23 August 2017

Synopsis

Scroll to read full summaries with links to news articles.

Ukraine's central bank has warned state and private lenders of the risk of further **malware** attacks, following an announcement by Ukrainian Security Services that the country continues to face the risk of a major **cyber attack**.

The results of the **UK** Government's latest **cyber governance** health check has found that senior management boards for UK businesses and charities require further work to protect themselves from **cyber threats**.

Following recent crackdowns on the online presence of **neo-Nazis** in the **US**, a number of leading technology companies have begun to question the role of industry in policing **internet access**.

Democratic legislators have called for an independent investigation into the **FCC's** response to a **DDOS attack** launched earlier this year, coinciding with the agency's decision to repeal Obama era **net neutrality** regulations.

Draft IT security measures from the **National Institute of Standards and Technology** have for the first time incorporated **privacy** as a core element of its guidelines, following an expansion in scope to cover **IoT** and smart devices.

The **Indian Government** have allegedly started a review of the country's **IT imports** from **China**, joining countries like Australia, the UK and the US in exercising extra scrutiny with Chinese products.

The **Phillipine Government's** Information and Communications Technology Department has launched three new projects designed to improve **internet access** in the country, through a National **Broadband** Plan and an increase in the provision of free **Wi-Fi** in public places.

TokenOne has become the first **Australian** company to be selected to work with the **USA's** National **Cybersecurity** Center of Excellence.

A new study of **IT** professionals in **Australia** has found that the industry strongly opposes the **encryption** backdoors proposed by Prime Minister Malcolm Turnbull in July.

ICANN have announced their initial dates for their public events from 2021-2023.

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

23 August 2017

Table of Contents

Synopsis 1

Europe 4
- Internet governance 4
- Cybersecurity 4
- Privacy 5
- Internet Inclusion 5

United States of America 5
- Internet governance 6
- Cybersecurity 6
- Privacy 6
- Internet Inclusion 9

Pan-Asia 9
- Internet governance 10
- Cybersecurity 10
- Privacy 10
- Internet Inclusion 11

Rest of the World 12
- Internet governance 12
- Cybersecurity 12
- Privacy 12
- Internet Inclusion 13

Global Institutions 14

Diary Dates 15

Europe

Internet governance

No new items of relevance

Cybersecurity

18.08.17

Reuters

Ukraine central bank warns of new cyber-attack risk

Ukraine's central bank has warned state and private lenders of the risk of further malware attacks, following an announcement by Ukrainian Security Services that the country continues to face the risk of a major cyber attack.

"The Ukrainian central bank said on Friday it had warned state-owned and private lenders of the appearance of new malware as security services said Ukraine faced cyber attacks like those that knocked out global systems in June.

The June 27 attack, dubbed NotPetya, took down many Ukrainian government agencies and businesses, before spreading rapidly through corporate networks of multinationals with operations or suppliers in eastern Europe."

21.08.17

Computer Weekly

Calls for UK boards to be better educated on cyber threats

The results of the UK Government's latest cyber governance health check has found that senior management boards for UK businesses and charities require further work to protect themselves from cyber threats.

"The latest government cyber governance health check and a survey of the UK's top 350 companies have revealed that more than two-thirds of boards have not received training to deal with a cyber incident, but this is no surprise, according to security commentators.

The reality that information security professionals are witnessing on a daily basis is that many organisations in the UK and worldwide are still unprepared for dealing with the impact of a cyber attack, despite increased awareness of the risk presented by cyber crime."

Privacy

21.08.17

SC Media

NHS 1.2 million patient name database hacked 'to expose weaknesses'

A data breach has affected the NHS' appointment booking system, exposing the confidential records of up to 1.2million people, though this has been refuted by the software provider.

"The NHS has suffered a data breach in its SwiftQueue appointment booking system whose database contains confidential records on up to 1.2 million people according to an exclusive report in the Sun tabloid newspaper.

The same report quotes SwiftQueue saying its database is not that big and its own initial investigation suggests only 32,501 "lines of administrative data" have been accessed, including patients' personal details, such as names, dates of birth, phone numbers and email addresses, but not patients' medical records and that passwords are encrypted."

Internet Inclusion

No new items of relevance

United States of America

Internet governance

21.08.17

CBC News

After cracking down on neo-Nazis, tech companies wonder who should police online hate

Following recent crackdowns on the online presence of neo-Nazis in the US, a number of leading technology companies have begun to question the role of industry in policing internet access.

"For more than two decades, a question with no easy answer has consumed international lawmakers, tech companies and internet users: How should we handle those who spread hate, racism and abuse online?

