THURSDAY THOUGHTS

Wow - this is edition 40 of Thursday Thoughts, how did that happen. This week there is a heavy focus on Apps and privacy. I was shocked to hear that companies in the US hold location data on European residents even though they have not been in the US. You can read about how a Norwegian Journalist found that an app he downloaded was shared with the company who supplies data to US Enforcement agencies. Also making the news are some high-profile Android Apps that are still not patched, and patches you should install on your Oracle Server.

Sticking with the social media theme, the latest Facebook marketplace scam features offers which sound too good to be true. My article contains a warning to be on your guard especially if you are asked to pay in pre-pay eBay cards. I found a really great video this week from Gabriel Friedlander which explained in simple terms how you can unintentionally become a direct target of a cyber-attack.

Neil Evans produced a great summary of Fines and Sanctions which I have added to. There is also some information on what Microsoft 365's "shared responsibility model" means for you as a business owner. This week has seen the Online PrivSec Global conference which featured over 200 speakers and more than 90 sessions which covered the most pressing and challenging topics in the data protection, privacy and security industry. I'll feature that next week when I have digested the content. Also this week the BSI Healthcare Webinar video was released which showed interesting statistics on what is of concern to healthcare organisations at the moment.

My "Blogs of the Week"
My Life Digital – The Importance Of Linking Consent Management With Customer Identity Management
RM Girl (Emily Overton) - Managing your HR Personnel Records effectively

Why We Should Take Time Installing Apps

Many of our apps are spying on us or at the very least tracking where we are all the time. The worrying thing is that this information, yes even that we are shopping, having a drink, or socialising, is attractive and is something that companies buy and sell. In order to look into this, Martin Gundersen a Journalist in Oslo started an experiment in February. He installed lots of apps on a spare phone which he then carried everywhere.

Martin knew that U.S. Immigration and Customs Enforcement (ICE) often use commercially available location data. So, in August he made a Subject Access Request to a company that had previously supplied ICE with information (Venntel). What he uncovered is quite shocking. The email attachment from Venntel showed where he had been 75,406 times since 15 February – he was able to retrace his every step.

His data had been shared through these apps with Venntel by their parent company a Data Broker (Gravy Analytics). But it makes you ask how a European resident's location data could end up in the

US when none of the apps mentioned this and he had not set foot outside Norway. More worrying too is that Venntel had shared the information with it's "customers" which could mean it was used for federal law enforcement and national security. You can read the full article here: https://nrkbeta.no/2020/12/03/my-phone-was-spying-on-me-so-i-tracked-down-the-surveillants/

Is Your Android App Unpatched

If you use any of the following apps on Android then you could be at risk of hacking because the App developer has not yet integrated the new Play Core library into their app. Even though Google did this in march. The at risk apps include:

Grindr	Bumble	OkCupid	Cisco Teams
Moovit	Yango Pro	Microsoft Edge	Xrecorder
PowerDirector			

You can read more here: https://thehackernews.com/2020/12/several-unpatched-popular-android-apps.html

If It Sounds too Good To Be True – There Will be a Catch

Chris Roberts shared a "Too Good to be True" story on Linked In – it featured a "Horse trailer for sale" (on Facebook) which "moved" to eBay. This could be any item so watch out. There was a sob story attached that the owner was TOO busy to deal with it, so they handed it to their finance person to deal. So if you see an all-time good deal and are presented with an "eBay issued invoice" which asks you to pay in pre-pay eBay cards. DON'T DO IT! Especially not if you are asked to take pictures and send them. Instead ask someone you trust for advice and in Chris' words "Please don't get scammed!"

Facebook Marketplace seems to be full of these ads at the moment. So keep safe. The tell-tale signs are when you see a number of accounts offering the same item. If this is combined with a goofy Facebook account name and the account has only been alive for a short time steer well clear.

Why Would Anyone Want To Hack Me

On a linked in post this week Gabriel Friedlander shared a Wizer video which explained in simple terms (in 1-minute) how you can unintentionally become a direct target of a cyber-attack. You will find the video on Gabriel's linked in feed. There are also many such free videos and guides on the Wizer website https://wizer-training.com

BSI Healthcare Webinar

Last week the BSI held a webinar entitled "Information Resilience in the cloud - a healthcare imperative". In preparation for the webinar BSI conducted a poll which identified:

- 57% were prioritizing security risk assessments (a result of the WannaCry outbreak).
- 50% were concerned about data breaches
- 37% were mitigating or remediating known gaps in their security
- 31% are working on cloud solutions
- 29% had some form of remote working

- 20% were concerned about sanctions and meeting regulations.

