13 September 2017

Synopsis

Scroll to read full summaries with links to news articles.

EU Commission President **Jean-Claude Juncker** has announced a raft of new **cybersecurity** proposals as part of a significant overhaul of the EU's existing systems.

The **UK** Government has expressed its interest in continuing its cooperation with the **EU** on **cybersecurity** after it has left the EU. Specifically the UK wishes to remain a member of **ENISA**, **CSIRT** and the **NIS** cooperation group.

A new report by **Privacy International** has found that as many as 21 **EU** member states are failing to dispose of **personal data** correctly despite national and EU wide legal mandates against the rentention of such data.

In the **United States** the **National Institute of Standards and Technology** and other stakeholders have announced a series of new guidelines to help companies recover data stolen during **ransomware** attacks.

The **White House** has suggested that the **Equifax** data breach, suspected to have affected over 143 million American consumers could lead the Trump Administration to re-evaluate **data protection** regulations.

A bipartisan alliance of Senators, including former Vice-Presidential candidate **Tim Kaine** have proposed a new amendment to expand the existing federal scholarships available for **cybersecurity education**.

A new report by **PwC** has suggested that **India** needs to develop its own indigenous tools to deal with the **cybersecurity** threats facing the country.

The **Chinese** government have developed a centralised threat database for the first time, which will allow the country to more efficiently respond to **cyberattacks** in future.

Bloomberg has revealed that **South Africa's data privacy** laws are not being fully enforced as a result of understaffing at the country's Information Regulator.

ENISA have held a **cybersecurity** exercise with defence ministers from across the European Union, for the first time bringing together the **EU's** highest level cybersecurity decision makers to respond to a simulated attack.

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

For more information, visit the IEEE Internet Initiative website, and see *IEEE Global Internet Policy Monitor* past issues. Join IEEE Collabratec™ Internet Technology Policy Community discussions related to internet policy issues and to collaborate with other members of the global technical and policy communities.

IEEE Global Internet Policy Monitor

13 September 2017

Table of Contents

Europe

Internet governance

12.09.17

Computer Weekly

UK Government wants to remain in EU cyber security club after Brexit

The UK Government has expressed its interest in continuing its cooperation with the EU on cybersecurity after it has left the EU. Specifically the UK wishes to remain a member of ENISA, CSIRT and the NIS cooperation group.

"The UK government will seek to continue to collaborate in-depth with its former European Union (EU) partners on cyber security matters after Brexit.

It hopes to maintain Britain's participation in the European Union Agency for Network and Information Security's (Enisa's) Cybersecurity Incident Response Team (CSIRT) Network and Network and Information Security (NIS) Cooperation Group, according to recently released position paper on foreign policy and defence."

Cybersecurity

07.09.17

CNN

Hackers warn of flaws in German election software weeks before vote

German hackers from the Chaos Computer Club have warned that the electoral system set to be used in this year's German Federal Elections feature a number of security flaws that could be exploited by external forces.

"A German hackers' collective has warned that software used to record and transmit voting tallies in many German states has "serious flaws" and is vulnerable to external attack just weeks before voters cast their ballots in federal elections.

Hackers from the Chaos Computer Club published an analysis of the PC-Wahl software package Thursday in which they reported finding a "host of problems and security holes" that even a moderately skilled hacker -- let alone a state-sponsored team -- could exploit."

13.09.17

Euractiv

Juncker announces massive cyber security overhaul

EU Commission President Jean-Claude Juncker has announced a raft of new cybersecurity proposals as part of a significant overhaul of the EU's existing systems.

"The European Commission will add funds and new powers for the EU cyber security agency and introduce a range of measures to limit threats from hackers, Commission President Jean-Claude Juncker announced in his annual state of the union speech on Wednesday (13 September).

Cyber security attacks can be "more dangerous to the stability of democracies and economies than guns and tanks," Juncker said during his address to the European Parliament."

Privacy

07.09.17

SC Media

21 EU members not complying with court ordered privacy rules: report

A new report by Privacy International has found that as many as 21 EU member states are failing to dispose of personal data correctly despite national and EU wide legal mandates against the retention of such data.

"The global privacy advocacy group Privacy International has found that 21 European Union members continue to retain personal data despite going against both their own and EU legal mandates.

