Thursday Thoughts – 1st July 2021

This week we can actually say that the "adequacy" decision is made! With effect the 28th June the UK ICO announced that the UK has granted adequacy by the European Commission. The UK also have a Telecommunications (Security) Bill making it's way through the House of Lords which hopefully will make our telecommunications providers, their networks and supply chains more secure. In Germany an investigation of media outlet websites found their cookie consents were "mostly invalid" This is likely to have repercussions for UK businesses as I think it's only a matter of time before this level of scrutiny comes to the UK.

This week it seems like every platform needs updating, the "software updates and warnings" section is brimming with information on issues with Edge, Windows, Microsoft, Dell and Adobe to name a few. There are also a wide variety of GDPR fines for inappropriate use of CCTV, accessing an ex-employee's email account, data breaches, buying in marketing lists, not getting permission to contact the data subject and making recordings on public busses, oh and the PECR fine in UK for making more than 11 million unlawful claims management calls.

Blogs/Podcasts of the Week

NCSC - Data Protection Training for Small Organisations and Charities
Databasix UK Ltd - The Data Rockstar's Coffee Podcast - Data Breaches Exposed on Social Networks

UK Adequacy Decision

After EU member states voted unanimously in favour of the UK obtaining an adequacy decision we had confirmation on 28th of June 2021 from the UK ICO that the UK has been granted adequacy by the European Commission. You can read more from the ICO here: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/06/ico-statement-in-response-to-the-eu-commission-s-announcement-on-the-approval-of-the-uk-s-adequacy/

UK Telecommunications (Security) Bill Reaches Committee Stage

The UK's Telecommunications (Security) Bill which will "introduce a new security framework to ensure that telecommunications providers operate secure and resilient networks and manage their supply chains appropriately" has passed the second reading in the House of Lords. It will now go through the committee stage before going back for it's final reading.

German Data Protection Authority Ruling on Cookie Consent

The Data Protection Authority in Saxony (Germany) has published the results of an investigation into Cookie consent. The investigation looked at the websites of several media companies from mid-August 2020 and have determined that the consents on those

websites are “mostly invalid and that the media companies examined must make improvements”. The main points of criticism are:

- Cookies are set first and then consent is asked for
- Insufficient or incorrect information is given about user tracking
- Scope of consent is insufficient
- There is no way to simply reject user tracking
- Users are manipulated into decisions (nudging).

Software Updates and Warnings

Microsoft Tricked Into Signing a Driver Loaded With Malware

Microsoft are investigating an incident where one of their signed drivers turned out to be malicious and was communicating with servers located in China. This is an example where signed drivers can be exploited to facilitate a large-scale software supply chain attack. In this case the driver ("Netfilter") is said to target gaming environments. As a result Microsoft said it intends to refine its partner access policies as well as its validation and signing process to enhance protections**.**

Microsoft Edge Update

Last week Microsoft produced updates for the Edge browser to fix 2 security issues. The attack exploits client-side vulnerabilities in browser or browser extensions in order to execute malicious code which can bypass or disable the security features. There was code within the translation feature that failed to sanitize input meaning that malicious code could be activated when a user clicks the translate button. In “Proof of concept” it was demonstrated that an attack could be triggered by adding a comment to a YouTube video and a second by sending a friend request from a Facebook profile. All that is required is for the material to be written in a language other than English. The latest Edge update (version 91.0.864.59) can be downloaded by visiting Settings on your Microsoft Edge.

Microsoft Windows Updates

It’s nearly time for July’s “Patch Tuesday” so here’s a reminder of the flaws that were patched my Microsoft in June. 50 vulnerabilities in Microsoft Windows, .NET Core and Visual Studio, Microsoft Office, Microsoft Edge (Chromium-based and Edge), SharePoint Server, Hyper-V, Visual Studio Code - Kubernetes Tools, Windows HTML Platform, and Windows Remote Desktop were patched.

Microsoft also fixed vulnerabilities in Paint 3D, Microsoft SharePoint Server, Microsoft Outlook, Microsoft Office Graphics, Microsoft Intune Management Extension, Microsoft Excel, Microsoft Defender, Windows Filter Manager, Windows Kernel, Windows Kernel-Mode Driver, Windows NTLM Elevation, and Windows Print Spooler. News has also emerged if vulnerabilities in affecting NETGEAR DGN2200v1 series routers.

If you haven’t done so already you can install the latest security updates via your Start button.

