La Kanzlei

CNIL verhängt erstmals Geldbuße gegen Auftragsverarbeiter

Datenschutz / IT

Jeanne Faymonville

Mélanie Allemand

Wegen unzureichender Sicherheitsmaßnahmen gegen Cyberattacken hat die französische Datenschutzbehörde CNIL (Commission Nationale de l'Informatique et des Libertés) am 27.01.2021 ein Bußgeld sowohl gegen den für die Datenverarbeitung Verantwortlichen als auch erstmals gegen den mit der Verwaltung seiner Website betrauten Auftragsverarbeiter verhängt.

Zwischen Juni 2018 und Januar 2020 waren der CNIL mehrere Verstöße gegen Datenschutzbestimmungen gemeldet worden, die eine Website betrafen, auf der mehrere Millionen Nutzer regelmäßig Einkäufe tätigen.

Bei einer Überprüfung stellte sich heraus, dass die Website wiederholt Ziel von Cyberangriffen geworden war. Bei der von den Hackern angewandten Methode, die als *Credential stuffing* bezeichnet wird, werden Nutzerdaten (in der Regel Listen mit Zugangsdaten aus vorhergehenden Datendiebstählen) verwendet, um mithilfe sogenannter *Bots* Anmeldeversuche auf einer Vielzahl von Websites zu unternehmen, in der Hoffnung, dass viele Nutzer dieselben Zugangsdaten für mehrere Websites verwenden. Ist die Authentifizierung erfolgreich, lassen sich auf diese Weise weitere, mit dem Benutzerkonto verbundene Daten einsehen.

Im vorliegenden Fall verschafften sich die Hacker auf diese Weise Zugang zu persönlichen Daten von etwa 40.000 Nutzern der Website.

Die CNIL wirft dem für die Datenverarbeitung Verantwortlichen und dessen Auftragsverarbeiter vor, geeignete Maßnahmen zur Bekämpfung dieser wiederholten Cyberattacken zu langsam ergriffen und damit gegen ihre Sorgfaltspflicht verstoßen zu haben.

Tatsächlich hatten der Verantwortliche und der Auftragsverarbeiter nach den ersten Cyberattacken beschlossen, ein Tool zur Abwehr derartiger Angriffe zu entwickeln. Allerdings nahm die Entwicklung des Tools ein Jahr Zeit in Anspruch. Nach Ansicht der CNIL hätten in der Zwischenzeit

weitere Maßnahmen ergriffen werden müssen, die ihre schützende Wirkung wesentlich schneller entfaltet hätten, beispielweise eine Beschränkung der Anzahl der Anmeldeversuche pro IP-Adresse oder die Anwendung eines CAPTCHA ab dem ersten Anmeldeversuch.

Die CNIL ist der Auffassung, dass der Verantwortliche und der Auftragsverarbeiter damit gegen Artikel 32 der DSGVO verstoßen haben. Infolgedessen verhängte sie ein Bußgeld sowohl gegen den Verantwortlichen (150.000 €) als auch gegen den Auftragsverarbeiter (75.000 €). Die Höhe des Bußgeldes wurde, so die CNIL, unter Berücksichtigung der jeweiligen Verantwortung beider Beteiligten festgelegt.

Denn gemäß geltenden Datenschutzbestimmungen ist es der für die Verarbeitung Verantwortliche, der über die zu ergreifenden Maßnahmen zu entscheiden hat und seinem Auftragsverarbeiter entsprechende Weisungen erteilen muss. Die CNIL betont allerdings, dass auch der Auftragsverarbeiter verpflichtet ist, nach den geeignetsten technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten zu suchen und diese dem Verantwortlichen vorzuschlagen.

Diese Entscheidung ist insofern überraschend, als die CNIL bis dato systematisch jegliche Haftung und damit auch jede Sanktionierung von Auftragsverarbeitern ausgeschlossen hat, da diese, so die bisherige Begründung der CNIL, stets im Auftrag und auf Weisung des für die Datenverarbeitung Verantwortlichen handeln. Aus diesem Grund wurden Sanktionen bislang – selbst im Falle einer Zuwiderhandlung durch den Auftragsverarbeiter – ausschließlich gegen den für die Datenverarbeitung Verantwortlichen verhängt.