The group's research uncovered that Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, France, Germany, Hungary, Ireland, Italy, Luxembourg, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom continue hold an illegal level of personal information, which goes against the Court of Justice of the European Union's (CJEU) ruling in the Tele-2/ Watsoncase."

Internet Inclusion

No new items of relevance

United States of America

Internet governance

No new items of relevance

Cybersecurity

07.09.17

The Hill

House panel advances measure to guard U.S. ports from cyberattacks

The Homeland Security Committee in the House of Representatives has approved a number of legislative proposals that seek to improve cybersecurity at ports across the USA.

"A House panel easily advanced legislation on Thursday aimed at protecting ports in the United States from cyberattacks, in the wake of a massive malware outbreak that crippled some operations at the Port of Los Angeles.

The House Homeland Security Committee approved the bill, introduced by a California Democrat, at a meeting Thursday morning as members commended it as a step toward boosting cybersecurity of America's infrastructure."

07.09.17

SC Media

NIST develops guidelines for dealing with ransomware recovery

In the United States the National Institute of Standards and Technology and other stakeholders have announced a series of new guidelines to help companies recover data stolen during ransomware attacks.

"The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) along with vendors and businesses within the cybersecurity community teamed up to develop a recovery guide for firms hit with ransomware attacks.

Researchers said the goal of the guide is to help organizations recover data from cybersecurity events, facilitate smooth recovery in the event of a compromise, and manage enterprise risks, according to the Data Integrity Recovering from Ransomware and Other Destructive Events report."

13.09.17

The Hill

DHS bans Kaspersky software in federal agencies

The Department of Homeland Security has ordered that federal agencies end their contracts with Kaspersky Lab as part of a wider ban of the company's software and technology. The agency has vindicated its decision by highlighting its concerns for the relationship between Kaspersky employees and the Russian government.

"The Department of Homeland Security (DHS) is ordering federal agencies and departments to stop using software produced by Russian firm Kaspersky Lab, citing potential risks to U.S. national security.

The department says it's concerned about ties between certain Kaspersky employees and the Russian government."

Privacy

11.09.17

The Hill

Equifax breach could warrant new regs on personal data: White House

The White House has suggested that the Equifax data breach, suspected to have affected over 143 million American consumers could lead the Trump Administration to re-evaluate data protection regulations.

"White House press secretary Sarah Huckabee Sanders said Monday that the massive Equifax breach could warrant more regulations to protect Americans' personal data.

Sanders said the White House would look into "the best ways to make sure that Americans are protected" from breaches, days after the credit reporting firm acknowledged that as many as 143 million U.S. consumers had their personal data exposed to hackers."

Internet Inclusion

12.09.17

The Hill

Senators to offer bipartisan amendment boosting cyber scholarships

A bipartisan alliance of Senators, including former Vice-Presidential candidate Tim Kaine have proposed a new amendment to expand the existing federal scholarships available for cybersecurity education.

"A bipartisan pair of senators is introducing an amendment to annual defense policy legislation aimed at expanding an existing federal cybersecurity scholarship program.

Sens. Tim Kaine (D-Va.) and Roger Wicker (R-Miss.) are offering their Cyber Scholarship Opportunities Act, introduced earlier this year, as an amendment to the fiscal 2018 National Defense Authorization Act (NDAA), an aide to the Democratic senator said Tuesday."

Pan-Asia

Internet governance

No new items of relevance

Cybersecurity

07.09.17

The Indian Express

India needs indigenous tools for cyber security: PwC Report

A new report by PwC has suggested that India needs to develop its own indigenous tools to deal with the cybersecurity threats facing the country.

"According to the report titled "Securing the Nations Cyberspace," businesses should not limit their efforts towards cyber resilience merely for compliance, but practice self-regulation, while the government should create robust policy environment and ensure adequate technology support.

Creation of indigenous tools along with building human capacity with relevant capabilities is imperative for India's cyber security, a report by business consulting firm PricewaterhouseCoopers (PwC) in collaboration with industry chamber ASSOCHAM said on Wednesday."

13.09.17

Reuters

China beefs up cyber defenses with centralized threat database

The Chinese government have developed a centralised threat database for the first time, which will allow the country to more efficiently respond to cyberattacks in future.

"China said on Wednesday it will create a national data repository for information on cyber attacks and require telecom firms, internet companies and domain name providers to report threats to it.