This long-simmering debate came to a boil this week, after white supremacist website The Daily Stormer helped organize a rally in Charlottesville, Va. that left 32-year-old counter-protester Heather Heyer dead. Its administrators spent much of the week trying to find a home online after multiple service providers declined to do business with the site."

Cybersecurity

17.08.17

The Hill

Dems want independent probe into FCC cyberattack

Democratic legislators have called for an independent investigation into the FCC's response to a DDOS attack launched earlier this year, coinciding with the agency's decision to repeal Obama era net neutrality regulations.

"Democratic lawmakers are calling for an independent investigation into how the Federal Communications Commission responded to a reported cyberattack in May that crippled the agency's comment filing system.

Sen. Brian Schatz (D-Hawaii) and Rep. Frank Pallone Jr. (D-N.J.) sent a letter to the Government Accountability Office (GAO) on Thursday that cast doubt on the FCC's version of the incident."

18.08.17

The Hill

Trump boosts US Cyber Command

The US Cyber Command is to be elevated to the status of a full combatant command, which will now lead to a review of its connection to the National Security Agency, given its heightened position.

"President Trump announced Friday he is boosting U.S. Cyber Command to a full combatant command, triggering a review of whether it should separate from the National Security Agency.

Speculation has swirled for months that Trump could elevate the command, a move that was also considered by the Obama administration."

22.08.17

The Hill

White House advisory group raises cybersecurity concerns

A report from the White House's National Infrastructure Advisory Council has argued that although the Federal Government has the resources to respond to cyber attacks, they are often prevented from doing so due to poor organisation and a lack of transparency between agencies.

"A White House advisory group says in a new report that federal agencies generally have the correct tools to protect from cyber attacks but face bureaucratic hurdles.

In its draft report circulated Tuesday, the National Infrastructure Advisory Council (NIAC) said that many of its key concerns deal with organizational woes."

23.08.17

IT Brief Australia

Sydney authentication provider to work with US National Cybersecurity Center of Excellence

TokenOne has become the first Australian company to be selected to work with the USA's National Cybersecurity Center of Excellence.

"Sydney-based cybersecurity firm TokenOne is now the first Australian company to be selected for a consortium project for the US National Cybersecurity Center of Excellence (NCCoE), alongside enterprise heavyweights such as RSA and CA Technologies.

The Multifactor Authentication (MFA) for e-Commerce project will put transaction security in the spotlight, particularly for those in retail and e-commerce industries in the US. The aim is to steer discussion away from passwords and to alternatives such as multifactor authentication."

Privacy

18.08.17

The Register

New NIST draft embeds privacy into US govt security for the first time

Draft IT security measures from the National Institute of Standards and Technology have for the first time incorporated privacy as a core element of its guidelines, following an expansion in scope to cover IoT and smart devices.

"A draft of new IT security measures by the US National Institute of Standards and Technology (NIST) has for the first time pulled privacy into its core text as well as expanded its scope to include the internet of things and smart home technology.

The proposed "Security and Privacy Controls for Information Systems and Organizations" will be the go-to set of standards and guidelines for US federal agencies and acts as a baseline for broader industry. As such, it has a huge impact on how technology is used and implemented across America."

22.08.17

The Hill

DOJ drops request for IP addresses from Trump resistance site

The Department of Justice has now recinded its request for IP addresses of protesters connected to disturbances in Washington D.C. during the Inauguration Day services for President Donald Trump.

“The Department of Justice (DOJ) is dropping its controversial request for visitor IP addresses related to an anti-Trump website.

The government said in a brief released Tuesday that it has "no interest" in the 1.3 million IP addresses related to the website disruptj20.org. It says it is solely focused on information that could constitute evidence related to criminal rioting on Inauguration Day.”

Internet Inclusion

No new items of relevance

Pan-Asia

Internet governance

No new items of relevance

Cybersecurity

19.08.17

Economic Times

India, Japan resolve to boost ties in cyberspace sector

India and Japan have announced that they will seek to further increase cooperation in digital and cyber sectors as both countries seek to improve their cybersecurity protection.

"India and Japan have resolved to strengthen their cooperation in the field of cyberspace, and reaffirmed their commitment to an open, secure and accessible cyberspace, enabling economic growth and innovation, the Ministry of External Affairs said.

The Second Japan-India Cyber Dialogue, held here on August 17, saw discussions on domestic cyber policy landscape, cyber threats and mitigation, mechanism on bilateral cooperation and possible cooperation at various international and regional forums."

