dann Statements, die da sind. Ich wiederhole mich, dass man nicht für bare Münzen nehmen darf, weil sie am Schluss hoffentlich bei einem Einzelfall nicht so durchgesetzt werden.

Das ist die andere Seite. Das habe ich leider auch immer wieder erlebt in Untersuchungen. Man muss sehr stark dagegen kämpfen, dass zum Teil auch Mitarbeiter oder Mitarbeiterinnen vom EDÖB vor Ort sind. Zum Teil fachlich, nicht wirklich das Gelbe vom Ei, irgendwelche Dinge behaupten, die einfach nicht stimmen. Man muss kämpfen, Das ist mühsam, aber das betrifft nicht viele.

Martin Steiger: Du hast den Konsumentenschutz erwähnt. Ich sehe auch ein Problem. Ich erlebe das auch bei den Digitalen Gesellschaften in der Schweiz. Die betroffenen Personen sind frustriert. Sie lesen beim EDÖB etwas, gelangen damit an Verantwortliche und bekommen nicht, was sie wollen, zum Beispiel Sachen Transparenz oder Widerspruch. Man kann sagen, mehr Transparenz ist sinnvoll, man soll die Leute selbst entscheiden. Aber es gibt auch Verantwortliche, die sauber korrekte Antworten machen und erklären, warum die Ansprüche, die der EDÖB genannt hat, wenn sie in den Medien stehen, eben nicht erfüllt werden. Das ist doch auch so eine Dissonanz, die eigentlich unerfreulich ist.

David Rosenthal: Ja, und ich glaube, wir werden das wahrscheinlich nicht ändern. Und das mit der Transparenz kann man meist relativ einfach erklären. Er sagt ja, dass man jeden Einsatz von KI offenlegen muss. Man muss sich transparent machen. Ich würde wissen wollen, wie viele Leute beim EDÖP, die Übersetzungsfunktionen wie DeepL, die klassische KI, einsetzen, und darüber informiert haben, dass sie das machen, und die im Prinzip hingehen und sagen, wir wollen jetzt diesen Text, ich kann leider nicht so gut Französisch übersetzen, das wird nicht passieren. An vielen anderen Orten auch nicht. Wenn man sieht, wie man das in der Praxis umsetzen möchte, funktioniert das nicht.

Deshalb ist am Schluss auch ein gewisser gesunder Menschenverstand erforderlich. Wenn jemand das macht und sich diese Frage überlegt, dann hat er schon sehr viel gemacht. Vielleicht will er auch diese Leute erreichen, dass man sagen kann, dass sie sich etwas dazu Gedanken gemacht haben. Insofern finde ich das eigentlich gut. Wir sehen das sehr häufig bei neuen Technologien, dass sich die Unternehmen zum ersten Mal überhaupt mit Fragen beschäftigen, die sie eigentlich schon lange hätten machen müssen. Ein anderes Beispiel ist die Aufbewahrungspflicht. Das ist alles nichts Neues. Aber jetzt kommen die Unternehmen und führen eine Cloud-Lösung ein. Und die wollen alle sagen, Cloud sei ganz schlimm. Also, Big Problem. Sie fangen sich jetzt an, ernsthaft mit diesen Fragen alles Punkt für Punkt anzugehen, was sie eigentlich schon seit zehn Jahren machen sollten. Und wenn das natürlich hilft, wenn man sich jetzt überlegen darf, wie das funktioniert, dann hat es natürlich etwas Gutes da.

Aber wir wissen es nicht. Es kommuniziert ja nicht sehr viel, sondern es sind meistens auch etwas sphinxhafte Statements, die dann herauskommen. Dann muss man sich überlegen, was man damit macht. Ich bin mir nicht sicher, ob ich es gut oder schlecht finde. Gut finde ich es vielleicht, weil es zu einer Diskussion führt, wo man sel-