Praxistipp:

Die CNIL weist Unternehmen auf die Notwendigkeit hin, größere Sorgfalt beim Schutz vor *Credential Stuffing*-Angriffen walten zu lassen und zusammen mit dem Auftragsverarbeiter geeignete Lösungen zu entwickeln, um den Schutz personenbezogener Daten zu gewährleisten.

Da dies künftige Kontrollen und Sanktionen seitens der CNIL erwarten lässt, sollten **Auftragsverarbeiter** Folgendes berücksichtigen:

- Eine Haftung des Auftragsverarbeiters ist nicht länger ausgeschlossen.
- Die Höhe des Bußgeldes richtet sich nach dem Grad der Verantwortung. Kann der für die Datenverarbeitung Verantwortliche beweisen, dass der Auftragsverarbeiter die Hauptschuld trägt, etwa weil er vertraglich vereinbarte Maßnahmen nicht umgesetzt hat, könnten Letzterem auch höhere Bußgelder drohen.
- Der Auftragsverarbeiter ist verpflichtet, dem Verantwortlichen die geeignetsten Sicherheitsmaßnahmen vorzuschlagen. Da diese Verpflichtung grundsätzlich für die gesamte Dauer der Vertragslaufzeit besteht, sollte der Auftragsverarbeiter regelmäßig überprüfen, ob es sich bei den ergriffenen Maßnahmen zum jeweils gegebenen Zeitpunkt tatsächlich noch um „die geeignetsten“ handelt.

Dass der Auftragsverarbeiter künftig haftbar gemacht werden kann, bedeutet indes nicht, dass die Haftung des Verantwortlichen dadurch gemindert oder gar ausgeschlossen ist. Der

Auftragsverarbeiter handelt nach wie vor im Auftrag und auf Weisung des Verantwortlichen, der seinerseits alle geeigneten technischen und organisatorischen Maßnahmen für ein angemessenes Schutzniveau zu treffen hat und sich darüber hinaus vergewissern muss, dass diese Maßnahmen auch umgesetzt werden.

Bezugnehmend auf die vorstehende Entscheidung der CNIL sollte der für die Datenverarbeitung **Verantwortliche** daher Folgendes beachten:

- Auch bei Zuwiderhandlung des Auftragsverarbeiters drohen dem Verantwortlichen Sanktionen.
- Um die Höhe von Bußgeldern zu minimieren, sollte der Verantwortliche nachweisen können, dass er alle erforderlichen Maßnahmen ergriffen hat (z. B. durch Vertrag) und seiner allgemeinen Überprüfungspflicht nachgekommen ist (z. B. durch regelmäßige Audits beim Auftragsverarbeiter).
- Darüber hinaus sollte er ergriffene Maßnahmen erforderlichenfalls anpassen, was insbesondere bedeuten kann, zeitnah spezifische Sicherheitsmaßnahmen zu ergreifen, um auf aktuelle Risiken zu reagieren.

Um das Risiko von Sanktionen für **beide Seiten** so gering wie möglich zu halten, empfiehlt es sich,

- die durch diese neue Haftungsteilung entstehenden rechtlichen Risiken auf vertraglichem Wege zu minimieren,
- zu dokumentieren, dass die ergriffenen Sicherheitsmaßnahmen ein dem Risiko angemessenes Schutzniveau gewährleisten, und
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zu entwickeln und diese zu dokumentieren.

12.02.2021

Qivive
Rechtsanwalts GmbH

qivive.com

Köln[D]
Konrad-Adenauer-Ufer 71
D – 50668 Köln
T + 49 (0) 221 139 96 96 - 0 F + 49 (0) 221 139 96 96 - 69
koeln@qivive.com

Paris[F]
50 avenue Marceau
F – 75008 Paris
T + 33 (0) 1 81 51 65 58 F + 33 (0) 1 81 51 65 59
paris@qivive.com

Lyon[F]
10 –12 boulevard Vivier Merle
F – 69003 Lyon
T + 33 (0) 4 27 46 51 50 F + 33 (0) 4 27 46 51 51
lyon@qivive.com