1 February 2017

Synopsis

Scroll to read full summaries with links to news articles.

Following a **cyber attack** on senior politicians in the **Czech Republic**, the government has made public their suspicion of Nation-state involvement in the hack. The complex malware is believed to have affected the country for several months, with Foreign Minister **Lubomír Zaorálek** hinting at **Russia's** possible involvement.

Donald Trump has this week issued an executive order reducing the **data privacy** protections of foreigners. The move has raised concern for the EU-US data privacy agreement, as the **EU** may look to abandon the agreement if equal protection is not guaranteed for its citizens.

The **Belgian** telecommunications regulator **BIPT** has this week cleared operator **Proximus** of breaching EU **net neutrality** regulations, finding that the use of favourite apps to give limited charge free use of social media did not breach zero rating restrictions.

In the **United States** this week the biggest digital issue has been the series of executive orders yet to be signed on **cyber security**. A much vaunted order for Cabinet appointees to be responsible for the cyber security of their departments has been postponed, along with an order calling for a 60 day report on the nation's cyber security.

Elsewhere **Ajit Pai** the new chair of the **FCC** has stated his intention to repeal regulations adopted during the Obama administration. Amongst these regulations will be **net neutrality**, which Mr Pai wants to repeal, though he has been less forthcoming on whether the FCC will continue to enforce the regulations until their repeal.

Twitter has this week disclosed two occasions on which the **FBI** issued national security demand letters for the personal details of users. The revelation was made possible after the FBI rescinded gag orders on the two letters which had previously barred disclosure.

Microsoft Security Intelligence have reported that countries in **Asia Pacific** markets are most suceptable to **malware** threats, in particular Vietnam and Indonesia who encountered twice the global average in malware attacks, with a 45% encounter rate. The report also identifies the variations across the region, with higher digital maturity countries like **Australia** and **Japan** facing fewer threats than countries with developing digital sectors.

I**sraeli** Prime Minister Benjamin **Netanyahu** has called for greater international collaboration on **cyber security**, during a speech at **Cybertech** Tel Aviv. Mr Netanyahu also announced his intention to place cyber security front and centre during his meeting with President Trump on the 15th February.

ENISA has this week announced a new report into **ICS-SCADA** systems and architectures, detailing how best to protect critical infrastructures.

ICANN's Board Candiatate Evaluation Committee has announced the final slate for the ICANN board director selection process, with **Alan Greenberg** (Canada) and **Leon Felipe Sanchez Ambia** (Mexico) reaching the final stage.

Europol has this week announced a memorandum with the **Global Cyber Alliance** to improve internet security both in the **EU** and abroad. As part of the agreement **GCA** will sign up to Europol's **No More Ransom** project and will work with Europol to develop **DMARC** email validation policies.

IEEE Global Internet Governance Monitor

1 February 2017

Table of Contents

Disclaimer: Please note that this monitor is a summary of news sources and does not reflect the official views of IEEE.

Europe

Internet governance

No new items of relevance

Net Neutrality

31.01.17
Regulators clear Proximus app zero-rating offer

Belgium's largest operator Proximus was cleared of breaking EU net neutrality regulations with a favourite app offer, after the country's regulator concluded the zero-rating deal was not discriminatory.

The Belgian Institute for Postal Services and Telecommunications (BIPT) investigated the company's deal, which allowed customers to select one favourite app – either Facebook, WhatsApp, Snapchat, Instagram, Twitter or Pokémon Go – and receive free data for its usage up to a defined limit. After the cap, all data used was charged at the standard rate.

In its statement, the BIPT said: "There are no elements at the moment indicating that the zero rating of apps by Proximus endangers the Internet users' rights to consult information and content freely, to share it and to use and provide the applications and services of their choice."

EU rules on net neutrality state all internet traffic should be treated equally and, following interpretation from national regulators, a number of operators have already been told to discontinue zero-rating offers, including Sweden's Telia earlier this month and T-Mobile in the Netherlands in December.

Last week, Telenor's Hungarian arm was found to be in breach of the EU guidelines by the National Media and Infocommunications Authority for its Mychal package – which offers 1GB of free Facebook, WhatsApp, Facebook Messenger, Instagram, Twitter and Viber – and its music package MyMusic Start.

