☎ +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 | 05 | February 2022

Data Privacy

Is Siri Snooping on You?

We think most people have sometimes suspected that our devices know too much about us and can seem to serve us ads as if they know what we're thinking. Well it turns out that some devices may have been listening a little too hard when they weren't supposed to be. This month Apple have fixed a bug in iOS which allowed Siri to record user's interactions with Siri, even if they had opted out. Apple typically sends recordings for analysis to improve performance. This serves as a reminder to us that even when we trust a company, they don't always get everything right when it comes to our information.

> Read more

Facebook: Feature or Faux Pas

Popular Chrome extension "L.O.C." has come under fire for its supposed ability to siphon data from Facebook users. The claim comes from a security engineer at "Brave", in which he states, "The API used by the extension does not cause Facebook to show a permission prompt to the user before the application's access token is issued." Users who are already logged into Facebook run the risk of having their data accessed by a third-party. Facebook calls this token a feature, instead of a security concern, how much longer can they deny this is an issue?

> Read more

Cyber Security

Defender Doubles Down on Mobile Protection

As part of a broader effort to expand Microsoft's security platform capabilities, they have announced threat and vulnerability management support for Android and iOS through Microsoft Defender for Endpoint. This coverage now supports all major device platforms, covering workstations, servers, and even mobile devices. As a result, Defender can now operate seamlessly within the workplace to identify and remediate vulnerabilities without the need for multiple vulnerability management programs, reducing business costs and simplifying security operations.

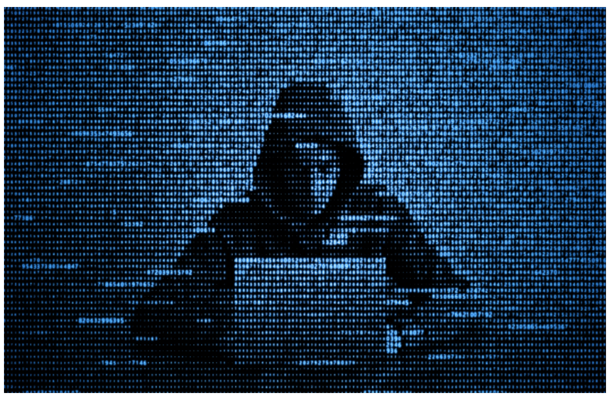
> Read more

Sentinel Steps Up GitHub Security

Good news for GitHub users! Microsoft have announced that Microsoft Sentinel, previously known as Azure Sentinel, now provides continuous support through threat monitoring. Potential threat actor activity is analysed by Sentinel's AI and allows you to investigate anomalies in your environment. Suspicious events will be picked up by built in analytics rules and be viewable under a single workbook! This means you'll be aware of any changes, creations, cloning, and deletions to any GitHub repositories under your control.

> Read more

Resilience



Ransomware Driving Us Nuts

A Conti ransomware attack on KP snacks has been announced in which data was held hostage and business supply lines were affected. This has meant no new orders or deliveries until the end of March, severely hampering KP's ability to conduct business. An attack such as this outlines the necessity of disaster recovery and business continuity planning. The reduction in availability to key resources alone can harm a business's bottom line more than the price tag on the ransom note. The group responsible for the attack have not been named but KP's company logo and data have been added to the Conti ransomware gang's data leak website.

> Read more

Say No to Malicious Macros

At last, the news we've all been waiting for! Microsoft have announced that they're updating their products to block macros downloaded from the internet by default. This step, along with making it more difficult for users to 'enable macros' has been welcomed by security professionals across the world as malicious macros have been a persistent challenge for decades. If a user wants to enable macros they will now be encouraged to follow a link to find out more about how much damage macros can cause. Hopefully this will help stop the increasing popularity of malicious macros as an attack vector.

> Read more

Regulation

Honesty Is the Best Policy

Whilst the efficacy of GDPR enforcement measures are often the source of some debate, we believe the protections it enshrines continue to be vital in providing citizens with a base level of confidence that their data will be protected. This month the Greek data protection authority has fined the largest technology company in the country around €9m for a range of infringements. One of these is the company's failure to adequately inform impacted individuals about the extent of the incident. We know we've felt before that breach notifications can sometimes feel slightly opaque. Perhaps this case will serve to change how open companies are with us when something goes wrong.

> Read more

Microsoft blocks around **25 billion** brute force attempts per year.

They claim enabling MFA would prevent **99.9%** of these attempts being successful.

However, only **22%** of Azure AD customers use MFA.

Is it time to reconsider rolling out MFA?