EARLY MORNING MEDIA

Produced by Early Morning Media

Wednesday, 13th March 2019

THREATS & ATTACKS

RBS customers at risk of cyber attack

Royal Bank of Scotland (RBS) customers have been put at risk of cyber attack after being recommended flawed security software. Since January, the banking group has begun to offer its business banking customers a product called Thor Foresight Enterprise free of charge. Heimdal Security sells it as ‘next generation protection’ against cyber threats. But security researchers uncovered a flaw in it that made customers less secure. The bug has now been fixed with Heimdal Security estimating that about 50,000 people were using the vulnerable software. RBS said it had only affected NatWest customers as it was not yet being offered to its RBS and Ulster banks.

BBC News

Cyber attacks could cost firms £1 billion per year

Cyber attacks may now cost the UK economy more than £1 billion every year, according to research by Netscout, which says that the majority of business affected by distributed denial-of-service (DDoS) attacks, which infect a network and block users from accessing it, suffered network outages costing an average of £140,000. The figures equate to costs of roughly £900 million for large UK companies but, with many SMEs now also affected by cyber attacks, the total cost may exceed £1 billion, the report warned.

City AM   Information Age

Hacked Asus computers warning

Research by Kaspersky Lab suggests that a million Asus computers worldwide were infected with spying software by hackers linked to a Chinese-speaking group known as Barium. The hackers reportedly infiltrated the Taiwanese manufacturer's systems to insert a ‘backdoor’ for espionage into legitimate software updates sent out last year. The attack was designed to identify 600 machines in specific networks. If it identified a computer as a target, it downloaded more malicious code to give the hackers greater access.

The Daily Telegraph   Forbes   Tech Radar

EU announces plan to manage 5G security risks

The European Commission has published an EU-wide plan to manage cybersecurity risks in next-generation 5G networks. However, the commission stopped short of suggesting a ban on Huawei products, despite pressure from the US, which has concerns about Beijing’s influence on the company. The report says EU member states should create 5G risk assessments, which will then be used to create an EU-wide assessment. The decision on whether to exclude companies like Huawei on national security grounds will be left to each country.

The Verge   Financial Times

Police Federation hit by cyber attack

The UK Police Federation has confirmed it has been the victim of a ransomware attack. The attack hit computers at the federation's Surrey headquarters on March 9. Several databases and email systems were encrypted, the organisation said, leading to some disruption to its services.
Tech Crunch

POLICY, REGULATION & COMPLIANCE

Labour MP slams cybersecurity strategy

Shadow Cabinet Office minister Jo Platt has claimed that the UK's cybersecurity strategy is in a "chaotic" state. Speaking at the ICT Public Sector event last week, the Labour MP told the audience the security measures in place to protect the UK against a cyber attack were insufficient. She pointed to the fact that six departments have various cyber responsibilities, with the same amount of secretaries of state and sets of civil servants who deliver six different responses to the cybersecurity issue, without any cohesion. Platt also stressed the need to address the skills gap. She said 54% of all businesses and charities had a basic technical cybersecurity skills gap, but the government hadn't even calculated the shortages in that particular area of expertise.
Computer Weekly

Experts to support global firms against cyber threats

The Cyber Readiness for Boards project - a consortium of UK cybersecurity experts funded by the National Cyber Security Centre (NCSC) and the Lloyd's Register Foundation, has launched to explore the factors shaping UK board decisions around cyber risk and develop interventions to provide guidance and support. "Understanding the decision-making process and the way that boards assess cyber risk will be fundamental to addressing some of the ongoing challenges we face – both here in the UK and globally," said project lead Dr Madeline Carr, of UCL. Meanwhile, the NCSC has published a cyber Board Toolkit, which provides a general introduction to cybersecurity as well as offering recommendations of best practice to anyone that is accountable for cybersecurity within an organisation.
UCL News   Tech UK   IT Pro