Cyber Security

31.01.17
Nation-state suspected in hacking of Czech foreign minister

The Czech government believes a nation-state actor is behind the hacking of high-ranking Czech politicians, including Foreign Minister Lubomír Zaorálek, according to reports.

Czech news site Neovlivní.cz reported that an official familiar with the investigation claimed thousands of files were stolen in the breach that is said to have lasted several months.

“We are trying to determine the extent of the infestation,” government spokesman Michael Lagronová told the site.

The complexity of malware used in the attack has led some to believe the attack is from a nation-state, according to The Guardian.

At a press conference, Zaorálek gave a hint he believed the attacker might be Russia.

“When I discussed this with the best experts that we have here, they told me that the character of the attack was such that the attack was very sophisticated, that it must have been, according to them, conducted by some foreign state, from the outside,” Zaorálek said, according to The Guardian.

Cyber Skills

27.01.17
Demand for security pros in UK rises by 46 percent

To say that IT security professionals in the UK are in demand would be a severe understatement. A new report by Experis says there has been an increase of 46 percent in the demand for both permanent and contract IT security professionals.

The report, entitled *Tech Cities Job Watch*, says companies are putting more emphasis on long-term investments.

There has been a 52.9 percent surge in demand for permanent staff, year-over-year. From Q4 2015, to Q4 2016, the demand had risen "just" 15.3 percent. The increase in demand has also affected IT security pros’ salaries. Annual IT security permanent salaries increased 4.99 percent to £57,706. Contractor day rates have also risen 0.62 per cent to £484 in the same period.

Geoff Smith, managing director, Experis UK & Ireland, comments: "In the wake of several high-profile hacks, from the likes of Yahoo, NSA, and the Bangladesh Bank Swift, and with the European Union’s GDPR set to come into effect from May 2018, cybercrime is at the top of the C-Suite agenda for companies of all sizes -- not just the big multinational players. And, with business leaders taking cyber security concerns more seriously than ever before, we’re starting to see a shift in how they integrate the necessary skills into their workforce. While there’s still a requirement for contractor support, employers are now prioritizing long-term defense, and are increasingly looking for permanent IT security professionals to do this."

The report takes a closer look at 10 of the UK’s major cities, and London is leading the charge, with 3,164 jobs advertised, three times as much as in all

other cities combined (1,278). The gap is even bigger with contractor roles – 80 percent of them (604) are in London.

Cyber Privacy

25.01.17
Encryption "critical" for GDPR but many deterred by complexity

Email encryption is a “critical” or “very important” business priority for 53 percent of organisations, despite only being used “extensively” by 40 percent of organisations.

The findings, published by Echoworx and conducted by Osterman Research, suggest the technology's stock among business leaders is increasing, but perception issues over ease of use still remain.

The study, titled “Enterprise Encryption and Authentication Usage: A Survey Report”, polled the views of almost 165 IT decision makers and influencers, managing on average 14,000 email users per organisation.

It was to assess the adoption of encryption in the context of email, file sharing and other communication modes used to share sensitive and confidential records. More than half of the respondents (53 percent) considered email encryption a priority, up almost 10 percent on 2015.

27.01.17
Trump executive order threatens major EU-U.S. data privacy agreement, activists say

An executive order signed this week by President Donald Trump curtails data privacy protections that were extended to foreigners during the Obama administration.

President Barack Obama signed the Judicial Redress Act into law last year, effectively expanding the scope of the Privacy Act of 1974 — which governs the use, collection, maintenance and dissemination of personally identifiable information stored by the federal agencies. Policy experts say the executive order will diminish the influence of the law, not dismantle it entirely.

“In effect, [Trump’s executive order] seems to push for a narrow application of the Judicial Redress Act, or JRA. Though the JRA’s protections were [always] limited, it was an important signal that the U.S. was beginning to respect the rights of non-U.S. persons,” said Drew Mitnick, policy counsel with Access Now, a nonprofit digital rights activist organization.