The Ministry of Industry and Information Technology (MIIT) said companies and telcos as well as government bodies must share information on incidents

including Trojan malware, hardware vulnerabilities, and content linked to "malicious" IP addresses to the new platform."

13.09.17

Asia One

Indian businesses least prepared for cyber breaches despite high cybersecurity awareness: ESET Survey

The newest iteration of ESET's SMB cybersecurity survey has found that companies in India are currently most at risk to cyber attacks when compared to other ASEAN countries.

"ESET, developer of award-winning cybersecurity software, today released data from the ESET 2017 SMBs survey showing that SMBs in India were least prepared for cyber breaches in the region, despite high cybersecurity awareness among employees.

Indian SMBs experienced the highest rate of cybersecurity breaches (73%) within the past three years, the highest in the region compared to Hong Kong (61%), Singapore (54%), Thailand (53%) and Japan (29%)."

Privacy

13.09.17

Economic Times

Privacy and security needs to strike a balance: Ravi Shankar Prasad

Ravi Shankar Prasad, India's Minister for Electronics and IT has stated his intention to balance privacy with security in light of the Supreme Court's recent ruling that privacy constitutes a fundamental right.

"Saying that Aadhaar is an innovation which has been "domestically produced", union minister for electronics and IT, Ravi Shankar Prasad said on Wednesday that it kept safely and there is a need to strike a balance between privacy and security. Last month, in a landmark judgment, the Supreme Court declared privacy as a fundamental right subject to reasonable restrictions."

Internet Inclusion

No new items of relevance

Rest of the World

Internet governance

No new items of relevance

Cybersecurity

13.09.17

The Hill

DHS bans Kaspersky software in federal agencies

The Department of Homeland Security has ordered that federal agencies end their contracts with Kaspersky Lab as part of a wider ban of the company's software and technology. The agency has vindicated its decision by highlighting its concerns for the relationship between Kaspersky employees and the Russian government.

"The Department of Homeland Security (DHS) is ordering federal agencies and departments to stop using software produced by Russian firm Kaspersky Lab, citing potential risks to U.S. national security.

The department says it's concerned about ties between certain Kaspersky employees and the Russian government."

Privacy

12.09.17

Bloomberg BNA

Enforcement of South Africa's Privacy Law Miles Away

Bloomberg has revealed that South Africa's data privacy laws are not being fully enforced as a result of understaffing at the country's Information Regulator.

"Full implementation and enforcement of South Africa's 2013 privacy law remains a long way off, so companies doing business there aren't facing an imminent threat of big fines or imprisonment for violations, privacy officials and attorneys told Bloomberg BNA."

Companies could be hit with fines of up to 10 million rand ($765,405)— and up to 10 years' imprisonment of company leaders—for violating South Africa's Protection of Personal Information Act (POPI)."

Internet Inclusion

No new items of relevance

Global Institutions

08.09.17

ENISA

European defence ministers meet for cyber exercise supported by ENISA

ENISA have held a cybersecurity exercise with defence ministers from across the European Union, for the first time bringing together the EU's highest level cybersecurity decision makers to respond to a simulated attack.

"One of the main events of this Ministerial conference has been EUCybrid 2017, a high level table top cyber exercise for the EU Ministers of Defence and senior EU representatives organized by the Estonian Presidency of the EU.

ENISA supported the planning of this exercise which received positive feedback by the participants. This exercise has allowed for the first time EU decision makers to discuss on a looming crisis scenario stemming from a coordinated cyber-attack against EU military assets."

13.09.17

ENISA

European Commission proposal on a Regulation of the European Parliament and of the Council on the future of ENISA

ENISA has outlined the impact of the cybersecurity proposals announced by EU Commission President Jean-Claude Juncker in his State of the Union Speech.

"Jean-Claude Juncker in his State of the Union Speech this morning has confirmed a European Commission proposal for a Regulation on the future of ENISA called the "Cybersecurity Act".

In this context, the new proposed mandate reinforces ENISA role and enables the Agency to better support the Member States in implementing the NIS Directive and to counter particular threats more actively by becoming a centre of expertise on cybersecurity certification."

Diary Dates

ITU WTDC-17 – 09.10.17–20.10.17

Buenos Aires, Argentina

ICANN 60 – 28.10.17-03.11.17

Abu Dhabi, United Arab Emirates

IGF 2017 – 18.12.17–21.12.17

Geneva, Switzerland