You can listen to the Webinar here: https://page.bsigroup.com/l/73472/2020-11-26/xcv8bg

Unpatched Oracle Servers

If you have yet to patch your Oracle servers or missed the October 2020 Critical Patch Update or the November (CVE-2020-14750). You should get it done as soon as possible. According to Hacker News there are still about 3,000 Oracle WebLogic servers that can be seen as unpatched on the Internet. These servers are a "lucrative target for threat actors" who turn them into a botnet that steals critical data and deploys malware. The botnet spreads across the network, downloading files, record keystrokes, and stealing credentials. It also acts as a "Bitcoin clipper" changing the user's bitcoin wallet address and rerouting transactions. You can read more here: https://thehackernews.com/2020/12/multiple-botnets-exploiting-critical.html

Microsoft 365 – Not as Protected As Some Think

Microsoft 365 is a very popular choice for businesses. But you may be unaware that their "shared responsibility model" means that it is your responsibility to actually secure your organization's data. Microsoft's role stops at protecting the infrastructure and keeping the systems up and available.

This means they do not offer a "long-term retention" or "point-in-time restore" capability and you will find that the recycle bin is cleared after 90 days with no way to recover data once it's gone. Similarly, you can only restore a deleted mailbox in the first 30 days.

To protect your data from a non-Microsoft software failure (ransomware, human error, intentional deletion etc.) you will need a data protection strategy. This will include looking at a Third-party data protection/backup solution so that you can restore data quickly. You can read more here: https://info.arcserve.com/blog/taking-the-mystery-out-of-protecting-microsoft-365-data?utm_campaign=Don%E2%80%99t%20Get%20Caught%20Assuming%3A%20How%20to%20Protect%20Microsoft%20Office%20365%20Data&utm_content=146364521&utm_medium=social&utm_source=linkedin&hss_channel=lcp-5251515

Fines and Sanctions

Lack of transparency when capturing consent

Here are some fines you may have missed in the news - they all share a common theme of lack of transparency when capturing consent to process data for marketing purposes:

- Facebook fined $6.1 Million in South Korea
- Carrefour fined just over €2Million by the French Supervisory Authority
- Vodafone Italy fined just over €12.25 Million by the Italian Supervisory Authority
- The UK ICO audit of the UK Political Parties
- The UK ICO take Enforcement against Data Brokers

These link to one of my blogs of the week "The Importance Of Linking Consent Management With Customer Identity Management"

Fake Call Centres

An Indian national was sent to prison for 20 years in the United States for operating fake Call Centres that defrauded U.S. victims out of millions of dollars and was ordered to pay restitution of $8,970,396 to victims.

The Right to be Forgotten

The Italian Garante have rejected Google's claim that there were no conditions for the exercise of the Right to be Forgotten and ordered it to proceed to the de-referencing of some articles. The authority stated that the prejudice to Google's reputation from making the articles available online was not counterbalanced by any public interest.

Guidance on Data Protection Impact Assessments for Digital Advertising

The Interactive Advertising Bureau are a European association for digital marketing and advertising. They have recently produced guidance on how to conduct a DPIA with respect to digital advertising. The aim is to explain how to incorporate the DPIA process into a company's normal course of product design and development. You will find the guide here: https://iabeurope.eu/knowledge-hub/guide-gdpr-data-protection-impact-assessments-dpia-for-digital-advertising-under-gdpr/

Blogs of The Week

My Life Digital – The Importance Of Linking Consent Management With Customer Identity Management

This blog by J Cromack and Aaron Provis discusses how the old regime of pre-ticked checkboxes and implied consent which were used as justification for data sharing, digital tracking and unwanted communications for years are no longer appropriate. Indeed the raft of data protection regulations around the world have made much of this a thing of the past and it is now time for companies to embrace data protection fully in order to remain competitive. Their example "one of our clients generated 68% more consent by adopting the transparent, progressive approach and have also benefited from increased trust" will be food for thought from the sceptics amongst you. You can read the blog here: https://mylifedigital.co.uk/the-importance-of-linking-consent-management-with-customer-identity-management/

RM Girl (Emily Overton) - Managing your HR Personnel Records effectively

Emily is releasing a mini-series on how to manage HR records on her blog. Managing your HR Personnel Records effectively and Retention of your HR Personnel records are this week's theme. Emily explains "Big Bucket retention" where you give the use fewer categories of retention to pick from (such as unsuccessful candidates, current staff, former staff who left in the last 6 years, former staff who left over 6 years and those who are no longer working scheme). She then explains how long you would keep those records. If you are struggling with your HR Personnel Records this should be on your essential reading list: https://rmgirl.co.uk/2020/11/23/hr-personnel-records-part-1-of-5/