Interne Organisation - Internal Organisation - Organisation interne

Informationstechnologie- und Kommunikationsabteilung
Information and Communication Technologies Unit
Unité Technologies de l'Information et de la Communication

CI/Ge 17/05/2020

IT Incident report

The ICT Unit in the EPP Group was informed on Friday evening 15th of May of a data breach and potential data leakage of personal data belonging to EU Official, Journalists and some public affairs persons.

Below is the chronological situation :

1. A private company ShadowMap based in India, that claims to be a digital risk management platform, informed the EP via Twitter, on Friday 15th of May 2020 in the afternoon, of a potential data breach of an **EU database**.

2. At **14:31pm** this company succeeded to access an outdated EPP Group database backup exposed on an external subcontractor server. It was accessed, afterwards, by EP security, EPP IT and the subcontractor company that removed the link at **22:35 on the same day**.

3. The database contains **email addresses** and mainly **public data** from 1st of August **2018**. (Annex 1) The only sensitive information were the **passwords** linked to the account needed to setup the preferences for our former newsletters platform. The passwords were **encrypted** and **salted individually.** This means that they were very strongly protected. They were indeed double protected, and it looks very unlikely that IT experts could decipher it.

4. We can ensure that, except this company, nobody else copied this backup database before. (Annex 2) However we do not know the real intention of this company or if they have forwarded the database to someone else. Probably they just wanted to promote their security services as they used Twitter to announce the exposed file. In any case, they could not do anything malicious with this data.

5. This incident does not have any consequence on our IT Systems or EP IT Systems, as there is absolutely no link between these data backup and other information systems.

   In the meantime, we have audited our Internet Servers with regards for potential threats, the results were negative.
   In others words, there has been no hacking of our servers. I would also like to inform you that our Internet Servers are attacked almost **on a daily basis** and we are monitoring these attacks constantly.

   We have informed the **Data Protection Officer** of the EP of this potential leak Saturday 16th of May 2020 in the Morning.

The EP CISO (**Chief Information Security Officer**) has informed others EU Institutions of this potential leak and the EU-CERT (Computer Emergency Response Team) on Saturday 16th of May 2020.

We have informed the **European Data Protection Supervisor** (EDPS) Monday 18 of May 2020

We have informed **all the users** impacted on Saturday 16th of May 2020 evening by a short statement email about "Important communication regarding your email address"

Figures:

The database had **16 715** entries in total,

We think this data breach concerned finally no more than **8 500** subscribers or email addresses that we can identify, as shown below:

393 **EPP MEPs** or former EPP MEPs

493 **EPP Staff** members or former Staff members

1303 Users of EU Institutions

- **1070** from EP
- **91** from the EC
- **10** from the Council

4526 Journalists or members of our Press service

Total identified: **6715**

In a total **16 715 entries** we estimate that a minimum of **8 000** entries are bulk or spam emails addresses, but it is difficult to have the exact number. We have **5790** who never connected, therefore who did not had entered **any password**.
Consequently, the potential leak of encrypted passwords concerns **2925** email addresses.

Annexe 1: What kind of data is inside this database?

USER Table - Common to Registered users, Newsletter users, Staff and MEPs	
Some of the fields were only filled in for certain categories of users.	
User first name	
User last name	
Email address	
Created by press officer	Was the contact entered by a press officer (eg: Distribution Lists)

User digest preferences	Newsletter Settings & Preferences
User digest special product	Newsletter Settings & Preferences
User pr preferences	Newsletter Settings & Preferences
User pr country preferences	Newsletter Settings & Preferences
User pr mep references	Newsletter Settings & Preferences
No substitution	
Is closed	
Is former	
has_unsubscribe	
twitter handle	
User country topic usage	Topics Staff can maintain
Only country level	If Staff is only allowed to post in his country
User contact	
Other allowed languages	Language Staff can post in
Responsible for	EP Bodies Staff can write to
Country	Country Staff is allowed to post to
MEP contact	Unused
Staff contact	Unused
User preferences	Unused
Titre	Title
Political body	Commission, delegation other bodies Staff is attached to
Precedence in main service	
Website	
Contact	Office Number & phone in STR+BXL + Fax + Mobile
Biography	
Is substitute	
Service	Service/Unit in the EPP Group
Nationality	
MEP Profile	Link to Mep profile on the website
I'm a member of the press	
Staff Picture	
Managed Topics	
Is Publishable	
User Organisation Name	
User Organisation Role	
User Organisation Type	
User news digest sending rate	

Why do we own this data?

1. **For EPP Members and Staff (5.3 % of the database)**

The maximum data fields were 44**.**
They only concerned EPP MEPs and EPP Staff on official information like Office numbers in Strasbourg and Brussels, phone numbers we could totally or partially display on our Internet website.

2. **For others subscribers (94,7 % of the database)**

The maximum data fields were in most cases no more than 7. (email address, encrypted password, first name, last name, organisation name, nationality and preferences).
The purpose was to send EPP Group newsletters to all these subscribers

Why was this backup was on a third party server ?

We were working with the Company Actency under a framework contract.

We exported the contents of this database to ACTENCY in order to run local tests on their premises, and to prepare the data migration for our new website launched in October 2018.

It is clear that this backup file should have never been exposed on Internet even if it was protected with a password.

Annexe 2: Who accessed this database ?

After analysing the logs file below nobody access this file between 7th of August 2018 and 15th of May 13:44 the link was removed at 22:35.

Date access	Description name	name lookup
07/Aug/2018:15:33:06		COMPLETEL SAS
15/May/2020:13:44:42		Reliance JIO INFOCOMM LTD GHANSOLI INDIA
15/May/2020:17:23:57		DigitalOcean, LLC
15/May/2020:19:20:35		Bukal Marek
15/May/2020:20:20:02		Telenet Operaties N.V.
15/May/2020:20:55:47	European Parliament - DG ITEC Cellule Marches	European Parliament - DG ITEC Cellule Marches
15/May/2020:21:01:37	European Parliament - DG ITEC Cellule Marches	European Parliament - DG ITEC Cellule Marches

15/May/2020:21:04:46		KOUTROUMPAS CHRISTOS
15/May/2020:21:07:13	EPP IT	Telenet Operaties N.V.
15/May/2020:21:09:59		Google LLC
15/May/2020:21:05:31	EPP IT	Scarlet Belgium NV
15/May/2020:21:47:11	European Parliament - EP Network operations	European Parliament - EP Network operations
15/May/2020:21:48:24		Proximus SA de droit public (Sébastien Jauquet)
15/May/2020:22:31:25	Giovanni Dacheux (Actency)	
15/May/2020:22:40:01		Paul RETTER
15/May/2020:22:35:38	Fatima Bahaoui (Actency)	
15/May/2020:22:37:45	Léo Prada (Actency)	SFR Tech Contact (formerly Neuf Cegetel / LDCOM Networks)

What are the risks ?

Regarding the fact that we have 50% of the database as junk email adresses, the only real sensitive data is the encrypted password.

We evaluate that **2925** real **encrypted passwords** could have potentially leaked.

Keeping in mind that this data is from August 2018 and that modern system impose to change regularly passwords, serious consequences should be very limited as we informed all the users immediately.

Cédric IVRY
Head of Unit