63% of IT managers plan to use AI for cybersecurity tasks

As many as 63% of IT decision makers plan to leverage AI technology solutions to automate their security processes, due to staffing shortages, new research has revealed. "There's a real and critical shortage of cybersecurity people. But there's a fix for it today. AI and machine learning can reduce the workload today on the people we have, by handling the low value tasks we currently use our high value people for," said Greg Young, vice president for cybersecurity at Trend Micro, which conducted the study.
TEISS

Complacency in supply chain puts SMEs at risk

SMEs are being urged to protect themselves against cyber attacks to mitigate the risk of being excluded from supply chains. Joe Collinwood, CEO at CySure, warns that "many organisations are focusing efforts on protecting the confidentiality, availability and integrity of their networks and systems," but he adds that "while this is important, SMEs are typically failing to understand the wider risks and to implement basic cyber hygiene measures." Mr Collinwood's comments come as new research conducted by the FSB identified that 65% of UK Small Businesses do not have plans in place to deal with potential supply chain disruption including cyber crime.
London Loves Business

New online regulator powers spark backlash

Plans to announce new regulations governing social media firms have been postponed by the UK government amid concerns from some ministers that they are too draconian. Leaked details reveal that a new watchdog dubbed Ofweb will be given sweeping powers to enforce a strict Online Harm code of conduct drawn up by Home Secretary Sajid Javid and Culture Secretary Jeremy Wright. Fines will be handed out to firms, as well as individual company bosses, if they breach a 'duty of care'. The rules would apply to 'a very wide range of companies of all sizes, including social media platforms, file-hosting sites, public discussion forums and messaging services', which would mean newspaper websites would have to sign up to the regulator. Meanwhile, Mike Cunningham, head of the College of Policing, has become the first police chief to voice support for regulation of social media firms, saying they have failed to crack down on "violent, insidious and criminal" content.

The Mail on Sunday   The Daily Telegraph

Facebook stored passwords unprotected

Security researcher Brian Krebs has raised concerns over the way Facebook stores data, saying that millions of user's passwords were accessible by up to 20,000 of the social network's employees. Mr Krebs found that up to 600 million passwords were stored in plain text, saying a source within the firm had told him that 'security failures' resulted in developers creating applications that stored passwords without encrypting them. Facebook said it had now resolved a 'glitch' that had stored the passwords on its internal network, adding that it would enforce a password re-set only if its investigation into the issue uncovered abuse of the login credentials. Facebook's Pedro Canahuati said the firm has so far uncovered nothing to suggest anyone had abused or improperly accessed the data.

The Daily Telegraph   The Guardian   Tech Crunch   BBC News

Lack of vigilance negates cyber insurance

Eoin Keary, CEO and co-founder, edgescan, has said that as the number of cyber threats to business continues to increase, it is vital that firms are purchasing the right cyber insurance policies. He also warned that insurers will refuse to pay out if businesses have failed to monitor their security standpoint. "The ability to demonstrate to insurers, compliance, and regulatory bodies that you are maintaining and following leading cybersecurity practices is invaluable from a liability and reputational perspective," he adds.

IT Pro Portal

Beazley updates cyber coverage for UK firms

Specialist insurer Beazley has updated its policies to make it simpler for UK businesses looking to take out comprehensive cyber cover. The company has streamlined its UK cyber policies, Infosec, aimed at larger organisations, and BBR for SMEs. Infosec has also been updated to include access to the Beazley Breach Response unit, the firm's in-house breach response team.

Insurance Age   Insurance Business

TSB owner blamed for IT meltdown

The Sunday Times reports that last April's botched switchover of TSB customers' online accounts came after the IT division of its Spanish owner Sabadell breached its contracts with the challenger bank. Sabadell ordered its subsidiary Sabis to build and test new technology for TSB's upgrade. However, Sabis suffered a 'series of issues' and failed to deliver on crucial aspects of the contracts, say sources close to TSB's board.