“Walking back those protections could have serious implications for Privacy Shield, a [separate] agreement that enables the sharing of commercial data from the European Union to U.S.,” explained Mitnick. “That agreement is still in its infancy and is at risk of being overturned if European data protection officers or the European Commission find the U.S. government and companies transporting data aren’t adequately protecting the rights of Europeans.”

United States of America

Internet governance

No new items of relevance

Net Neutrality

27.01.17
Congress Pressured to Rescind FCC Privacy Rules

Internet providers and conservative groups are mounting pressure on Congress to undo privacy rules passed by the Federal Communications Commission last year, the strongest ever adopted by the federal government.

Industry groups including USTelecom, the American Cable Association, and CTIA, who collectively represent the biggest internet providers in the U.S., including AT&T, Verizon and Comcast, asked congressional leaders Friday to wind back the rules.

“Amongst other flaws, the FCC Order would create confusion and interfere with the ability of consumers to receive customized services and capabilities they enjoy and be informed of new products and discount offers,” a letter to House Speaker Paul Ryan and Senate Majority Leader Mitch McConnell reads. “Further, the order would also result in consumers being bombarded with trivial data breach notifications.”

The rules passed in October ban providers from collecting and monetizing virtually any subscriber information without users’ advanced permission, including browsing history and app usage. An outgrowth of the FCC’s net neutrality rules, the privacy order goes beyond the Federal Trade Commission’s privacy rules, which only require advance permission from users to collect sensitive data.

01.02.17
FCC’s Ajit Pai on net neutrality: “I favour an open Internet and I oppose Title II”

Ajit Pai today presided over his first Federal Communications Commission meeting since being named chairman by President Donald Trump, and he promised that the FCC will eliminate regulations under his leadership.

He also said that consumer protection and enforcement are important priorities for the commission—but he wouldn't comment about whether he'll enforce the existing net neutrality rules.

In a press conference after the meeting, Pai was asked several times about net neutrality. While Pai has repeatedly made it clear that he opposes the current

rules and wants to overturn them, he has not said whether the commission will continue to enforce all of the rules while they are still in place.

When asked by a reporter if the agency will continue to enforce the rules, Pai pointed out that he and fellow Republican Commissioner Michael O'Rielly already said they wouldn't punish small ISPs for violations of the net neutrality order's "enhanced transparency" rules. The FCC is finalizing an order that will exempt ISPs with 250,000 or fewer subscribers from those truth-in-billing rules and will not enforce them against the small ISPs while they're still in place.

Cyber Security

31.01.17
Trump signs exec order on cybersecurity

The executive order designates a number of reviews of the nation's posture regarding both offensive and defensive cyber capabilities.

President Trump today said he would put his signature to an executive order calling for an assessment of the nation's cybersecurity capabilities and weaknesses, according to a report from Reuters.

The move will likely designate a number of reviews of the nation's posture regarding both offensive and defensive cyber capabilities.

On announcing the order at the White House, Trump pledged to "hold my Cabinet secretaries and agency heads accountable, totally accountable, for the cyber security of their organizations."

31.01.17
Federal agencies leasing in foreign owned buildings may cause cyberespionage risks

Several federal agencies may be at risk of cyberespionage as a result of leasing space in foreign-owned buildings, a recent Government Accountability Office (GAO) report found.

The report found at least 25 different offices used by the agencies including FBI, Department of Justice, State Department, Social Security Administration, Homeland Security – U.S. Secret Service, and Treasury Department rent space in buildings with whom the nationality of a building's beneficial owner is not a U.S. citizen, according to the report.

In addition to sensitive information systems, the facilities also contained weapons, evidence, data centers, and were used for classified operations.

The GAO's reported its findings to the agencies that were potentially at risk and recommended the agencies “determine whether the beneficial owner of high-security space that GSA leases is a foreign entity and, if so, share that

information with the tenant agencies so they can adequately assess and mitigate any security risks."

Cyber Skills

No new items of relevance

Cyber Privacy

27.01.17
Twitter: FBI forced it to reveal data on two users

Twitter disclosed on Friday that the FBI had issued the tech company two national security letters accompanied by gag orders in the past two years.

In a blog post on Twitter's website, Elizabeth Banker, an associate general counsel for the company, published both national security requests, redacted to hide the identities of the users being probed as well as law enforcement officials.