ber etwas dazu sagen kann und es nicht so absolut überkommt, dass er das Recht für sich beansprucht, wie das zum Beispiel die deutschen Aufsichtsbehörden sagen. Die sagen nicht, es muss dann ein Gericht entscheiden, we will see. Ich sage, es ist einfach so. Schlecht finde ich es, weil das ist das, was du vorher am Anfang gesagt hast, was für eine Verunsicherung und Diskussionen sorgt. Wir hatten es auch beim Thema Cloud, du hast Cookies erwähnt, wenn es um besonders schützenswerte Personendaten geht. An x Ort kommen immer wieder State-ments, die schräg in der Landschaft stehen. Für uns zwei, wir könnten auch sagen, es sei gut, es wäre ein Beratungsauftrag, und ich sage das immer wieder, ich finde es schade, weil es Geld verschwendet. Man könnte es für TOMs einsetzen statt für Juristen, Dann wäre viel mehr für den Datenschutz da.

Martin Steiger: Es wäre eine böse Unterstellung, dass der EDÖB verschiedene Aktien von Consent-Management-Firmen hat. Das ist eindeutig ein Business-Development. Aber nein, das will ich auf keinen Fall unterstellen. Da bin ich ziemlich sicher, dass es nicht so ist, dass das auch nicht die Absicht ist. Und du sagst es ja mit den Ressourcen. Also wir haben beschränkte Ressourcen, beschränkte Zeit. Es ist ja nicht nur das Geld. Und dann könnte man das wie für anders einsetzen.

Was ich dann aber noch lustig finde, ist jetzt auch mit dieser gerichtlichen Klärung. In dem Medienbericht, den ich auch verlinke, in den Shownotes, wird EDÖB auch quasi zitiert. Ja, eben, das werde dann gerichtlich geklärt, wenn jemand seine Anordnungen bestreitet. Also, es ist ja noch mal ein Schritt zurück, weil du hast richtig gesagt, das ist sehr selten etwas zu erwarten. Das kennt man auch. Im Normalfall, wenn jemand nach dem neuen DSGVO beim EDÖB Anzeige mache, dann wird man mal recht nett im Normalfall kontaktiert. Man soll eine Aufklärung leisten. Es gibt eine Empfehlung, wie man sich das anders machen sollte. Von dem her ist das auch noch ein weiteres Kuriosum. Wir sind sehr weit entfernt, das jemals klären zu können. Und wenn es geklärt wird, dann wieder häufig im falschen Fall.

David Rosenthal: Und das ist auch nicht der Stil in der Schweiz. Der Stil in der Schweiz ist weder Strafverfahren. Er selbst sagt, es werde in seiner Amtszeit, hätte er letzthin er öffentlich gesagt, es werde kein Straffall zum Abschluss kommen. Er glaubt das nicht. Auch seine Verfahren sind vor allem dort, wo es ein sehr hoher Leidensdruck ist. Aber wenn ich jetzt natürlich hingeh, und ich hatte auch schon Klienten, die zu mir kamen, und dann gesagt haben, dass sie bei mir dort waren, und er konnte ihnen nicht weiterhelfen. Das kann man ja gar nicht mit diesen Massen. Dann versickern sie halt eben meist, weil das nicht zu einem Verfahren führt. Und die zivilen Verfahren gibt es ja auch nicht. Also, das ist ganz anders.

Ich habe mich kürzlich mit einem Anwaltskollegen aus Deutschland unterhalten. Ihr Hauptbusiness ist nicht die Compliance-Beratung. Sie sagen, es sind Verfahren mit den Aufsichtsbehörden. Es ist eine ganze Industrie. Sie wissen genau, wenn hier etwas kommt, und da ist ein Zettel drauf und steht «Aufsichtsbehörde», dann wissen sie, das geht jetzt zwei Jahre, weil dann nehmen sie die auseinander. Und das haben wir natürlich in der Schweiz auch nicht. Also wir haben auch die Verfahren, die, wenn wir dort laufen, bei uns etwas anderes laufen, was ich aber auch richtig finde, weil dort passt keine Kuhhaut, die man dort im Ausland sieht.

Martin Steiger: Ja, die Hürden sind hoch, je nachdem, wo man steht, natürlich im Guten wie im Schlechten. Also es gibt sicher Aktivisten und betroffene Personen in der Schweiz, die da gerne ein bisschen mehr Verfahren hätten, die ein bisschen neidisch nach Deutschland oder nach Europa schauen, was Max Schrems so macht.

