Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

Welsh Language Commissioner
Market Chambers
5-7 St Mary Street
Cardiff
CF10 1AT

By email only to: [redacted]

18 January 2022

Dear [redacted]

Case Reference Number: INV/0001/2021

I write to inform you that the Information Commissioner's Office ('**ICO**') has now completed the investigation into the personal data breach reported by the Welsh Language Commissioner ("WLC").

Based on my assessment and the information provided, the ICO have decided to issue the WLC with a reprimand in accordance with Article 58(2)(b) of the General Data Protection Regulation ('**GDPR**'). The specific terms of the reprimand can be found towards the end of this letter.

In summary, it is our understanding that:

- The threat actor gained initial access to the WLC's systems via a phishing email which contained a malware attachment.

- The threat actor compromised a legitimate Active Directory account called '[redacted]. This account is a privileged account which was created by IT officers so they could manipulate, handle, and configure the activities of [redacted] on the local network. Following an investigation by [redacted] the method by which the [redacted] account was compromised is unknown.

- The threat actor deployed Makop ransomware to encrypt any data files on the WLC's systems. The ransomware successfully encrypted all of WLC's systems including the backups and all automatic and manual snapshots of files created by the system ('Shadow Copies') were deliberately deleted as well. As a result of this, the WLC permanently lost all their data as there was no viable backup solution.

- The threat actor provided examples of stolen data, with the claim that the rest of the corporate data was also exfiltrated. However, following an investigation, there was insufficient evidence to determine whether the attackers' claims were accurate. The Police carried out a search of the dark web and found no evidence of data being published.

Our consideration of this case

This case has been considered under the GDPR due to the nature of the processing involved.

For more information about our powers under the data protection legislation please see the attacked leaflet.

- ICO Enforcement Leaflet – GDPR and DPA 2018.

We have investigated whether the WLC has complied with the requirements of data protection legislation. In the course of our investigation, we have noted that:

- The backups which were encrypted as part of this incident were limited to a single location which was accessible from the main network. NCSC guidance[1] states that offline backups should 'only connect to live systems when absolutely necessary' and organisations should use multiple backups which are logically separated. By ensuring multiple backups are available, and not all of these backups are available from the main systems at any one time, this mitigates the risk of local incidents such as ransomware affecting all an organisation's backups.

- The WLC failed to follow best practice in regard to backups, including the above guidance, by not utilising multiple backups and allowing access to their backups from their main systems. This enabled the ransomware to affect their backups and it prevented the WLC from recovering impacted data, aggravating the loss of accessibility to personal data in the incident as the WLC had to rebuild their systems and data from scratch. Due to the failure to follow industry standards in regard to backups, leading to an inability to recover personal data impacted by the incident, the ICO have determined that the WLC failed to comply with Articles 5.1(f) and 32 of the

[1] Offline backups in an online world - NCSC.GOV.UK

GDPR which require appropriate technical and organisational measures to be in place to protect personal data.

- Following an investigation by [redacted], it was discovered that the security posture of the affected machines was critical as they were operating on end-of-life [redacted] infrastructure which has been without security updates for 12 months. The systems were also operating outdated and known vulnerable versions of [redacted] from 2017 and, in some cases, earlier. The WLC also confirmed that there was no written patching policy in place at the time of the incident.

- There are many industry standards regarding patch management, for example from NIST[2] where it is stated that "From a security perspective, patches are most often of interest because they are mitigating software flaw vulnerabilities; applying patches to eliminate these vulnerabilities significantly reduces the opportunities for exploitation. Patches serve other purposes than just fixing software flaws; they can also add new features to software and firmware, including security capabilities" and the NCSC, whose guidance on protecting against malware such as ransomware states "Applying these updates (a process known as patching) is one of the most important things you can do to improve security" and "At some point, these updates will no longer be available (as the product reaches the end of its supported life), at which point you should consider replacing it with a modern alternative"[3].