The FBI's letters ordered the social media company to provide the name, address, length of service and records of message transactions of the specific users. The letters added, however, that Twitter should not turn over the contents of any communications."We're encouraged by the lifting of these two gag orders and those recently disclosed by Cloudflare, Google, the Internet Archive, and Yahoo," Banker wrote.

27.01.17
Trump executive order threatens major EU-U.S. data privacy agreement, activists say

An executive order signed this week by President Donald Trump curtails data privacy protections that were extended to foreigners during the Obama administration.

President Barack Obama signed the Judicial Redress Act into law last year, effectively expanding the scope of the Privacy Act of 1974 — which governs the use, collection, maintenance and dissemination of personally identifiable information stored by the federal agencies. Policy experts say the executive order will diminish the influence of the law, not dismantle it entirely.

"In effect, [Trump's executive order] seems to push for a narrow application of the Judicial Redress Act, or JRA. Though the JRA's protections were [always] limited, it was an important signal that the U.S. was beginning to respect the rights of non-U.S. persons," said Drew Mitnick, policy counsel with Access Now, a nonprofit digital rights activist organization.

"Walking back those protections could have serious implications for Privacy Shield, a [separate] agreement that enables the sharing of commercial data from the European Union to U.S.," explained Mitnick. "That agreement is still in its infancy and is at risk of being overturned if European data protection officers or

the European Commission find the U.S. government and companies transporting data aren't adequately protecting the rights of Europeans."

Pan-Asia

Internet Governance

No new items of relevance

Net Neutrality

No new items of relevance

Cyber Security

31.01.17

APAC countries among most vulnerable to malware threats: report

Asia Pacific markets, especially the emerging ones, are among those at highest risk of cybersecurity threats with three out of the top five global spots for rate of malware encounters in the region, according to the latest edition of the Microsoft Security Intelligence Report which covers threat data from the first half of 2016.

Out of the top five locations across the globe most at risk of infection, two are located in Southeast Asia, namely Vietnam and Indonesia. Both locations have a malware encounter rate of more than 45 percent in the second quarter of 2016, which is more than double the worldwide average of over 21 percent during the same period.

Other top markets under malware threats include large developing markets and Southeast Asia countries – Mongolia, Pakistan, Nepal, Bangladesh, Cambodia, the Philippines, Thailand and India – each with encounter rates of more than 30 percent.

However, markets in the region with higher levels of IT maturity such as Japan, Australia, New Zealand, South Korea, Hong Kong and Singapore have displayed malware encounter rates that are below the worldwide average, highlighting the diverse cybersecurity landscape in the Asia Pacific.

01.02.17

Budget 2017: CERT-Fin Welcome but Cyber-Security Needs More Focus, Say Experts

While welcoming the government's move to establish the Computer Emergency Response Team for Financial Sector (CERT-Fin) to curb hacking and securing online data, cyber experts on Wednesday said much more is needed to be done in order to safeguard our computer networks and payment gateways as India aims to go digital.

During his Union Budget 2017-18 speech in the Lok Sabha, Finance Minister Arun Jaitley announced that CERT-Fin will be set up soon.

"Cyber-security is critical for safeguarding the integrity and stability of our financial sector. A CERT-Fin will be established. This entity will work in close coordination with all financial sector regulators and other stakeholders," Jaitley said in Parliament.

01.02.17
Cyber Security Agency of Singapore and British security company sign agreement

When Singapore's prime minister Lee Hsien Loong launched the country's cyber security strategy in October 2016, it marked a new chapter in the cyber security readiness roadmap of the Association of Southeast Asian Nations (Asean).

Lee said Singapore's cyber security strategy comprised of four pillars: building a resilient infrastructure, creating a safer cyber space, developing a vibrant cyber security ecosystem and strengthening international partnerships.

The developing a vibrant cyber security ecosystem pillar envisages developing companies and nurturing local startups. It also encourages fostering of closer partnerships between academia and industry to harness cyber security research and development (R&D).

It was in this context that BAE Systems – a British multinational defence, security and aerospace company with headquarters in London – announced the signing of a memorandum of collaboration (MOC) with the Cyber Security Agency of Singapore (CSA). This is to develop national capabilities through collaboration in capabilities-building and incident response.

