IEEE

GLOBAL INTERNET POLICY MONITOR

Read summaries of significant recent internet technology policy activities around the world

15 February 2017

Synopsis

Scroll to read full summaries with links to news articles.

In the **UK** this week, **Ciaran Martin** the head of **the National Cyber Security Centre** has stated that 188 serious cyber attacks have been identified in the past three months, with tens of thousands successfully blocked in the past year.

In **France**, **President Hollande** has requested a full briefing on the Government's current activity to protect this years Presidential election. The request follows notable outbursts by Independent candidate **Emmanuel Macron**, who has accused **Russia** of interference.

Following their meeting at the White House on Monday, **President Trump** and **Canadian** Prime Minister **Justin Trudeau** have agreed to strengthen cooperation on **cybersecurity** issues. A particular focus has been placed on the protection of critical infrastructure from cyber attacks.

A Federal judge has ruled that **Microsoft** are allowed to sue the government on the behalf of their customers. The existing legal case focuses on the gag rule applied to **National Security** demands for customer data which then prevent companies like Microsoft from informing their clients of the privacy intrusion for an undefined period of time.

The **Internet Registry** of **Pakistan** and **ICANN** have agreed this week that domain name applications can now be made through **Urdu**, the predominant language of Pakistan.

A new report to the **Indian** Parliament has revealed that 50,300 **cybersecurity** incidents where identified during 2016. This figure is largely in line with the 49,455 incidents in 2015, but signals a significant increase from the 44,600 incidents in 2016.

TRAI the **India's** Telecoms Regulator has announced that its consultation on **Net Neutrality** will be extended to 15th March, providing an extra month for comments. The news comes as **Chinese** internet giant **Alibaba** has announced plans to provide free **Internet Access** to Indian citizens, a potential challenge to any future net neutrality regulations.

In **Australia** this week the Senate has passed a law mandating that businesses declare any **cybersecurity** breaches. The regulations are expected to be introduced in the next 12 months.

A **UN** expert has this week called upon the Government of **Cameroon** to reinstate **internet access** for the English speaking parts of the country, after they were turned off at the end of January.

ENISA has this week produced an analysis of the security measures used by digital communication providers in the **EU**. The report finds that all providers provide a basic level of protection with most also using previous ENISA recommendations to bolster their security.

Following a court ruling in California **ICANN** have been given power to proceed with the delegation of the **.AFRICA** generic top-level **domain.09.02.17**

IEEE Global Internet Policy Monitor

15 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

Cybersecurity

14.02.17

Ars Technica
UK gov't hit by 188 serious cyberattacks in the past three months

Britain has blocked tens of thousands of "potential" cyberattacks from external threats in the past year, amid reports that both Russia and China have significantly stepped up their cyber-espionage against the country in recent months.

The NCSC, which has been operational since October, was formally opened by the Queen on Tuesday. In an official report it was claimed that the NCSC had mitigated "a total of 54,456 attacks." 19,906, or 36 percent, of these attacks "were hosted in IP ranges delegated to the UK," and involved phishing and Web-inject malware. The remaining 64 percent, meanwhile, or 34,550 attacks, "specifically targeted UK government departments to exploit British citizens by fraudulently obtaining their online credentials and personal data."

Ciaran Martin, the head of GCHQ's National Cyber Security Centre, told the *Sunday Times* that there had been a "step change" in Russian online aggression, which had seen the government buffeted by 188 "high-level" attacks in the past three months alone, "many of which threatened national security."

The NCSC claimed that its work has improved take-down times for phishing sites from a mean of 27 hours before it became operational, to just one hour since.

14.02.17

SC Magazine
Tallinn cyber-warfare manual 2.0 refines definition of cyber-warfare

The Tallinn Manual's sequel has been released and builds on its predecessor's work by greatly expanding its gaze to peacetime cyber operations

The Tallinn Manual 2.0 is here to not only underline the presence of international law in the shadowy world of cyberspace, but to refine the meaning of cyber warfare.

The second iteration of the landmark document was launched in Washington on 8 February by the Netherlands Government, the Asser Institute and principally the Cooperative Cyber Defence Centre of Excellence.

