+44 113 322 27 90 info@dcrpartners.co.uk dcrpartners.co.uk

DCR Partners
DIGITAL | CHANGE | RISK

Byte Size Security

YOUR MONTHLY CYBER UPDATE

Issue | 04 | January 2022

Data Privacy

Google GDPR Gaffe

Regulators in Austria have this month announced that the protections provided by Google for analytics data shipped to the US are not sufficient to meet the requirements of the GDPR. In a decision that has the potential to be as high profile as the ruling on Privacy Shield in 2020, Austrian data regulators set out their belief that the fact that Google are able to access analytics data in plain text means that there is an increased risk that intelligence services may be able to gain access to PII contained within the dataset. Similar investigations into Google Analytics are taking place in a number of EU countries, however it remains to be seen if these rulings will impact how organisations use Google Analytics, or if new data privacy provisions within the US will be established.

Read more

Oversharing in Safari

Researchers have identified a bug in Safari which violates a fundamental security feature of web browsers and could allow websites to learn about the other websites you're browsing, in some cases including your username. Same-origin policy is used by web browsers to ensure that scripts contained in one webpage are unable to interact with information on another webpage you may have open. Apple have been made aware of the bug however at the time of writing no fix is available. The researchers who discovered the bug have depressingly concluded that 'until there is a fix users can't do much to protect themselves' their only advice is to either block JavaScript, or switch browser.

Read more

Cyber Security

An Email from Who-ber?

A security researcher has expressed his concern this month after being told that a weakness he identified in Uber's email infrastructure has been deemed, 'Out of Scope' of their public bug bounty program. Seif Elsallamy was able to take advantage of weak input validation on an Uber endpoint to send emails to any email address, which appeared to be sent from a verified '@uber.com' email address. Whilst this weakness may technically be out of scope of their programme, we're pretty certain that it could be used to dupe unwitting recipients into handing over personal information. Interestingly, emails sent using this weakness were able to pass DKIM and DMARC checks which are often an organisation's key controls against email spoofing.

Read more

Revenge of the Cloud

It turns out it's not just legitimate organisations who are rushing to take advantage of the benefits public cloud services offer. Cisco Talos have begun to see an increasing amount of malware campaigns being underpinned by C2 infrastructure hosted in public cloud giants AWS and Azure.

This model benefits criminals in a number of ways. No longer do they have to maintain physical infrastructure which can be tracked down and taken offline. Also many organisations will have opted to 'trust' vast swathes of AWS / Azure IP ranges, which could now be linked to malicious activity. We're interested to see what response cloud providers put in place to address malicious activity hosted on their infrastructure.

Read more

Regulation

Cryptographic Controversy

The Home-Office has this month kicked off a campaign arguing against the use of end-to-end encryption by messaging apps. The campaign is based on the belief that using encryption in messenger apps could hide indicators of child abuse. This stance, however, has been criticised by the ICO. The ICO argues that there are most likely other solutions that can help to address the problem which do not involve weakening encryption and potentially reducing online privacy for all. We're monitoring this story to understand any wider privacy implications for all users of messenger apps.

Read more

Licenced to InfoSec

The Government has issued a consultation document which sets out a number of plans for the future of the information security industry in the UK. Included in this document is reference to a formal register of InfoSec Practitioners, which would open up the potential for individuals to be barred from working in the industry if they don't meet 'competence and ethical requirements'. There are understandably concerns from a wide range of industry professionals as it's unclear as yet who will set the definition of competency and ethical behaviour. The consultation is open until 20th March, so there's plenty of time to have your say.

Read more

Resilience

The Ultimate Business Continuity Test

In response to country-wide protests over rising fuel prices, the Kazakhstani government has taken the drastic step to 'shut down' the internet. This is yet another example of a concerning trend occurring across a range of countries who are undergoing civil unrest / protests. A nationwide communications blackout was first identified on 4th Jan which will have undoubtedly impacted consumers and businesses alike. We can only imagine the disruption caused to critical national infrastructure and emergency healthcare during the blackout which reportedly lasted for six days. Initial estimates of the economic damage exceed $429m.

Read more

Allianz Risk Barometer 2022

This month Allianz have published their annual risk barometer, taking into account responses from their corporate customers around the world. Here are a few headlines:

- Cyber retains top spot
- Ransomware on the rise
- Supply chain attacks increasingly concerning
- Record numbers of insurance claims