- In failing to keep systems updated and failing to consider implementing a written patching policy to ensure software remained up-to-date and secure, the WLC fell short of industry standards in a fundamental aspect of enterprise cyber security. Therefore, the ICO have determined that the WLC failed to comply with Article 5.1(f) and Article 32 of the GDPR in regard to their patch management.

- [redacted] also stated that logging/auditing was switched off on almost all machines on the network. However, this was later corrected by the WLC who stated that at the time of the attack logging/auditing was in place on all desktop computers and servers. As one of the actions taken by the

[2] Guide to Enterprise Patch Management Technologies (nist.gov)
[3] Step 2 - Protecting your organisation from malware - NCSC.GOV.UK

attacker, logging/auditing on the infected equipment appears to have been switched off. The NCSC provide guidance on designing monitoring systems[4]. A section of this guidance states that "Protect your logs from tampering so that it is hard for an attacker to hide their tracks and you can be confident that they accurately represent what has happened".

- Whilst logging was in place, the ability for the attacker to tamper with the logging systems suggests a failure to properly protect these systems from the attack. Therefore, the ICO has also considered the lack of logs available post-incident in its decision making.

We have also considered and welcome the remedial steps taken by the WLC in light of the incident, including the migration of your infrastructure to [redacted] cloud, the implementation of technical measures to ensure software automatically updates and Multi-Factor Authentication has been deployed for all system users.

Having considered the above, we have determined that the WLC has not complied with the requirements of Article 5.1(f) and Article 32 in relation to this incident. These articles require personal data be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised disclosure or unlawful destruction, loss, or alteration using appropriate technical or organisational measures.

Therefore, after careful consideration and based on the information provided, we have decided to issue the WLC with a reprimand in accordance with Article 58 of the GDPR.

Details of reprimand

The reprimand has been issued in respect of the following processing operations that have infringed on the requirements of the GDPR:

- Processing personal data in non-compliance of the requirements set out in Article 5.1(f) and Article 32.

Further Action Recommended

The Commissioner recommends that the WLC could take certain steps to improve compliance with the GDPR. In particular:

[4] Logging and monitoring - NCSC.GOV.UK

- During the course of the investigation a number of remedial measures have been discussed to prevent a reoccurrence of the incident. We expect these remedial measures to be implemented, where they haven't already.

- In addition to our above recommendation on remedial measures, we suggest that specific consideration is made to your backup solution. As we note that this area is still under development, the ICO strongly recommends the WLC ensures that a suitable backup solution is implemented in line with industry guidance.

- Following the incidents effects on your logging/auditing systems, the ICO recommend that you review your logging and monitoring systems, including any measures in place to secure such systems, to ensure they are in line with industry guidance.

Whilst the above measures are suggestions, I would like to point out that if further information relating to this subject comes to light, or if any further incidents or complaints are reported to us, we will revisit this matter and further formal regulatory action may be considered as a result.

Further information about compliance with the data protection legislation which is relevant to this case can be found at the following link:

https://ico.org.uk/for-organisations/guide-to-data-protection/

We actively publicise our regulatory activity and outcomes, as this helps us to achieve our strategic aims in upholding information rights in the public interest. We may publish information about cases reported to us, for example where we think there is an opportunity for other organisations to learn or where the case highlights a risk or novel issue.

Therefore, we may publish the outcome of this investigation to publicise our regulatory authority and new powers under the GDPR. We will publish information in accordance with our Communicating Regulatory and Enforcement Activity Policy, which is available online at the following link:

https://ico.org.uk/media/about-the-ico/policiesandprocedures/1890/ico_enforcement_communications_policy.pdf

Please let us know if you have any concerns about this.

Thank you for your co-operation and assistance during the course of our investigation.

We now consider the matter closed.

Yours sincerely

[redacted]
Lead Technical Investigations Officer
Information Commissioner's Office
[redacted]