Nebenbei fand ich interessant, bei dem neuen Angemessenheitsbeschluss der Europäischen Kommission, wie sie Rechtslage in der Schweiz im Zusammenhang mit dem Überwachungsbereich beurteilt haben. Wir haben das auch schon diskutiert. Wir haben frapante Ähnlichkeiten mit den USA, so bei den Rechtsmitteln und so. Geschichten kann man gerne nachlesen, haben wir ausführlich diskutiert. Aber ja, da sind wir, glaube ich, alles in allem so gut unterwegs.

Und für die, die ein bisschen mehr darüber nachdenken, ist es ja auch eine Chance. Also die, die jetzt ein bisschen bequem sind, vielleicht sagen, wir machen es, wie es EDÖB empfiehlt, unverbindlich oder wie auch immer, vielleicht zum eigenen Nachteil. Und alle anderen können sich Gedanken machen und sagen, sie machen es vielleicht nicht wie EDÖB, aber trotzdem richtig. Aber trotzdem richtig.

David Rosenthal: Genau.

Bilder: OpenAI / ChatGPT 4.

Rechtsanwalt Martin Steiger

Martin Steiger ist Anwalt und Unternehmer für Recht im digitalen Raum. Er befasst sich insbesondere mit Datenschutzrecht, Immaterialgüterrecht, IT-Recht und Medienrecht. Neben seiner Anwaltstätigkeit engagiert er sich unter anderem bei der Digitalen Gesellschaft und bei TEDxZürich. Martin Steiger ist ausserdem Mitgründer der Legal Tech-Unternehmen Datenschutzpartner AG (Schweiz) und VGS Datenschutzpartner GmbH (Deutschland).



[Rechtsanwalt Martin Steiger kontaktieren](#)

Alle Rechtsanwältinnen und Rechtsanwälte bei Steiger Legal sind eingetragen im Anwaltsregister des Kantons Zürich sowie Mitglied im Schweizerischen Anwaltsverband (SAV) und im Zürcher Anwaltsverband (ZAV).

Steiger Legal AG
Florastrasse 1

E-Mail info@steigerlegal.ch
Telefon +41 44 533 13 60

8008 Zürich
Schweiz

NZZ

Cyberangriff auf das Unternehmen NZZ: Veröffentlichung von NZZ-Daten im Darknet

Die NZZ wurde Ende März Ziel eines Cyberangriffs. Die Angreifer haben nun gestohlene Daten veröffentlicht, auch von Kunden. Nach aktuellen Erkenntnissen handelt es sich dabei um öffentlich zugängliche Daten.

NZZ-Redaktion

11.05.2023, 19.15 Uhr ⌚ 2 min



Das Logo der NZZ auf dem Dach des Hauptsitzes an der Falkenstrasse in Zürich.

Goran Basic

Die NZZ ist ein Unternehmen, das in der Schweiz ansässig ist. Es ist ein führendes Medienunternehmen in der Schweiz und hat eine lange Geschichte. Die NZZ ist bekannt für ihre unabhängige Berichterstattung und ihre hohe Qualität. Die NZZ ist ein Unternehmen, das in der Schweiz ansässig ist. Es ist ein führendes Medienunternehmen in der Schweiz und hat eine lange Geschichte. Die NZZ ist bekannt für ihre unabhängige Berichterstattung und ihre hohe Qualität.

Mit de

Unternehmen in der Lage, den Betrieb mit nur geringen Einschränkungen aufrechtzuerhalten und den Angriff damit weitgehend einzudämmen.

Die Ransomware-Gruppe «Play» hat nun, wie angedroht, gestohlene Daten im Darknet veröffentlicht. Wie bereits kommuniziert, können wir leider nicht ausschliessen, dass auch Kundendaten betroffen sein können. Darunter wären nach jetzigem Kenntnisstand Namen und Adressdaten einzelner Abonnentinnen und Abonnenten in der Schweiz.