The document itself updates the legal advice of the original manual, the world's first attempt to define the legal framework of cyber-warfare.

The original manual brought together 20 of the world's top international law experts to determine what the legal implications of an act of cyber warfare were. The legal scholars created an academic, non-binding study on how international law applies to cyber conflicts and cyber-warfare, and is widely referenced by lawyers globally.

Version 2.0 builds on that to discuss "cyber operations", acts which fall below the threshold of acts of war, yet trouble the cyberspace of nation states on a far more regular basis.

14.02.17

SC Magazine
Nuclear industry gets new cyber-security strategy from UK government

A new Civil Nuclear Cyber Security Strategy has been issued by the Department for Business, Energy and Industrial Strategy in the UK.

BEIS says the strategy helps ensure the UK has a secure and resilient energy system "by ensuring that the civil nuclear sector is able to defend against, recover from, and is resilient to evolving cyber threats".

The 25-page document addresses the threat posed by a range of potential attackers including terrorists, hacktivists, criminals and foreign intelligence services. BEIS fears disruption through the interruption of power generation or the compromise of sensitive information.

A blended attack is another scenario that it is concerned about, in which an adversary uses a cyber-attack to enable or reinforce a physical attack.

And SCADA legacy equipment – that is, computers and electronics that play a part in running nuclear plants but were developed prior to the advent of the internet – are widely regarded as dangerous because they lack robust online security systems.

The civilian nuclear industry generates about 18 percent of the UK's power and is seen as a way of helping the government meet its obligations to reduce carbon emissions.

15.02.17

Bloomberg
Hollande Requests Cybersecurity Briefing on French Election

French President Francois Hollande requested a full briefing on what is being done to fend off cyber interference in the 2017 presidential race.

"The defense council studied the level of threat," Hollande's office said in a statement after the security committee's weekly meeting Wednesday. "The president asked to be shown in the next meeting the specific protective measures and the heightened attention being given for the electoral campaign, including in the cyber sector," Hollande's office said.

Hollande's request comes after independent candidate Emmanuel Macron reported repeated cyber-attacks on his campaign and blaming Russian interference. Kremlin spokesman Dmitry Peskov denied Russia had any involvement in hacking the campaign in a conference call on Tuesday. He said there is no possibility that the Russian government had any connection to the attacks and that the accusations were "absurd."

Still, the Macron campaign hasn't backed down and has called for action on the part of the French state.

"Let's not let Russia destabilize France's presidential election!" Macron's campaign chief, Richard Ferrand, wrote in a column in Le Monde newspaper dated Wednesday. "What we want to do is to dedicate ourselves to our campaign and our program within the calm assured by the rules of our democracy."

Privacy

No new items of relevance

Internet Inclusion

No new items of relevance

United States of America

Internet governance

No new items of relevance

Cybersecurity

10.02.17

SC Magazine
Trump White House CISO Cory Louie reportedly removed from post

The White House has reportedly fired its chief information security officer Cory Louie leaving another key internal cybersecurity position open less than a month after former Federal CISO Gregory Touhill resigned from his post.

Louis was let go late last Thursday, according to Steve Clemons, Washington editor-at-large with *The Atlantic*, who is credited with breaking the story. The White House has not yet publicly commented on any such personnel move. However, Paul Innella, CEO of TDI Security, a consulting firm that regularly briefs government representatives on executive transitions, told SC Media in an interview that Corey is, indeed, no longer with the administration, based on his intimate knowledge of the Washington cybersecurity community.

“Everybody in the cybersecurity community saw this coming,” said Innella, who warned that the simultaneous absence of a U.S. CISO and White House CISO means that “We don't have two very critical CISOs that should be watching the house,” leaving cyber experts “a little trepidatious about what going to happen next, mostly in terms of how this is going to affect national security.”

A former Secret Service special agent and former security executive with Google and Dropbox, Louie was appointed to the position in 2015 by former President Barack Obama, who created the role as part of his Cybersecurity National Action Plan. Louie’s primarily responsibility has been protecting the president’s and his staff members’ digital assets from cyberthreats.

10.02.17

The Hill
House Homeland Security Committee plans cyber hearing next month

The House Homeland Security Committee is planning a hearing on cybersecurity threats early next month, The Hill has learned.