22.08.17

Security Brief Australia

ShadowPad exploit 'one of the biggest' APAC supply chain attacks

The Computer Emergency Response Team of Malaysia has labelled the ShadowPad exploit to NetSarang Server Management software as a major threat to the country, as it has continued to frequently target Malaysian IP addresses over other APAC countries.

"Malaysia's Computer Emergency Response Team (MyCERT) has commented on what has been called one of the biggest known supply chain attacks which affected multiple software products in the NetSarang range.

Several recent versions of NetSarang Server Management software were compromised by the 'ShadowPad' exploit. The exploit is capable of allowing attackers to download additional malware or steal confidential business data."

22.08.17

The Hans India

India initiates review of IT imports from China

The Indian Government have allegedly started a review of the country's IT imports from China, joining countries like Australia, the UK and the US in exercising extra scrutiny with Chinese products.

"Amid the Doklam standoff, India appears to have opened a whole new front with China which could potentially escalate into a trade war. On August 16, the Ministry of Electronics and Information Technology (MeitY) initiated a review of the IT products imported from China in the wake of growing concerns over data security."

Privacy

No new items of relevance

Internet Inclusion

18.08.17

Networks Asia

Philippines announces three flagship ICT projects

The Phillipine Government's Information and Communications Technology Department has launched three new projects designed to improve internet access in the country, through a National Broadban Plan and an increase in the provision of free Wi-Fi in public places.

"In line with the National ICT Month, the Philippines' Department of Information and Communications Technology (DICT) launched its three priority projects: the National Broadband Plan, the National Government Portal and the Free Wi-Fi in Public Places on June 23, 2017."

Rest of the World

Internet governance

No new items of relevance

Cybersecurity

23.08.17

IT Brief Australia

Sydney authentication provider to work with US National Cybersecurity Center of Excellence

TokenOne has become the first Australian company to be selected to work with the USA's National Cybersecurity Center of Excellence.

"Sydney-based cybersecurity firm TokenOne is now the first Australian company to be selected for a consortium project for the US National Cybersecurity Center of Excellence (NCCoE), alongside enterprise heavyweights such as RSA and CA Technologies.

The Multifactor Authentication (MFA) for e-Commerce project will put transaction security in the spotlight, particularly for those in retail and e-commerce industries in the US. The aim is to steer discussion away from passwords and to alternatives such as multifactor authentication."

Privacy

21.08.17

Security Brief Australia

IT professionals say government-endorsed encryption backdoors are 'dangerous'

A new study of IT professionals in Australia has found that the industry strongly opposes the encryption backdoors proposed by Prime Minister Malcolm Turnbull in July.

“Venafi has announced the results of its recent survey of 296 IT security professionals on encryption backdoors.

The cybersecurity company asserts it is widely accepted that backdoors into encryption technology create vulnerabilities that can be exploited by a wide range of malicious actors, including hostile or abusive government agencies.”

Internet Inclusion

18.08.17

Hurriyet Daily News

Internet usage rises to 66.8 percent in Turkey

The Statistical Institute of Turkey has found that Turkish internet users are increasingly turning to mobile devices rather than computers, with only a 2% rise in computer usage over the last year, compared to an increase of 7% for internet usage more generally.

“Internet usage among Turks aged between 16 and 74 rose to 66.8 percent in 2017 from 61.2 percent the previous year, according to a recent Turkish Statistical Institute (TÜİK) survey on information and communication technology usage in households in 2017.

The rate of computer usage among individuals between the ages of 16 and 74 was at 56.6 percent in 2017, a rise from 58.7 the previous year, the survey carried out in April showed.”

Global Institutions

21.08.17

ITU

Last chance to enter ITU Telecom World Awards 2017

ITU have issued a reminder that the deadline for the ITU Telecom World Awards 2017 is August 30th.

"Less than two weeks remain to submit entries for ITU's high-profile international ITU Telecom World Awards 2017. The awards recognize outstanding and innovative ICT-based solutions realizing social impact. Submit your entry today at bit.ly/ITU-Telecom-Awards-2017.

First launched in 2015, as an integral component of the annual ITU Telecom World events, the awards also serve to highlight best practices and provide a platform from which to network, mobilize investment and create new business opportunities for information and communication technology (ICT) solutions."

21.08.17

ICANN

Proposed Dates for ICANN Public Meetings 2021–2023

ICANN have announced their initial dates for their public events from 2021-2023.

"ICANN has proposed dates for Public Meetings to be held in 2021, 2022, and 2023. In choosing meeting dates, ICANN took care to avoid conflicts with global, national, and religious holidays and other community events. The public comment period is an opportunity for the community to review the proposed dates, and bring any concerns or potential conflicts to our attention before we post the official meeting dates."

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