Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

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

535.2128
631.326
CR 187764
DD 187943
FD 291424

Berlin, 23 April 2021

Final Decision

1. Core information on the data breach

Controller	Sandbox Interactive GmbH
Incident	In the forum of Albion Online (https://forum.albi-ononline.com), a security gap was exploited. The security gap had its origin in a forum software provided by a third party (WoltLab Burning Board). The controller was using the most current version of the software.
Time of the incident	unknown, probably also 16 October 2020
Time when the incident was known	16 October 2020, 22:51 Extortion email received
Affected EU/EEA member states	~ 293.000 affected in total. Since users only provide an email address to register and due to the high number of affected individuals, it must be assumed that all EU countries are affected.
Category of affected data subjects	Online gamers
Category of data types/records affected	Email addresses and password hash values (bcrypt)
Likely consequences of personal data breach:	Email addresses could be used to send promotional or malicious code emails

2. Description of the data breach from the technical-organizational point of view

In the forum of Albion Online (https://forum.albiononline.com), the security gap described below was exploited in a forum software of the third-party provider WoltLab Burning Board. The controller had made sure to have the latest version. The attacker/hacker tried to blackmail the provider.

The exploited security gap was a flaw in the image upload function of the software. The third-party provider's software did not effectively prevent an attacker from using the image upload function to upload code and then execute it by exploiting the security gap in the third-party software.

In this regard, the company´s layers state: "The attacker apparently managed to manipulate an image file so that he could hide an exploit kit called C99 Shell in it. The security gap in the forum software was based on the fact that files uploaded by users could be executed under certain circumstances. Our client's customizations closed this attack path. The subsequent penetration test was unable to exploit this (and possible other) vulnerabilities. It is thus clear that the current configuration of the software used is secure."

Security gaps such as buffer overflows are widespread and occur regularly even in well-maintained standard software. Once detected, these vulnerabilities are usually fixed more or less quickly by new versions or patches of the respective software.

An analysis of the attack using the available log files showed that the attacker had tried unsuccessfully to work his way into other systems. The corresponding protective measures were effective.

In this regard, the company´s lawyers state: "Our client immediately isolated the entire infected server and took it offline as soon as they became aware of the incident. Our client stored the server for investigation and prosecution purposes in the same condition as the attacker left it. Our client reverse-engineered the attack script and determined that it was a multi-encoded (via base64 encode and php eval) exploit kit called C99 Shell. The exploit kit was used by the attacker to install the Adminer database frontend, which was then used to download backups of the forum database. However, the attacker's attempts to penetrate even deeper into the systems and onto other servers of our client were prevented by further security measures already in place at the time (including IP restrictions)."

This is the first data breach report from this particular controller.

3. Description and analysis of the effectiveness of the measures taken to address the data breach or mitigate any negative consequences (Article 33 (3) (d) GDPR).

The security gap was found by analyzing the attacker's activities on the systems and closed immediately. The affected server was taken offline and new internal system passwords were assigned.

On 17 October 2020 at 14:40 o'clock the forum was restarted on a new server. The affected users were asked to change their passwords. In addition, the login had already been secured with a second factor since December 2015: When attempting to log in from a previously unused device, a code from a confirmation e-mail needs to be entered.

With the closure of the specific security gap, several penetration tests and the upcoming switch of the forum software to another provider (which is the medium-term plan) it is ruled out that the security gap can still be exploited.

4. Notification of the affected parties or public announcement (Article 34 (1) or Article 34 (3) (c) GDPR)

Data subjects were notified by e-mail on 17 October 2020. In addition, information about the attack was posted on the forum page. Users were also advised to change their passwords for other services if the same password was used there.

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

HTTPS encryption and two-factor authentication were already in place. The passwords were hashed (bcrypt).

6. Subsequent measures by which the controller has ensured that a high risk to data subjects is unlikely to persist (Art. 34 (3) (b) GDPR).

See Section 3.

7. Measures intended by the Lead Supervisory Authority (Berlin DPA)

The Berlin DPA intends to discontinue the procedure, since the data subjects were informed comprehensively and quickly and this was the first data breach notification by the controller. No negligence can be attributed to him, since the security vulnerability occurred in a third-party software in the latest version, and sufficient technical and organizational measures were taken after the security gap was discovered. It must be taken into account that a large number of data subjects are affected. However, given that only the e-mail addresses were affected, only few and no special categories of personal data are affected per data record.

The Berlin DPA