The committee is expected to hold a full hearing on the Department of Homeland Security’s (DHS) cyber defenses and threats to the U.S. on March 1, according to a committee aide.

The hearing will be the committee's first focusing on cybersecurity since the intelligence community concluded that Russia engaged in a cyber and disinformation campaign aimed at influencing the 2016 U.S. presidential election.

The hearing will not focus on the Russian election hacks but will instead cover the full scope of the threat landscape, touching on cyber threats from Russia, China, North Korea and other hostile actors, the aide said.

Hackers tied to North Korea's government made waves with the breach of Sony Pictures' computer systems in 2014, in retaliation for the Hollywood studio's production of the movie "The Interview," which mocked leader Kim Jong Un. The massive Office of Personnel Management hack detected in 2015, in which more than 20 million people had their personal data stolen, has been traced to hackers in China.

13.02.17

The Hill
Trump, Trudeau commit to cooperation on cyber

President Trump and Canadian Prime Minister Justin Trudeau committed to working together on cybersecurity and protecting critical infrastructure on Monday.

The pledge of cyber cooperation was one of several U.S.-Canadian partnerships highlighted by the two leaders during their first meeting in Washington, D.C.

"Given the integrated nature of the infrastructure that supports our intertwined economies, cyber threats to either country can affect the other," Trump and Trudeau said in a joint statement provided by the White House on Monday afternoon.

"We therefore commit to further cooperation to enhance critical infrastructure security, cyber incident management, public awareness, private sector engagement, and capacity building initiatives," they said.

Trump has signaled that cybersecurity policy will be a priority of his administration, though a planned executive action on cyber rolled out in January has been delayed without explanation from the White House.

Lawmakers have paid increased attention to cybersecurity and vulnerabilities in the wake of Russia's alleged hacking of Democratic organizations and individuals during the U.S. presidential election in an attempt to influence the outcome.

13.02.17

Forbes
IBM Turns Watson Into A Cybersecurity Weapon Amid White House Interest

IBM keeps doubling down on Watson, the company's heavily marketed cognitive software that has won *Jeopardy!* and reportedly helped find treatments for patients with cancer. Now IBM's putting Watson onto the case in the cybersecurity field.

Watson for Cyber Security, announced by IBM on Monday, takes the same core capabilities of Watson—the ability to read millions of documents and terabytes of information to derive insights a human might not spot—and puts them into a security operations center. With security officers at large corporations sometimes scanning several hundreds of thousands of events happening over their networks each day, IBM says it can add another line of defense by proactively helping to spot breaches and hacking attempts that might slip through unnoticed, then making suggestions on the best response.

"This is breaking new ground," says Mark van Zadelhoff, general manager of IBM Security. "Watson for Cyber Security will let customers very quickly go through these events and be more accurate."

The cybersecurity software was in use by 50 of IBM's customers before its release and will now be available in the company's online app exchange for a free trial, then billed as a premium software offering. Large corporations are the most natural sales target, but the product could make sense for companies as small as 100 people, says van Zadelhoff. Industries represented by customers so far include financial services and healthcare but also airlines and automakers, IBM says.

14.02.17

SC Magazine
One third of U.S. companies breached last year, study

A third of companies in the U.S. were breached in 2016, according to a study from Bitdefender issued on Tuesday.

And nearly three-quarters of those targeted are unaware of how the incident occurred, the survey found.

The statistics are a warning for CEOs and board members who "face increasing internal and external security risks that could ruin customer trust and business forecasts,"the study stated.

While the good news for security professionals is that the increasing threat landscape has motivated executives to regard CIOs as top C-level managers – joining COOs and CFOs in business decisions – indications are that not all C-suites include CIOs/CISOs in the business decision-making process.

The study, "Virtualization makes CIOs role key," [PDF] was conducted in October 2016 with 250 IT decision-makers at companies with more than 1,000 PCs.

14.02.17

Info World
Microsoft's president wants a Geneva Convention for cyberwar

Microsoft is calling for a Digital Geneva Convention, as global tensions over digital attacks continue to rise. The tech giant wants to see civilian use of the internet protected as part of an international set of accords, Brad Smith, the company's president and chief legal officer, said in a blog post.