Nach aktuellen Erkenntnissen handelt es sich dabei um öffentlich zugängliche Daten. Aktuell werden die Daten analysiert, was aufgrund des grossen Datenvolumens einige Zeit in Anspruch nehmen wird. Wir werden wieder zum Thema informieren, sobald gesicherte Informationen vorhanden sind. Wir bedauern den Vorfall und bitten Sie für die Unannehmlichkeiten um Entschuldigung.

Für die weiteren Abklärungen arbeitet das Unternehmen wie bisher eng mit den zuständigen Behörden, der Kantonspolizei und ihren Cybersicherheitsexperten zusammen. Die NZZ hat bereits zusätzliche Massnahmen ergriffen, um die Sicherheit ihrer IT-Infrastruktur weiter zu erhöhen und das Risiko von zukünftigen Angriffen zu minimieren.

Die Zeitungsproduktion der NZZ ist weiterhin sichergestellt. Alle kundenkritischen Systeme stehen zur Verfügung. Das digitale

Angebot unter nzz.ch und in der NZZ-App ist wie immer vollumfänglich verfügbar.

Passend zum Artikel



Wenn die Benzinversorgung ausfällt und das Spital stillsteht: Warum Ransomware-Angriffe so gefährlich sind

11.12.2022 ⌚ 7 min



Cyberangriffe im Auftrag des Kremls: Wenn kriminelle Banden für den russischen Geheimdienst arbeiten

07.05.2023 ⌚ 8 min



Mehr zum Thema Cyberangriff >



Elon Musk ist dafür, Nancy Pelosi dagegen: Kalifornien plant ein KI-Gesetz, das die Tech-Szene entzweit

11.09.2024 ⌚ 6 min



Pro

Iran mischt sich in die US-Wahlen ein. Das Land baut seit Jahren seine Hacker-Fähigkeiten aus und ist zu einer Gefahr für den Westen geworden

28.08.2024 ⌚ 5 min





US-Geheimdienste: Iran steckt hinter Hackerangriffen auf Wahlkampfteams

20.08.2024 ⌚ 2 min



Der Batteriehersteller Varta ist dank Porsche gerettet, doch die Aktionäre erleiden einen Totalverlust

19.08.2024 ⌚ 4 min



Pro

China, Iran, Russland: Eine Allianz der Skrupellosen will die US-Wahlen manipulieren

15.08.2024 ⌚ 8 min



Trump macht Iran für den Hackerangriff auf seine Kampagne verantwortlich

13.08.2024 ⌚ 3 min



Weitere Themen

Darknet

Für Sie empfohlen >



NZZ ERKLÄRT

Neue Hymne, mehr Teams, keine Gruppenphase: So funktioniert die neue Champions League

Aktualisiert vor 1 Stunde 5 min



Wohnmobil im Test: der Pragmatiker unter den Camper-Vans

16.09.2024 4 min



Pro

Wenn Einzeltäter und Terrorgruppen sich das IS-Label anhängen, maximieren sie ihre Wirkung

17.09.2024 5 min



DATENANALYSE

Harris ist so populär wie seit Jahren nicht mehr, doch das Rennen bleibt offen – die wichtigsten Grafiken zur US-Wahl 2024

Aktualisiert vor 4 Stunden 4 min





NZZ ERKLÄRT

Warum Wien trotz Hochwasserschutz mit den Wassermassen zu kämpfen hat – eine Videoanalyse vor Ort

vor 4 Stunden 2 min



Landtagswahlen in Brandenburg: Ein linkes Bündnis hätte eine Mehrheit – die neuesten Umfragen

16.09.2024 2 min



NZZ AKZENT

In Mosul verkündete der IS sein Kalifat. Wie geht es der Stadt heute, 10 Jahre nach dem Terror?

