The ICO exists to empower you through information.

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113
ico.org.uk

DATA PROTECTION ACT 2018 AND UK GENERAL DATA PROTECTION REGULATION

REPRIMAND

To: The Electoral Commission

Of: 3 Bunhill Row, London, EC1Y 8YZ

The Information Commissioner (the Commissioner) issues a reprimand to The Electoral Commission in accordance with Article 58(2)(b) of the UK General Data Protection Regulation in respect of certain infringements of the UK GDPR.

1. Summary of Incident

1.1 The Electoral Commission is the independent body which oversees elections and regulates political finance in the UK. They also work to promote public confidence in the democratic process and ensure its integrity.

1.2 It is the Commissioner's understanding that unknown Threat Actors gained unauthorised access to The Electoral Commission's on-premise Microsoft Exchange Server ([redacted]) via the ProxyShell vulnerability chain.

1.3 The personal data affected by this incident relates mainly to the Electoral Register, which contains the names and home addresses for approximately 40,000,000 data subjects.

1.4 During the course of this incident, three separate clusters of Threat Actor activity were identified. [redacted] investigated Clusters one and two, and [redacted] investigated Cluster three. A summary of each Cluster is below.

2. <u>Cluster 1</u>

2.1 On 24 August 2021, an unknown Threat Actor gained access to an on-premise Microsoft Exchange Server 2016 via the ProxyShell vulnerability chain. The vulnerability chain consisted of the following vulnerabilities: CVE-2021-31207, CVE-2021-34523 and CVE-2021-34473. A user account was impersonated during the exploitation of these vulnerabilities, which led to web shells being created on the system.

2.2 One of these web shells ([redacted]) persisted on the system and was accessed on 16 September 2021, 13 June 2022 and 02 August 2022. From

14 March 2022, backdoors in the form of [redacted] were also installed on the system.

3. Cluster 2

3.1 On 03 October 2021, a second Threat Actor successfully exploited the ProxyShell vulnerabilities and deployed a web shell to the server. This web shell was quarantined and deleted by [redacted]

3.2 On 14 March 2022, a scheduled task was created on server [redacted] were unable to determine whether the Threat Actor retained access to the Exchange Server or if they re-compromised it in March 2022. The scheduled task was configured to download and execute a [redacted] payload, the IP address for these actions was the same as the one used in October 2021.

3.3 The last observed threat activity occurred via a connection from a host to [redacted]. [redacted] did not identify any follow-on activity associated with this [redacted] malware.

4. Cluster 3

4.1 On 28 October 2021, an alert was raised when an employee reported that spam emails were being sent from The Electoral Commission's Exchange Server. Emails from the sent items queue in Exchange Server were being sent from the server, but were not in the individual's visible sent items in Outlook. A [redacted] scan was carried out on the on-premise Exchange Server which showed that it had been injected with malware ([redacted]).

4.2 Following this, the Exchange Server was shut down and scrubbed using [redacted], before being restarted. A new scan showed that the virus had been removed. At this stage, [redacted] were engaged to support initial remediation and carry out a penetration test.

4.3 The Electoral Commission also advised the National Cyber Security Centre (NCSC) about this incident. The NCSC raised concerns about the incident being similar to activity which was discussed in a Microsoft blog in March 2021. The NCSC strongly recommended that a wider investigation into The Electoral Commission's IT systems should be carried out by a CIR accredited company. At the time, The Electoral Commission considered that the incident was isolated and as they were moving closer to migration to the Cloud, remedial action with

the old servers was limited. The Electoral Commission stated that they were aware of the problems with out-of-date infrastructure.

5. The reprimand

5.1 The Commissioner has decided to issue a reprimand to The Electoral Commission in respect of the following alleged infringements of the UK GDPR:

- Article 5(1)(f) which states that personal data shall be *"Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures"*

  Article 32(1)(b) which states *"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*

  b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services."

5.2 The reasons for the Commissioner's findings are set out below.

5.3 Our investigation found infringements in relation to the security requirements of the UK GDPR and these are set out below.

6. Article 5 (1) (f)

- The Electoral Commission were not ensuring the security of personal data as per Article 5(1)(f).

6.1 The Electoral Commission did not have an appropriate patching regime in place at the time of the incident. This led to a number of vulnerabilities being present on their on-premise Exchange Server. The ProxyShell vulnerability

chain was utilised on several occasions during this incident and the patches[1] for these vulnerabilities were released in April and May 2021.

6.2 Furthermore, a report produced during this incident highlighted a further eight vulnerabilities which were also present on the servers. Although not utilised on this occasion, any one of them could have been exploited by a Threat Actor whilst they existed on the relevant systems.

6.3 The NCSC[2] and NIST[3] have both produced extensive guidance on patching which highlight the importance of having an appropriate patching plan in place as well as the actions organisations can take.

6.4 This failing is a basic measure that we would expect to see implemented in any organisation processing personal data – regardless of potential severity of risk or size of organisation.

7. Article 32 (1) (b)

- The Electoral Commission were not ensuring the ongoing confidentiality of its processing systems as per Article 32(1)(b).

7.1 The Electoral Commission did not have appropriate password management policies in place at the time of the incident. During the Electoral Commission's investigation, they discovered that one of the compromised accounts was still using a password which was allocated to the account upon creation. Following this, [redacted] were instructed to perform an audit of user passwords in The Electoral Commission's Active Directory.

7.2 [redacted] were able to rapidly crack 178 active accounts using passwords identical or similar to the ones provided to users by the Service Desk upon account creation or password reset. An additional 33 deactivated accounts with similar password were also found. Following their audit, [redacted] stated that this practice of reusing passwords makes The Electoral Commission's passwords highly susceptible to password guessing.

7.3 The Electoral Commission did not have a dedicated password management policy in place at the time of the incident. The policy (Acceptable Use) which was in place did not contain any specific password management guidance, the only reference to passwords stated 'do not reveal or write down passwords'.

7.4 The NCSC[4] and NIST[5] have produced guidance on passwords which

[1] Description of the security update for Microsoft Exchange Server 2019, 2016, and 2013: April 13, 2021 (KB5001779) - Microsoft Support
[2] The problems with patching - NCSC.GOV.UK
[3] Guide to Enterprise Patch Management Technologies (nist.gov)
[4] password_policy_infographic.pdf
[5] NIST Special Publication 800-63B

highlight the importance of staff training as well as password length and other mitigations like rate limiting.

7.5 This failing is a basic measure that we would expect to see implemented in any organisation processing personal data – regardless of potential severity of risk or size of organisation.

8. Remedial steps taken by The Electoral Commission

8.1 The Commissioner has also considered and welcomes the remedial steps taken by The Electoral Commission in the light of this incident. In particular:

- Implemented a Technology Modernisation Plan;
- Onboarded [redacted] to provide a Managed Infrastructure Support Service;
- Implemented [redacted] which monitors all servers, firewalls and internet traffic;
- Implemented [redacted] solution which supports Threat and Vulnerability programs;
- Implemented password policy controls within their Active Directory;
- Implemented Multi-factor authentication (MFA) for all users.

9. Decision to issue a reprimand

9.1 Taking into account the circumstances of this case, including the remedial steps, the Commissioner has decided to issue a reprimand to The Electoral Commission in relation to the infringements of Articles 5(1)(f) and 32(1)(b) of the UK GDPR set out above.[6]

[6] The Electoral Commission has had an opportunity to make representations to the Commissioner in response to the Notice of Intent regarding this reprimand. The Electoral Commission accepted the Notice of Intent and the Commissioner's findings.