Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Berlin, 13 July 2020

631.184.2
535.1133
A56ID 109329
DD 129684
FD 135781

Final Decision

The Berlin DPA closes the case.

1. Facts concerning the data breach

- **Controller:** Xara GmbH
- **Incident**: Hacker attack on email account
- **Date of occurrence**: 16 August 2019
- **Date of acknowledgement of the incident**: 5 September 2019
- **EU/EEA Member States concerned, with the number of data subjects concerned**:
    - Establishment in Germany: 17
    - Establishment in UK: 20
    - Data subjects who are employed both in Germany and the UK (in home-office): 16

- **Category of data subjects**: Employee data
- **Category of the data types/data records concerned**: First name, surname, email-address
- **Likely consequences of the violation of the protection of personal data**: data misuse

2. Description of the data breach from a technical-organizational perspective

It is highly probable that unknown persons captured Office365 account login data via an e-mail containing modified hyper-links. Utilising this login data, they created an administrator account and gained access to the e-mail accounts of several employees. Afterwards fake e-mails were sent.

3. Description and analysis of the effectiveness of the measures taken to address the personal data breach or to mitigate its adverse effects (Art. 33 (3) (d) GDPR)

Once the activities were detected, the passwords of all accounts, including accounts with other services, were changed and a multi-factor authentication was immediately activated for accounts with access to sensitive data (including all employees in the finance department). As a further measure,

Berlin Commissioner for Data Protection and Freedom of Information

Friedrichstr. 219
10969 Berlin

Visitors' entrance:
Puttkamer Str. 16-18

The building is fully accessible to disabled members of the public.

Contact us

Phone: +49 (0)30 13889-0
Fax: +49 (0)30 215 50 50

Use our encrypted contact form for registering data protection complaints:
www.datenschutz-berlin.de/beschwerde.html

For all other enquiries, please send an e-mail to:
mailbox@privacy.de

Fingerprint of our PGP-Key:

D3C9 AEEA B403 7F96 7EF6
C77F B607 1D0F B27C 29A7

Office hours

Daily from 10 am to 3 pm,
Thursdays from 10 am to 6 pm
(or by appointment)

How to find us

The underground line U6 to Kochstraße / Bus number M29 and 248

Visit our Website

https://privacy.de

be Berlin

the introduction of multi-factor authentication for all accounts is planned. In addition, all affected workstations were subjected to a virus scan.

The technical measures are considered to be effective, since login data is much more difficult to be misused when multi-factor authentication is activated.

4. Communication to the data subjects concerned or public communication (Art. 34(1) or Art. 34(3) (c) GDPR)

All data subjects concerned were notified on 6 September 2019 via email.

5. Technical and organisational security measures that the controller had already taken when the incident occurred, e.g. encryption (Article 34 (3) (a) GDPR)

Standard Microsoft security features for Office 365, no multi-factor authentication.

6. Subsequent measures by which the controller has ensured that a high risk to the data subjects concerned is no longer likely to materialise (Article 34 (3) (b) GDPR)

As a further measure, the introduction of multi-factor authentication for all accounts is planned.

7. Intended measures by the LSA Berlin DPA

7.1 Intended measures regarding Articles 33, 34 GDPR

In the light of the above-mentioned considerations regarding Articles 33, 34 GDPR, the Berlin DPA closes the case.

7.2 Intended measures regarding data protection violations beyond Articles 33, 34 GDPR

Furthermore, the Berlin DPA has not identified any data protection violations beyond Articles 33, 34 GDPR.