EurActiv.com EU News & Policy Debates

SPECIAL REPORT | 4 - 8 March 2013

With the support of Microsoft

CYBERSECURITY

http://www.euractiv.com/specialreport-cybersecurity

Contents

EU, US go separate ways on cybersecurity

Europe and the United States look set to implement different approaches to cybersecurity, with Washington adopting voluntary reporting mechanisms against Brussels' compulsory measures. The difference approaches threaten to create problems for companies across the two major trade blocs.

President Barack Obama on 12 February issued an executive order on cybersecurity that calls for voluntary sharing of information on cyberattacks between business and government.

This followed the failure in November of the US Senate to approve administration-backed cybersecurity legislation, amid fierce opposition from businesses complaining about over-regulation.

The abandoned legislation would have increased information-sharing between intelligence agencies and private companies, with some privacy protections. It also would have set voluntary standards for businesses that control electric grids, water treatment plants and other essential facilities.

On 27 February, White House cybersecurity coordinator Michael Daniel told reporters at the RSA security conference in San Francisco that the White House would re-submit the cybersecurity bill to Congress.

White House not giving up

Daniel acknowledged that the attempt might prove fruitless, however, saying: "I don't want to leave anybody with an impression that we underestimate the challenges."

Proposals will be brought forward in the next two months, Daniel said, but he also admitted that – if any new attempt failed in Congress – Obama would seek stronger executive measures.

The executive order directs federal authorities to improve information-sharing on cyber-threats - including some that may be classified - with companies that provide or support critical infrastructure, but the approach to reporting obligations in the private sector is overwhelmingly voluntary.

Whatever path the US goes down now looks set to be considerably more voluntary and flexible than proposed European legislation.

Alongside an over-arching Cybersecurity Strategy, the European Commission last month proposed

Continued on Page 2

Continued from Page 1

a Directive with measures to ensure harmonised network and information security across the EU.

EU rules set to be tighter, more compulsory

The proposed legislation will oblige companies to be audited for preparedness and to notify national authorities of cyber incidents with a "significant impact."

The directive also suggests that market operators will be liable regardless of whether or not they carry out the maintenance of their network internally or if they outsource it.

The EU singled out a number of sectors which it claimed require more action on cybersecurity including "critical" infrastructure operators in energy, transport, banking, and healthcare services.

Key internet companies including payment services, social networks, search engines, cloud services, apps providers, e-commerce platforms, video sharing platforms and voice-over-Internet providers were also earmarked by the EU strategy.

This raises the likelihood that the Brussels and Washington will implement differing levels of cybersecurity vigilance, threatening to create inconsistencies for companies whose operations span both jurisdictions, and posing problems for the high-profile attempt to broker a free trade deal between the two blocs.

Problems for trade deal and companies

Marietje Schaake, a Dutch liberal MEP and rapporteur for the first Digital Freedom Strategy in EU foreign policy, said: "It is also in the best interest of our citizens if companies are required to comply with the same high quality standards on both sides of the Atlantic, especially because many online services that EU-citizens use are incorporated in the US."

"The EU and the US should join hands to ensure that security and freedom will not become a zero sum game. The challenge for both the EU and the US will be to ensure sufficient democratic oversight over cybersecurity measures," Schaake added.

"Personally I think it is not realistic to divide the world once again in European firms who shall carry higher security standards than firms form other parts of the world. Why?" A senior executive with an internet-based company spanning both sides of the Atlantic asked EurActiv on condition of anonymity.

"Many leading companies are located outside the EU already and this pattern will not change quickly and definitely not because of a new European legislation," the internet executive added.

Firms see smartphones as weak link in cybersecurity

The explosion in smartphone use is leaving businesses vulnerable to cyberattacks since almost half of their employees' mobile phones can become a target, according to new research.

The 2012 Cyber Security Risk Report – published by Hewlett-Packard at the recent RSA security conference in San Francisco – found that mobile phone vulnerabilities rose significantly (68%) from 2011 to 2012, mirroring the growth of mobile applications and the use of smartphones.

Of the mobile applications tested by HP, 48% of them were found to be vulnerable to unauthorised access.

