Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

631.36 / 535.525

Final Decision A60DD 67260 – Schwarzkopf-Stiftung Junges Europa; European Young Parliament

The Berlin DPA has completed the process and closed the case.

The controller immediately submitted the information required for the notification pursuant to Art. 33 GDPR, including the technical information of the hacked service provider, and has behaved very cooperatively with regard to providing all information required for processing the case.
The controller (on 14/11/2018) informed all affected parties via e-mail of the incident and the measures taken, so that Art. 34 GDPR was also complied with.

Causes of the injury

A hacker attack occurred on the member platform of the European Young Parliament, which is operated by the company CB.e AG on a contract basis. The attacker created 20 fake user accounts and published posts containing malicious code that were publicly accessible to platform users. This is how the malicious code was disseminated. The malicious code carried out a cross-site scripting attack (XSS) whenever a user displayed such a post, which essentially enabled other users' sessions to be taken over and part of their profile data being accessed (e.g. posts and comments on forum and event pages); not, however, the profile data itself, which remained accessible only to the users. In fact, it was discovered that the malicious code only caused redirects to third party websites.

Security measures taken by the data controller when the incident occurred / Specific technical and organizational measures taken by the data controller to combat data breaches

A number of software components have since been updated to current versions. Furthermore, an additional filter has been integrated to prevent cross-site scripting. All active sessions were closed and users have since been prompted to change their passwords, which must now comply with stricter rules. In addition, texts uploaded by platform users are now automatically checked; according to CB.e, manual checks of platform activity are also carried out on a regular basis. Of course, the contributions made by the 20 fake user accounts that contained the malicious code have also been removed.

Analysis of the effectiveness of these measures, particularly regarding the ability to avoid similar data breaches in future

Further XSS attacks should be effectively prevented by the user-generated content being filtered before it is published. Possibly still active user sessions that might have been taken over by the attackers have since been

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

closed. Implementing stricter password rules and prompting users to change passwords was a generally sensible security measure. It is assessed that the attacker was unable to access or change the password.
A second reported data breach comprised an unauthorized access to the e-mail inbox belonging to the e-mail account info@eyp.org using valid credentials. Fewer than 500 e-mails containing malware were sent. A connection to the first data breach was suspected by the responsible party, but this is not assessed as very likely. Instead, it is more likely that the access password for the aforementioned e-mail account was either guessed or, for example, collected using a Trojan on the client PC used for an authorized login. In my opinion, further inquiries into the cause of the breach would not yield any new findings, since the responsible party has no further information to share/provide.
According to the responsible party, in addition to changing the access password to the e-mail account, a switch to a 2-factor authentication sys-tem was implemented. In our opinion, this ensures that unauthorized ac-cess to the e-mail account is excluded in the future to a reasonable degree.