Dell PC and Tablet BIOS Disconnect

A "chain of vulnerabilities" affecting the Dell BIOS Connect feature have been identified which could be used to "subvert the operating system and undermine fundamental trust in the device. The flaws affect 128 Dell models (laptops, desktops, and tablets) and accounts for an estimated 30 million devices. The issue was reported to Dell in March and Dell have since released updates and workarounds to remediate the issue. If you have a Dell it is worth checking with your IT specialist that your system is up to date/unaffected.

Software Patches From Other Vendors

A number of other vendors have also released patches last month including Adobe, Android, Dell, Intel, Linux distributions SUSE, Oracle Linux, and Red Hat, SAP, Schneider Electric, and Siemens. You will find links to all these patches here: https://thehackernews.com/2021/06/update-your-windows-computers-to-patch.html

Cyberattacks target the video game industry

Cyberattacks which target the video game industry spiralled during the pandemic. Reports suggest there were more than 240 million web application attacks in 2020, a 340% increase over 2019.

Fines

ICO fines Brazier Consulting Services Ltd (BCS) £200,000

The Information Commissioner's Office fined Brazier Consulting Services Ltd (BCS) £200,000 under PECR for making more than 11 million unlawful claims management calls. The company did not provide evidence that it had consent to contact the complainants and there was no evidence that staff had received any training in relation to the Privacy and Electronic Communications Regulations. The ICO also issued the company with an Enforcement Notice compelling them to stop their illegal marketing activity and informing them that failure to do is a criminal offence.

Icelandic DPA fines Huppuís ehf €34,000

Huppuís ehf were fined €34,000 by the Icelandic DPA because employees (mostly minors) had to change in the general employee area, which was covered by a video camera rather than the designated changing area which insufficiently large for the purpose and was being used to store products.

The Lithuanian DPA (VDAI) issue a €8,000 fine

The Lithuanian DPA (VDAI) fined a company € 8,000 for making sound recordings on public transport buses.

The Norwegian DPA fined the municipality of Moss €49,200 for a data breach

The municipality of Moss was fined €49,200 for a data breach involving the data of 2000 people which resulted in errors in vaccine registration and follow-ups for pregnant women. Undocumented access to patient information was provided to health workers when it was not required.

Italian DPA fines Iren Mercato S.p.A. €2,856,169

The Italian Garante fined Iren Mercato S.p.A. €2,856,169 for "failing to verify that all transfers of data of recipients of promotional activities were covered by consent". Data subjects therefore received unsolicited advertising. It emerged that the controller was processing data it had acquired from other sources and had not checked that valid consents were in place.

Norwegian DPA imposes a fine of € 14,800 for accessing an ex employee's inbox

The Norwegian DPA fined a company €14,800 after the company's managing director logged into an ex-employees email inbox on a daily basis for a period of six weeks. The DPA found there was insufficient legal basis for this access and that the controller had breached its information obligations and its obligation to delete the contents of the ex-employees e-mail account.

Blogs/Podcast of the Week

NCSC - Data Protection Training for Small Organisations and Charities

If you haven't found this yet the NCSC have issued some free online training for small organisations and charities. The training package is available on the NCSC website or you can download it in a zip file. It will guide you through what you need to do to reduce the likelihood of your organisation becoming a victim of a cyber-attack covering the following areas:

- Backing up your organisation's data correctly
- Protecting your organisation against malware
- Keeping the devices used by your employees secure
- The importance of creating strong passwords
- Defending your organisation against phishing

You will find the package here https://www.ncsc.gov.uk/blog-post/training-for-small-organisations-and-charities-now-available .

Databasix UK Ltd - The Data Rockstar's Coffee Podcast - Data Breaches Exposed on Social Networks

For the second week running Data Rockstar's Coffee podcast gets a mention for it's discussion on "that CCTV video" (yes the one featuring Matt Handcock). A great exploration of both sides of the argument and the balance between public interest and the expectation that your employer should protect your personal data. Also included a story from twitter of a Solicitors firm leaving documents in the street for disposal – why would you do that!! Again an interesting listen:
https://podcasts.google.com/feed/aHR0cHM6Ly9mZWVkLnBvZGJlYW4uY29tL2RieHVrL2ZlZWQueG1s/episode/ZGJ4dWsucG9kYmVhbi5jb20vZjZhODYwODMtMTFlOC0zMTUwLWI0NzgtNjQxYzEzNDFkMjcz?sa=X&ved=0CAUQkfYCahcKEwiAjpKb9MHxAhUAAAAAHQAAAAAQHw&hl=en-GB