The Sunday Times

Adults relying on youngsters for online security

Research conducted for the NCSC suggests that adults are more likely to seek online security advice from teenagers than their work colleagues or partners. Teenagers over the age of 16 were the preferred choice for advice on how to be secure online by 15%,

compared to 10% who said they would ask work colleagues and 8% who would speak to a partner. “Children are a vital cog in protecting online devices but we can’t emphasise enough the importance of increasing the numbers of those actively participating in cyber security,” said Chris Ensor, NCSC deputy director for skills and growth.
Tech Digest

GDPR

Uber faces legal challenge from drivers

A group of Uber drivers are suing the firm over claims it did not provide them with information under GDPR, saying the company failed to ‘respect their digital rights’ by not granting them a copy of their trip ratings, performance data and the duration of time that they worked. Doing so, they argue, has blocked them from calculating potential money owed in back pay and holiday pay. Ravi Naik of ITN Solicitors, who is representing the drivers, said that this case will be a "stress-test of Uber’s commitment to data protection".
The Daily Telegraph

British Airways data warning

British Airways staff have claimed that customer data has been handled insecurely and been open for potential misuse for several years. Employees at a call centre in Northern Germany say data is being protected on an ‘archaic’ system, while also suggesting that the airline’s flexible work-at-home policy posed risks to the airline’s data processing rules. Commenting on the claims, BA said: “We take the protection of our customers’ data very seriously, and we continue to invest heavily in data security. All our systems and procedures at our call centres are regularly audited”.
PYMNTS *Financial Times*

LEGAL SECTOR

DLA Piper bringing cyber case against insurer

The Times reports that DLA Piper is bringing a case against Hiscox after the insurer refused to pay out on a multimillion-pound insurance claim for damage caused by a cyber attack. The cyber attack on DLA Piper, in 2017, wiped out emails and telephones for 3,600 lawyers in 40 countries for two days. The firm is challenging its insurance provider’s decision in a private legal proceeding known as an arbitration. The Times cites several sources who suggest reasons that Hiscox may be refusing to pay out, with one suggesting there may be a ‘war exclusion’ in the law firm's cover, while a source close to Hiscox said that the dispute centred on the type of insurance cover DLA Piper had.
The Times

INDUSTRY & TECHNOLOGY

Scammers steal £1.2 billion from British bank customers

Figures from UK Finance show criminals fraudulently stole a total of £1.2 billion from UK bank customers in 2018 - up almost a quarter on 2017, when £968 million was stolen. The amount stolen in authorised push payment (APP) scams rose to £354 million, although financial providers were able to return a total of £83 million of these losses. Banks recorded 84,624 cases of APP fraud last year, almost double the number reported in 2017. Furthermore, cheque fraud losses jumped to £20.6 million in 2018, more than double the 2017 figure of £9.8 million. Consumer groups described the soaring numbers as ‘alarming’ and warned the true number of victims and losses were likely to be even higher as many

people are too ashamed to come forward. Research by UK Finance also shows More than four in 10 businesses in the UK are unaware of the risks posed by invoice fraud. There were 3,280 invoice and bank mandate scam cases involving businesses over 2018, costing firms almost £93 million. Some £29.6 million of the money lost to this type of fraud was returned to business customers, UK Finance said.
Financial Times   *The Guardian*   *The Sun*   *The Daily Telegraph*   *Daily Mail*   *BBC News*

Study of pre-installed Android apps finds privacy 'Wild West'

A study of pre-installed apps on Android devices has found there is little oversight or control over the data collected and sent to remote servers. While the findings did not discover any single point of data insecurity, researchers at the Carlos III University in Madrid, along with IMDEA Networks and the International Computer Science Institute at the University of California, Berkeley, said they bring to light the extent of preinstalled apps' reach, their lack of transparency and the way they stand outside the systems that regulate other Android software.
Silicon.co.uk