Cyber Skills

26.01.17
IT and data security roles to dominate Singapore job market in 2017

Singapore's technology job market will be dominated by demand for professionals specialised in data security, applications and software development, and data management, according to a research by Robert Half.

Yet, according to Singapore information technology (IT) leaders, these high in-demand IT roles are also some of the most difficult to recruit for, Robert Half said in a press statement on 24 January 2017. This is due to a supply/demand imbalance of skilled technology professionals.

More than half (56 percent) of Singapore Chief Executive Officers (CIOs) say IT and data security is the key functional area within IT that will create the most jobs over the next five years.

"To counter and respond effectively to potential cyber attacks, companies are not only increasingly investing in technology, they are also bringing on board IT risk and security professionals," said Matthieu Imbert-Bouchard, Managing Director, Robert Half Singapore. "However, companies need to recognise they

are competing for a limited pool of IT professionals with the appropriate specialist skills in IT and data security making the skills shortage within IT even more apparent."

Cyber Privacy

No new items of relevance

Rest of the World

31.01.17
Netanyahu calls for International Collaboration to beef up Cyber Security

Just two weeks before his upcoming meeting with President Donald Trump, Prime Minister Benjamin Netanyahu called for strengthened multinational collaborations in the cyber security sector.

“By working together, we can more effectively defend against the force of terror, this cyber terror,” Netanyahu told participants at Cybertech Tel Aviv on Tuesday. “It’s important to have cooperation between some governments, especially like-minded governments.”

As countries around the world continue to face increased security threats to their cyber infrastructure, it behooves governments like those in Israel and the United States to share their capabilities to battle such dangers, the prime minister said. Heading into his meeting with Trump on February 15, Netanyahu said that one subject he was determined to raise was the issue of cyber security, an area on which the two nations have long been collaborators.

“We need to expand this and recognize that there is a core interest of the civilized countries and the democratic countries to protect themselves against cyber attacks,” Netanyahu said. “The more we work together, the stronger and safer we will become.”

Cybertech Tel Aviv 2017 is a three-day conference and exhibition involving more than 10,000 participants from around the globe.

31.01.17
Australian organisations forced to take cyber insurance seriously

Demand for cyber insurance remains patchy across Australia, with estimates ranging from 3% to 14% of organisations currently having some form of coverage.

The persistent lack of mandated data breach notification is regularly cited as a reason for this. While Australia’s proposed data breach notification legislation is making slow progress, the nation certainly does not lack data breaches.

At the tail end of 2016, big four bank NAB announced it had accidentally sent the personal details of 60,000 customers to the wrong website, while in early 2017, a slew of hacktivist attacks were launched – some by a Tunisian Islamist group which defaced the website of Victoria’s treasurer and a handful of schools. Another was launched against Victoria’s Human Rights Commission website.

In its 2016 threat report, the Australian Cyber Security Centre noted that there had been 1,095 serious security incidents affecting government systems, and 14,804 affecting private business in the 12 months to the end of June 2016.

Global Institutions

28.01.17
Is anyone spying on you through your webcam?

Happy Data Protection Day!

Today, 28 January 2017, is Data Protection Day. To mark the occasion, Europol's Data Protection Office (DPO) would like to raise awareness on webcam hacking, which can seriously threaten users of phones and laptops.

Webcam hacking: someone might be spying on you
Web cameras on laptops have become very popular nowadays: they are involved in everyday activities such as chatting with friends or for business-related activities. However, like with most technological developments, inherent advantages can be twisted and become a threat for users.

In the case of a web camera, the greatest possible risk is that a hacker gains access to it - even without being noticed - and records the user in order to blackmail them or to collect valuable information from the user's surroundings.

To prevent this happening to you, Europol's Data Protection Office (DPO), in cooperation with the European Cybercrime Centre (EC3), is raising awareness on spyware attacks, how to recognise the signs and how to protect yourself (download infographic here).