The manifesto, published alongside his keynote address at the RSA conference in San Francisco on Tuesday, argued for codifying recent international norms around cyberwarfare and for establishing an independent agency to respond to and analyze cyberattacks.

What's more, he called on the tech industry to band together to protect users.

Such an agreement is necessary, in his opinion, because warfare in cyberspace involves infrastructure that's controlled and operated by private companies like Microsoft. Furthermore, some attacks, like the 2014 Sony hack widely attributed to North Korea, have targeted civilians.

"There's an additional consequence that results from all this," Smith wrote. "The tech sector today operates as the first responders to nation-state attacks on the internet. A cyber-attack by one nation-state is met initially not by a response from another nation-state, but by private citizens."

Privacy

10.02.17

Ars Technica
Judge sides with Microsoft, allows "gag order" challenge to advance

On Wednesday, a federal judge in Seattle allowed Microsoft's lawsuit against the government to go forward. US District Judge James Robart ruled that the company does, in fact, have standing to sue the Department of Justice on behalf of its customers.

Microsoft's case has drawn support from a number of major tech companies, including Apple, Twitter, Google, and Snapchat, among others.

The lawsuit first began nearly a year ago. Microsoft sued, arguing that when the government presents it with legal demands for user data held in online storage, those court orders often come with a gag order that has no end date. Because Microsoft is effectively forbidden from alerting its customers, even well after the fact, that such a data handover took place, the company alleged that its customers' First and Fourth Amendment rights are consistently violated.

In earlier court filings, Microsoft argued that in data or document handover situations prior to cloud storage, the "government had to give notice when it sought private information and communications, except in the rarest of circumstances." Effectively, the company claimed, this means the government expanded its ability to conduct “secret investigations.”

The government asked the judge to dismiss the case, arguing that the company lacked standing since Microsoft had not suffered any “concrete injury" by not being allowed to disclose further to its customers. Under current law, the DOJ argues, Microsoft can’t bring a "Fourth Amendment claim on behalf of others."

Internet Inclusion

10.02.17

Reuters
New FCC chair closely guards his strategy to restructure net neutrality

The new chairman of the U.S. Federal Communications Commission under President Donald Trump is keeping under wraps his strategy to revise or reverse the Obama administration’s “net neutrality” rules, but emphasized he is committed to ensuring an open internet.

Ajit Pai, 44, a Republican lawyer who has served as a FCC commissioner since 2012, strongly opposed former Democratic President Barack Obama administration's 2015 net neutrality rules that reclassified broadband providers and treated them like a public utility.

“I believe, as I think most Americans do, in a free and open internet and the only question is what regulatory framework best secures that,” Pai said in an interview in his FCC office, where several storage boxes remain to be unpacked. “Before the imposition of these Depression-era rules, we had for 20 years a bipartisan consensus on a regulatory model.”

In December Pai vowed to take a “weedwacker” to unneeded rules and has not backed away from his prior criticism of net neutrality, when he again said net neutrality's “days are numbered.”

The net neutrality rules bar internet access providers from slowing consumer access to web content. A federal appeals court upheld the rules last year.

Pan-Asia

Internet governance

11.02.17

The Express Tribune
Website names can now be acquired in Urdu

The country achieved a major milestone towards becoming ‘Digital Pakistan’, as users will now be able to acquire their website names and addresses in Urdu language.

“Internet Corporation for Assigned Names and Numbers (ICANN) Board has passed resolution on Internet Registry Pakistan through which the local community will be enabled to register and use internet domains in our native languages and scripts,” Federal Minster for Information and Technology, Anusha Rahman said in a statement on Friday.

ICANN is responsible for managing and coordinating the Domain Name System (DNS) to ensure that every address is unique and all internet users can find valid internet addresses.

“This is an important milestone to proliferate digitalisation in Pakistan through local content,” she said.

She lauded the efforts of her ministry team, multi-stakeholder technical committee members on internet registry Pakistan and team National Telecommunication Corporation (NTC) on achieving this major internet governance initiative.

