SME Cyber Digest

14th February 2017

- Sports Direct Hack: Employees Unaware
- Cost of a Data Breach
- GDPR: The SME Challenge
- Unpatched WordPress Sites Hacked
- Fake Chrome Font Update Attack
- Twitter Account Phishing Scam
- Vulnerabilities Found In Printers

CESG Certified Training · CREST · TIGERSCHEME · CHECK IT Health Check Service · PCI DSS COMPLIANT · Cyber supplier to: HM Government

Customer Services
+44 (0) 845 600 4403
pgicyber@pgitl.com

Cost of a Data Breach

Cisco has released its annual cybersecurity report. The survey, covering 3,000 respondents at chief executive level, found that 50% of companies face public scrutiny after a breach, leading to reputational risk, and 20% reported that they lost customers as a result. Additionally, 23% had identified lost business opportunities from prospects. The main reasons cited for the breaches include budget constraints, incompatible systems and inadequately skilled staff. However, the overall cost of a data breach was harder to quantify. While a third of victim companies reported a 20% loss of revenues, other surveys such as IBM's Cost of Data Breach Study, report the cost of a breach as an average consolidated cost totalling $4m in the last year. Regardless of what metrics they use, most reports suggest that data breaches are growing and the ramifications painful.

Sports Direct Hack: Employees Still Unaware

In September 2016, Sports Direct suffered a data breach that led to the personal details of 30,000 employees being released. A hacker accessed the company's IT network and exploited a vulnerability affecting software Sports Direct were using to administer a staff portal. However, it wasn't until December that the company learned of the data breach (which included names, email, postal addresses, and phone numbers) yet staff had still not been notified. According to the Register, 'Sports Direct filed an incident report with the Information Commissioner's Office after it became aware that its workforce's information had been compromised, but as there was no evidence that the hacker had made further copies or shared the data, the company did not report the breach to its staff.'

Sports Direct staff have therefore been denied the opportunity to check their financial records or change passwords, giving potential rise to further attacks. Under the forthcoming General Data Protection Regulation (GDPR), due to be introduced in 2018, Sports Direct would not achieve GDPR compliance; they would have received a fine of up to 4% of global turnover totaling some £116 million.

It is of paramount importance that companies start to think now about how they plan to implement appropriate technical and organisational measures to ensure privacy and data protection in 2018. The onset of GDPR will widen the definition of "personal data". It will cover a wider range of data types relating to an identifier such as a name, an identification number, location data or an online identifier such as an IP address or a cookie identifier.

GDPR: The SME Challenge

BUSINESS CONSIDERATIONS

1. Privacy Policy
2. Fulfilling the Right to be Forgotten
3. Subject Access Requests
4. Data Portability
5. Data Processors
6. Procurement Projects
7. System Upgrades
8. Data Protection Impact Assessments (DPIA)

CASE STUDIES

SPORTS DIRECT

Breach: Details of 30,000 staff released

How: Hacker accessed internal network

Fine under GDPR: £116 million

TESCO

Breach: £2.5 million stolen from 9,000 accounts

How: Details and source yet to be made public

Fine under GDPR rules: £1.9 billion

MORRISONS

Breach: Details of 100,000 staff released

How: By a disgruntled employee

Fine under GDPR rules: £680 million

GDPR

In 2018 it becomes the principal law regulating how companies protect EU citizens' personal data

Any company that markets goods or services to EU residents, regardless of location, will be subject to GDPR

Aims to create more consistent protection of consumer and personal data across EU nations

Non compliance, or any breach that puts individuals at risk, could result in fines of up to 4% of global turnover

LONG-TERM BENEFITS OF GDPR

- GDPR should not be viewed as a burden for organisations
- GDPR recognises human factors are just as important as technical measures
- An opportunity to cleanse and consolidate data
- It will help to decrease the number of vulnerabilities and reduce attack surface
- The impact of failing to comply, and the current likelihood of a breach, will ensure corporate and board-level support

Other Stories

Unpatched WordPress Sites Hacked

We have previously reported on several alarming stories regarding WordPress vulnerabilities. This week security firm Sucuri suggested thousands of websites have been hacked solely because system administrators have not updated their WordPress, as advised by the company. The latest vulnerability allows hackers remote unauthorised access to edit or delete WordPress pages. Unsurprisingly, attacks intensified less than 48 hours after the disclosure. At the same time, Sucuri report that they are currently tracking four different hacking groups conducting mass scans and exploits attempts across the Internet. In fact, one of the defacers has already compromised over 66,000 pages, and the number will likely increase.

Fake Chrome Font Update Attack

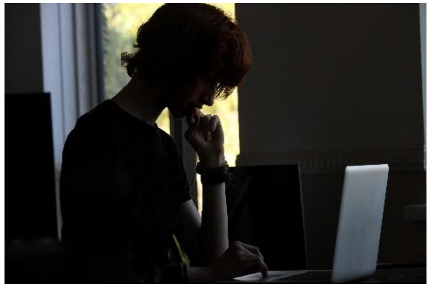
A malware campaign targeting Chrome users with fake font update notifications is now distributing ransomware instead of ad fraud malware. According to researchers, the campaign is unique because it was targeting Chrome for Windows users with automated social engineering tactics. Code injected into compromised websites would fingerprint visitors and, if certain criteria were met, it would make the text on the page look unreadable while also displaying a fake alert informing users they needed to install a font pack update to properly view content. Victims were told that the browser couldn't find the font needed to properly display the page and that the update should be installed immediately. Users were prevented from closing the fake alert via the "x" button, and the malware would immediately start installing in the background if the user approved the update. The campaign is utilising Spora ransomware which, although new, has well-implemented encryption procedures, a well-designed payment site, and provided victims with several "packages" to choose from, all of which made researchers believe the threat was the offspring of professionals.

Twitter Account Phishing Scam

Attackers are targeting Twitter users in a phishing campaign purporting to offer account verification for Twitter users. Legitimate ads target senior management and originate from an account that copies the official Twitter support account, @SupportForAll6. The link then takes users to a malicious domain called twitterhelp.info. The site looks genuine but when users follow instructions to get their accounts verified, they are asked for plenty of compromising information such as their Twitter usernames, emails, phone numbers, account password. They are then asked for credit card details. This latest scam reflects a growing trend in social media phishing which has seen a 150% increase in the first six months of 2016.

Vulnerabilities Found In Printers

Attackers are actively seeking popular printer models made by HP, Lexmark, Dell, Brother, Konica and Samsung to exploit vulnerabilities that expose passwords, allow remote shut-down of printers and even stealing print jobs. Academic researchers have published a series of advisories and an informational wiki regarding their findings. According to the research, nearly 20 printer models have vulnerabilities tied to common printing languages, PostScript and PJL, used in most laser printers. Attacks can be performed by anyone who can print, for example through a USB or network. In total, researchers have published six separate advisories advocating patches for the vulnerabilities.



Visit Our Websites

Protection Group International:
www.pgitl.com

Protection Vessels International:
www.pviltd.com

Cyber Services:
www.pgicyber.com

Cyber Academy:
www.pgicyberacademy.com

Intelligence Services:
www.pgi-intelligence.com
www.riskportal.pgitl.com

JTip:
www.jtip.co.uk

Follow us on Social Media:

Customer Services
+44 (0) 845 600 4403
pgicyber@pgitl.com