30.01.17
BCEC Announces the Final Slate of ICANN Board Director Candidates Selected by the At-Large Community

The optional Regional At-Large Organization (RALO) petition process in the ICANN Board Director selection did not result in a successful petition to add names to the Board Candidate Evaluation Committee (BCEC) Slate of Candidates and this stage of the process has now concluded.

As such, the Final Slate of Candidates, who were selected by the BCEC and will go forward to the next stage of the selection process organized by the Board Member Selection Process Committee (BMSPC), are (listed in alphabetical order of the last name):

- Alan Greenberg (Canada)
- Leon Felipe Sanchez Ambia (Mexico)

Expressions of Interest (EoIs) of the Final Slate of Candidates

You may view the EoIs (with personal and private information removed) of the Final Slate of Candidates HERE.

30.01.17
Europol and Global Cyber Alliance team up to fight cybercrime

Today, Europol and the Global Cyber Alliance (GCA)signed a Memorandum of Understanding (MoU) to cooperate on decreasing systemic cyber risk and improving internet security throughout Europe and beyond. The signing ceremony took place at Europol's headquarters in The Hague.

As part of the MoU, Europol and GCA will fight cybercrime through the exchange of information on cybercrime trends and joint international projects to increase cybersecurity.

To this end, the two organisations will partner to offer best practice recommendations that help organisations secure their networks and domains through the Internet Immunity project. Europol and GCA will initially focus on improving adoption of the DMARC email validation policies, a vital tool that enables organisations to authenticate email and prevent spoofed and fraudulent email.

Additionally, as part of the common efforts in the fight against cybercrime, GCA has agreed to sign up as a supporting partner of the No More Ransom project. Due to continuous interest from public and private sectors, a third enlargement of the No More Ransom project is expected to be announced in the coming weeks.

30.01.17
DIGITALEUROPE's President meets with Commissioner Moedas

On 27 January, DIGITALEUROPE's President Markus Borchert continued his high-level Commissioner outreach and met with Commissioner Carlos Moedas (Research, Science and Innovation) to discuss the priorities of DIGITALEUROPE including the mid-term review of Horizon 2020, open science, investments in innovation, the European Innovation Council and text & data mining.

Mr Borchert stressed the importance of the proper protection of IP rights in EU funded projects as well as the need for the Commission to support a broad application of text & data mining exceptions for commercial use. Mr Borchert noted that such actions would foster private investment in research and innovation in Europe.

Mr Borchert also welcomed the Commission's initiative of funds to foster further innovation in Europe. He expressed that a strict application of the 'Innovation Principle' accompanied by increased attention to demand-side measures such as standardization and public procurement can lead Europe towards innovative solutions.

01.02.17
Attacks on ICS-SCADA: How to protect critical infrastructures

The use of long-range communication networks, and specially the Internet, has revolutionised ICS-SCADA systems and architectures. The use of network

communication in these systems has proven to be an effective way of gaining a means for remotely operating and maintaining these infrastructures in real-time. Therefore, these have become vital assets providing a functionality otherwise impossible. However, this also opens up the way for new threat vectors that can potentially compromise the efficient and secure operation of these systems.

These threats are not necessarily new; many are inherited from the use of networking technologies - in use in IT areas for a long time now - which ultimately results in countermeasures being already available to mitigate or even eliminate them.

ENISA's study on communication network dependencies aims to help asset owners defend their critical infrastructures from emerging cyber threats. The main objective is to provide insight into the communication network interdependencies currently present in industrial infrastructures and environments, mapping critical assets, assessing possible attacks and identifying potential good practices and security measures to apply.

Diary Dates

CyberTech Israel 2017

31.01.17 - 01.02.17
Tel Aviv, Israel

ENISA evaluation and review

Open **from 18 January to 12 April 2017.**

3rd International Conference on Information Systems Security and Privacy – ICISSP 2017

19.02.17 - 21.02.17
Porto, Portugal

European Information Security Summit 2017 (TEISS)

21.02.17 - 22.02.17
London, UK

Singapore Cyber Security R&D Conference (SG-CRC 2017)

21.02.17 -22.02.17
Singapore

Emerging issues in building the European data economy

Foreseen for **1st quarter of 2017**

European Dialogue on Internet Governance

06.06.17 - 07.06.17
Tallinn, Estonia