Cybersecurity

10.02.17

India Today
India saw more than 50,300 cyber security incidents in 2016

Over 50,300 cybersecurity incidents like phishing, website intrusions and defacements, virus and denial of service attacks were observed in the country during 2016, Parliament was informed today.

“As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), a total number of 44,679, 49,455 and 50,362 cybersecurity incidents were observed during the year 2014, 2015 and 2016, respectively,” Minister of State for Electronics and IT P P Chaudhary said in a written reply to Lok Sabha.

He added that the types of cybersecurity incidents included phishing, scanning/probing, website intrusions and defacements, virus/malicious code and denial of service attacks.

“With the proliferation of Information Technology and related services, there is a rise in instances of cyber crimes in the country like elsewhere in the world,” he said.

As per the data maintained by National Crime Record Bureau (NCRB), a total of 5,693, 9,622 and 11,592 cybercrime cases were registered during the years 2013, 2014 and 2015, respectively, showing a rise of 69 per cent during 2013 to 2014 and 20 per cent during 2014 to 2015.

15.02.17

Reuters
Hong Kong police struggle to stop brokerage hacking spree

Hong Kong police are struggling to deal with digital pump-and-dump schemes targeting brokerages - a little-known type of computer-generated fraud that surged in the Chinese territory last year.

Although the money involved was small - only about $20 million worth of shares - there were 81 such incidents reported in 2016, more than triple the number in 2015, according to police.

In the scheme, criminals invest in thinly traded penny stocks and then manipulate their share prices by ordering trades from hacked brokerage accounts. They earn profits by selling before the fraudulent trades are reported.

After last year’s cyber-heist of $81 million at Bangladesh’s central bank and a series of hacks of ATM’s around the world, authorities fear such pump-and-dump schemes could be increasingly used for electronic theft.

Hong Kong is a favoured place for such attacks because of the number of thinly-traded penny stocks in the territory and because its securities industry has fallen behind other financial centres in defending against cyber fraud.

At least seven brokers and eight banks have been targeted in Hong Kong, including HSBC Holdings Plc and Bank of China International (BOCI) Securities, according to regulators and people familiar with confidential investigations.

Privacy

No new items of relevance

Internet Inclusion

09.02.17

Yibada
Alibaba Wants to Give Free Internet Access to Indians

Alibaba, through its software and Internet services arm UCWeb, is looking to offer free data to Indian consumers, Business Insider India reported.

The company is in talks with Wi-Fi providers and local telecom operators to provide such free services.

“We will definitely look at the opportunity to work together with service providers or even some Wi-Fi providers," said Jack Huang, president of overseas business at Alibaba Mobile Business.”

We are trying to offer lower cost data to users and better connectivity, even free of cost connectivity. Wi-Fi providers and other players can be potentials and we are in talk."

This is not the first time that a foreign company has attempted to offer free Internet access to Indian consumers. Facebook launched the internet.org, an initiative to enable low-cost Internet connectivity to third-world countries.

14.02.17

Gov Insider
Singapore Government partners with polytechnics to build digital skills

The Singapore Government is tapping its student pool to build and groom tech expertise.

GovTech agency yesterday signed agreements with eight polytechnics and universities to “develop the technology ecosystem” by building the “capabilities and competencies of the students”, it wrote in a press release.

GovTech will train over 300 students, and provide opportunities to learn industry skills through final-year projects, internships and attachments.

The agency will hold workshops and consultations with public sector agencies to understand the challenges faced, and reach out to institutes of higher learning, universities and research institutes for possible solutions.

“We believe that an active partnership between public agencies, academia and commercial entities can help us create the best digital services for citizens and smart solutions for our city”, said Jacqueline Poh, Chief Executive of GovTech.

The institutes of higher learning are the Institute of Technical Education; Nanyang Polytechnic; Ngee Ann Polytechnic; Republic Polytechnic; Singapore

Institute of Technology; Singapore Polytechnic; Singapore University of Technology and Design; and Temasek Polytechnic.

14.02.17

Economic Times (India)
Trai shifts deadline for Net neutrality comments to March 15

Telecom regulator Trai today extended the last date for comments on the contentious Net neutrality by a month to March 15.

Telecom operators and Internet-based companies have been at loggerheads on the issue which is linked to providing preferential access to select customers.