17.09.2024 18 min



Pro

Kosovo unter Spannung: Wenn es hart auf hart kommt, sind die Schweizer Friedenstruppen ganz vorne dabei

17.09.2024 7 min



Copyright © Neue Zürcher Zeitung AG. Alle Rechte vorbehalten. Eine Weiterverarbeitung, Wiederveröffentlichung oder dauerhafte Speicherung zu gewerblichen oder anderen Zwecken ohne vorherige ausdrückliche Erlaubnis von Neue Zürcher Zeitung ist nicht gestattet.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Justiz BJ

Information zum Datenabfluss bei Xplain

Ende Mai 2023 wurde bekannt, dass die Schweizer Firma Xplain, eine Anbieterin von Behörden-Software, Opfer eines Ransomware-Angriffs geworden ist. Bei einem Ransomware-Angriff werden Dateien des Opfers verschlüsselt und somit unbrauchbar gemacht, damit Lösegeld erpresst werden kann. Dabei hat die unter dem Namen "Play" auftretende Hackergruppierung grosse Datenmengen gestohlen. Darunter befinden sich auch operative Daten der Bundesverwaltung, welche durch den laufenden Betrieb der Informationssysteme der Bundesverwaltung entstehen.

Da Xplain in Absprache mit den Strafverfolgungsbehörden und dem Nationalen Zentrum für Cybersicherheit (NCSC) keine Lösegeldzahlung an die Hacker geleistet hatte, veröffentlichten diese am 14. Juni 2023 das entwendete Datenpaket im Darknet.

Seit Bekanntwerden dieses Datenabflusses hat das NCSC in enger Zusammenarbeit mit den betroffenen Behörden eine Organisation zur Bewältigung des Vorfalls etabliert. Es laufen intensive Arbeiten zur Auswertung und Analyse der gestohlenen Daten. Der Bund hat zudem Massnahmen eingeleitet, um das Sicherheitsrisiko für die Bundesverwaltung zu minimieren.

Nach wie vor gibt es keine Hinweise darauf, dass Bundessysteme direkt angegriffen wurden. Da operative Daten vom Angriff betroffen sind, haben verschiedene Stellen der Bundesverwaltung Strafanzeige erstattet oder prüfen diesen Schritt. Mit dem Vorgehen soll insbesondere geklärt werden, wie und warum Daten aus der Bundesverwaltung auf das System der Firma Xplain gelangen konnten.

Auch das Bundesamt für Justiz ist betroffen

Vom Datenabfluss bei Xplain sind auch Personendaten betroffen, für deren Bearbeitung das Bundesamt für Justiz (BJ) zuständig ist.

Gemäss aktuellem Stand der Analysen handelt es sich um Daten im Zusammenhang mit den Aufgaben des BJ im Bereich der internationalen Rechtshilfe in Strafsachen. Dies betrifft die Auslieferung, weitere Rechtshilfemassnahmen, die stellvertretende Strafverfolgung und -vollstreckung sowie die Überstellung von verurteilten Personen.

Besonders betroffene Personen werden vom BJ mit einem persönlichen Schreiben direkt informiert. Sonstige Anfragen in diesem Zusammenhang werden ausschliesslich über das untenstehende Formular entgegengenommen.

Das BJ hat den Vorfall dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gemeldet. Die vorliegenden Informationen zu diesem Vorfall werden nach dem Stand der Kenntnisse laufend ergänzt.

Links

[Untersuchung gegen fedpol und BAZG](#)

Medienmitteilung vom 21. Juni 2023

[Hackerangriff auf Firma Xplain: Bundesrat mandatiert politisch-strategischen Krisenstab "Datenabfluss"](#)

Medienmitteilung vom 28. Juni 2023

[Hackerangriff auf die Firma Xplain: Erste Erkenntnisse aus Datenanalysen zeigen Handlungsbedarf](#)

Medienmitteilung vom 14. Juni 2023

[Hackerangriff auf die Firma Xplain: Auch die Bundesverwaltung ist betroffen](#)

Medienmitteilung vom 8. Juni 2023

Kontaktformular

Von*

Ihre E-Mail-Adresse

Anrede*

- ☐ Herr
- ☐ Frau
- ☐ Keine Anrede

Name*

Vorname*

Adresse*

Wohnort*

Telefon

Ihr Anliegen*

5 + 2*

Bitte geben Sie das Ergebnis ein.

Alle Felder, die mit * gekennzeichnet sind, müssen ausgefüllt werden.

Letzte Änderung 07.09.2023

<https://www.bj.admin.ch/content/bj/de/home/staat/datenschutz/info-xplain.html>