☎ +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 | 03 | December 2021

Resilience

Burnout Drives Security Indifference

Possibly confirming what many of us have suspected for some time, 1Password have undertaken research which concludes that pandemic-related burnout is not only a real problem, but increases the likelihood of security incidents occuring. Their research found that burnout is negatively impacting organisations in a number of ways. Generally, employees are tired, worn down, more likely to use weak passwords, and more likely to 'bend' the rules to get things done, for example by using new SaaS applications. Compounding this, 10% of security professionals reported that as a result of the ongoing pandemic they are feeling completely checked out and doing the bare minimum at work which means it's more likely that incidents slip through the net.

> Read more

Too Many Eggs, Not Enough Baskets

Another month, another outage at AWS. It feels like we touch on this topic every month, and these outages continue to highlight the huge dependencies we have on a handful of technology mega-corps. Back in the halcyon days of cloud migration one of the assumptions that was consistently bandied about was the fact that 'they can run it more reliably than we can'. We're keeping an eye on these AWS outages, which have global reaching impacts, to see if there is any indication of a shift away from cloud infrastructure as companies seek to remove all their eggs from the AWS basket.

> Read more

Cyber Security

Disgruntled Developer Wields Devastating Power

We spend a lot of time and effort supporting our colleagues to better identify and avoid security threats they may encounter day to day, however it would take something a little more robust to stop a determined malicious insider like Nickolas Sharp. Nickolas purportedly used his administrative privileges to steal gigabytes of confidential files from his employer, before trying to extort them for $2m dollars, all whilst appearing to be helping the company to 'investigate the incident' whilst at work. Ultimately a brief outage in his VPN service appears to have allowed investigators to identify him as the source of the attack. Questions must surely be asked to understand how an individual was able to undertake such an attack without falling foul of privileged access management, data loss prevention, or activity monitoring controls.

> Read more

Last Chance to Lock Down LastPass

Worrying reports of large scale credential stuffing attacks against LastPass serve to highlight the importance of thinking long and hard about where you choose to secure passwords that could give an attacker unfettered access to your systems and information. Many users have reported on social media that they were receiving multiple emails suggesting someone was attempting to log into their LastPass accounts. LastPass have not suggested that any of these attempts were successful but again, another reminder to make sure the basics are in place when it comes to password management. Put them somewhere only you can get to them, protect them with more than just a username and password.

> Read more

Regulation

GDPR - Big Teeth, No Bite?

When GDPR came into force in 2018, a lot of privacy and security professionals were waiting with bated breath to see who would be first to fall foul of the terrifying new power wielded by the ICO. Most organisations had spent the previous 12 months frantically mapping data flows, understanding data types, and updating privacy policies to establish a robust data protection framework. We think it's fair to say that since the enforcement of GDPR began, many of the fines issued to organsiations have appeared to be slightly underwhelming. This new investigation suggests that there are a number of organisations who receive nothing more than a 'reprimand' from the ICO, despite some of these organisations having lost control of millions of pieces of personal information.

> Read more

Focussing In On Critical Infrastructure Attacks

In our opinion the more that policy makers, regulators, legislators and government bodies talk about information security, the better. This month the US Department for Homeland Security (not the one with Damien Lewis) has issued instructions to obligate operators of critical national infrastructure to report cyber incidents within 24 hours. This edict shows that the potential colossal impact of issues in complex interconnected systems is really being taken seriously. It will also allow for better centralised visibility of ongoing or emerging attacks which, if disseminated effectively, could allow organistaions to enhance how they proactively defend against real life threats.

> Read more

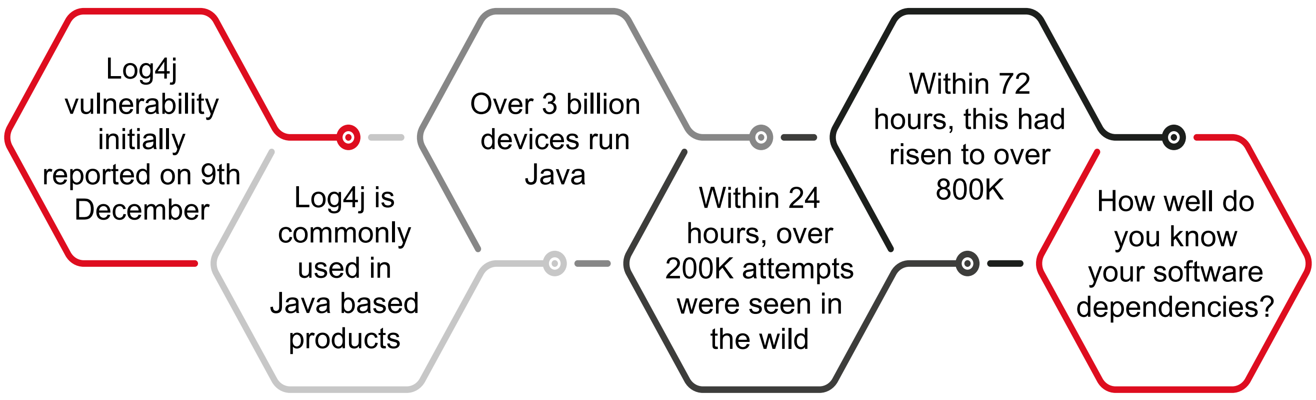
Data Privacy

Police Data Pinched From Supplier

Yet another worrying tale of supply chain compromise. This time the Clop ransomware group managed to successfully phish an IT support firm who work with 90% of the UK's law enforcement agencies. Reports suggest that when the IT support firm refused to pay a ransom demand, 13 million records stolen during the attack were released onto the dark web. It is unclear as yet the full extent of the data stolen in this attack, which is still under investigation, with support from the NCSC, however it does serve as yet another reminder that your security controls are only as good as the weakest link. More often these days we see those weakest links materialising in supply chains, despite ongoing efforts to undertake assurance / due diligence over the security posture of 3rd parties.

> Read more

Log4j - Why are security teams losing sleep?



Log4j vulnerability initially reported on 9th December

Log4j is commonly used in Java based products

Over 3 billion devices run Java

Within 24 hours, over 200K attempts were seen in the wild

Within 72 hours, this had risen to over 800K

How well do you know your software dependencies?