“On request from the stakeholders, the last date for receipt of written comments, if any, from the stakeholders has been extended up to March 15, 2017, and counter comments by March 22, 2017,” the Telecom Regulatory Authority of India said in a statement.

Earlier, the last date for comments was February 15 and counter comments February 28.

The regulator has already conducted the first round of consultation to understand key issues that need to be looked at for framing rules around Net neutrality.

14.02.17

Networks Asia
Strong demand for cyber security professionals in HK

Cybersecurity professionals top the list of IT professionals in hot demand this quarter as companies invest in developing stronger defences against cyber-attacks, according to recruiting experts Hays.

The latest Hays Quarterly Report reveals many companies are creating new headcount during the January to March quarter to bring on cybersecurity talent to bolster their defences against attacks on data integrity, big data systems and more.

“Trying to stay one step ahead of hackers and cyber crime is a crucial issue for organisations and governments the world over with major financial hubs like Hong Kong particular targets,” says Dean Stallard, Regional Director for Hays in Hong Kong.

“A company’s cyber defence capabilities are fast becoming significant factors in a range of business areas from how a company is viewed by investors, clients, insurers and potential business partners to reputation and issues management,” says Dean. “Having the best cybersecurity talent on board and retaining that talent is crucial this quarter and beyond.”

Rest of the World

Internet governance

No new items of relevance

Cybersecurity

13.02.17

The Hill
Trump, Trudeau commit to cooperation on cyber

President Trump and Canadian Prime Minister Justin Trudeau committed to working together on cybersecurity and protecting critical infrastructure on Monday.

The pledge of cyber cooperation was one of several U.S.-Canadian partnerships highlighted by the two leaders during their first meeting in Washington, D.C.

“Given the integrated nature of the infrastructure that supports our intertwined economies, cyber threats to either country can affect the other,” Trump and Trudeau said in a joint statement provided by the White House on Monday afternoon.

“We therefore commit to further cooperation to enhance critical infrastructure security, cyber incident management, public awareness, private sector engagement, and capacity building initiatives,” they said.

Trump has signaled that cybersecurity policy will be a priority of his administration, though a planned executive action on cyber rolled out in January has been delayed without explanation from the White House.

Lawmakers have paid increased attention to cybersecurity and vulnerabilities in the wake of Russia’s alleged hacking of Democratic organizations and individuals during the U.S. presidential election in an attempt to influence the outcome.

Privacy

14.02.17

Financial Review
Data breach notification laws force business cyber security revamp

Australian businesses have been warned they can no longer keep quiet about cybersecurity breaches, after the Senate passed laws mandating their disclosure 15 years after they were introduced in the US.

Under the long-anticipated Notifiable Data Breaches Bill, which passed the Senate on Monday, any organisation that is accountable to the Privacy Act will be required to inform the Australian Information Commissioner and members of the public if their data has been compromised.

This brings Australia into alignment with other countries, which have had the same requirement for years, and industry figures said it would provide Australians with greater clarity about the privacy of their personal information.

The new rules will come into effect within 12 months, and former Telstra chief information security officer Mike Burgess, who is now an independent strategic cybersecurity adviser, said he hoped the laws would lead to cybersecurity rising up the boardroom agenda.

Internet Inclusion

10.02.17

The Guardian (Nigeria)
NITDA seeks curriculum review for national ICT development

National Information Technology Development Agency (NITDA) has commenced process of engaging the National Universities Commission (NUC), the National Board for Technical Education (NBTE) and other relevant Agencies for a review of the national (educational) curriculum to incorporate courses on information and communication technologies.

The Control Objectives for Information and Related Technology (COBIT 5) National Implementation Committee inaugurated in Abuja recently is believed to be the vehicle to push for the curriculum review.

Members of the committee were drawn from various MDAs comprising of Central Bank of Nigeria (CBN), National University Commission (NUC), National Agency for Food and Drug Administration and Control (NAFDAC), Security and Exchange Commission (SEC), Nigeria Maritime Administration and Safety Agency (NIMASA), Nigeria Communication Commission (NCC), Nigeria Electricity Regulation Commission (NERC), National Environmental Standards and Regulations Enforcement Agency (NESREA).

13.02.17

BBC
UN expert calls on Cameroon to restore net services

A UN expert has called on Cameroon to restore net access to English-speaking parts of the country.

Net services in the south-west and north-west regions of the nation were cut on 17 January.

Cutting net services was an “appalling violation” of the right to freedom of expression, said UN special rapporteur David Kaye.

He said the widespread net shutdown also broke international law and he called for links to be restored.

“I am particularly concerned at the tightening of the space for free speech at a time when its promotion and protection should be of the utmost importance,”

Global Institutions

09.02.17

ENISA
Analysis of security measures deployed by e-communication providers

ENISA's new report provides a collection of good practices, implemented security measures and approaches by e-communication providers in the EU, to mitigate the main types of incidents in the telecommunication sector.

This document focuses on the security measures providers have deployed to protect networks for the provision of services, and equally important, for the personal and operational data of their customers. The report is targeted primarily at e-communication providers, and at a second level, to National Regulatory Authorities as members of ENISA's Article 13a Experts Group.

Most of the providers, report a very good level of using ENISA recommendations on security requirements, while virtually all providers have deployed a good level of basic security controls. In some security domains, the level of maturity reported, is high as well as the sophistication of implemented controls.

It is important that providers of electronic communications take the appropriate measures to address major security concerns. A key conclusion seems to be that while all IT security basics are covered, the achievement of the next level of maturity is impeded mostly by lack of sustainability mechanisms, i.e. repeatable processes and the regularly maintained documentation.

The full report is available here

09.02.17

ICANN
ICANN Free to Proceed with the Delegation of .AFRICA Following Court Decision

The Internet Corporation for Assigned Names and Numbers (ICANN) announced that a California Superior Court has denied DotConnectAfrica's (DCA's) second Motion for Preliminary Injunction to stop the delegation of the .AFRICA generic top-level domain (gTLD) to ZA Central Registry (ZACR). DCA's first Motion for Preliminary Injunction was denied by the Superior Court in December 2016.

Among other things, the Judge found that it appears the "Covenant Not to Sue" found in the New gTLDApplicant Guidebook is enforceable, citing to the recent Federal District Court Order in the Ruby Glen, LLC v ICANN matter [PDF, 62 KB], wherein the Court held that the "covenant not to sue" in the Guidebook is enforceable. Accordingly, the Superior Court Judge ruled that "DCA's claims against ICANNfor fraud and unfair business practices are likely to be barred. As a result, DCA cannot establish that it is likely to succeed on the merits."

View the Court Order here.

In accordance with the terms of its Registry Agreement with ZACR for .AFRICA, ICANN will now follow its normal processes towards delegation.

13.02.17

ICANN
ICANN Publishes "Identifier System Attack Mitigation Methodology" Document

Today, ICANN published “Identifier System Attack Mitigation Methodology” document, authoring of which commenced on 25 August 2016, as part of ICANN’s effort to contribute to enhancing the Stability, Security, and Resiliency (SSR) of the Internet's system of unique identifier by working with the Community to identify and increase awareness of related attacks and to promote broader adoption of attack mitigation practices.

View Identifier System Attack Mitigation Methodology [PDF, 876 KB] document.

This effort also addresses Recommendation #12 of the Security, Stability & Resiliency (SSR) Review.

15.02.17

Digital Europe
Europe needs more people with strong technical skills to lead innovation

On 26 January 2017, DIGITALEUROPE’s Director General John Higgins moderated a debate at the High-Tech and Leadership Skills for Europe Conference.

As Europe’s global competitiveness relies on digital innovation and transformation of businesses, there is a growing need for people who can plan and lead digital changes in enterprises and public services effectively as well as exploit the opportunities of key enabling technologies. Conservative scenarios reckon that in 2020 Europe will need 694,000 innovation leaders and 805,000 in 2025. Most of them (60%) will find positions outside IT departments. The talent shortfall puts also at risk industrial innovation driven by Key Enabling Technologies, where leaders with a mix of strong technical skills, business sense and strategic vision are crucial.

The approach to best satisfy skills supply for digital transformation points to modernising education and training, and exposing future leaders to necessary work and leadership experience.

Diary Dates

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