The European Council and Parliament are to consider a Commission-proposed cybersecurity strategy in the coming months. In January, the EU opened a cybercrime centre as part of a broader strategy to encourage electronic commerce.

The HP report backed up other recent studies in finding that security risks faced by businesses and governments of all sizes are complicated and increasing and that anonymous "hacktivism" is on the rise.

The findings on mobile phone risks were most pronounced, however, reflecting growing concern on the issue, evident at the Mobile World Congress in Barcelona – the largest telecommunications sector conference – which took place last week.

Risk will rise as hyper-connection increases

"With the recent reports of attacks on Microsoft, Apple, Facebook and the New York Times, it further demonstrates that everyone is a target. Mobile devices have become a lucrative asset to hackers due to BYOD ['Bring your own device'] unmanaged security," said Itzhak Avraham, chief executive of the Israeli tech security company Zimperium.

"It is estimated that 81% of employees now use at least one mobile device for their work-related tasks. This trend exposes enterprises to a host of security risks which can't be ignored, yet most organisations have not even begun to address these risks," Avraham explained.

Mobile malware jumped up 185% last year, according to the report, exposing enterprises to mounting security risks on network and data.

"If even one infected mobile device connects to your enterprise network, it could jeopardise the security of the entire network and all data. You could end up compromising the network, leading perhaps to drastic network failures and, worse, loss of confidential and

Continued on Page 3

Continued from Page 2

proprietary data," Avraham added.

US financial companies disrupted

The risk of attackers seeking entry to corporate networks through their employees devices is likely to increase sharply as cities become increasingly connected and 'big data' becomes more widely used through the use of off-site storage, or cloud computing.

Arthur Coviello, head of strategy with US network and computer security company RSA, said all threats can be reduced to one of three things: intrusions on security, attempts to destroy a piece of critical infrastructure, and disruptions. He said that disruptions are on the rise.

"In the last several months, the financial services community in the US has been under assault in distributed 'denial of services' attacks, and I think this just the first wave in disruptive attacks," said Coviello.

"As we create the internet of things, then it is going to be more facile to do attacks against critical infrastructure. When everything physical is tied back to the internet this is a very disturbing development," Coviello told delegates at the San Francisco conference last week.

"Criminals will also look at ways to generate revenue from features only mobile devices have," according to the latest Mobile security report from antivirus manufacturer McAfee.

Mobile payments pose new risks

One obvious example is mobile payments, a fast-growing sector.

At the Mobile World Congress in Barcelona, two key partnerships were announced in the mobile payments sector, pushing the issue to the forefront of industry strategy and suggesting such payments will become more prevalent over the next months.

South Korean electronics giant Samsung announced an agreement that will see it introduce Visa's payment technology on its next generation of handsets, and Canadian handset maker BlackBerry announced its instant-messaging service, BBM, will have person-to-person payments added to its capabilities in a pilot.

"We anticipate more fraud-oriented malware in 2013. One likely innovative content swindle will abuse the tap-and-pay near field communications [NFC] technology used in mobile payment programs, or 'digital wallets'," according to the McAfee report.

"When the newly infected device is used to "tap and pay" for the next purchase, the scammer collects the details of the wallet account and secretly reuses these credentials to steal from the wallet," it explained.

Fears about phones reflect European report

A report by the European Network and Information Security Agency (ENISA) published in January also said that cyberattackers are set to target smartphones and social media increasingly over the next year.

The ENISA Threat Landscape report provides an overview of risks, together with current and emerging trends, based on analysis of over 120 recent reports by the security industry, standardisation bodies and other institutions.

The report identified emerging threats for the next year, and claimed that mobile phones will come under increased risk, since communications over them is often less secure than conventional computer systems.

Security reports say EU needs more ‘honeypots’ to lure cyberattackers

European computer emergency response teams, which are being beefed up as part of the EU’s cybersecurity strategy, need to set more ‘honeypot’ traps to snare cyber attackers, according to reports.

Two internal memoranda drafted last month by the European Network and Information Security Agency (ENISA) said that the response teams, or CERTS, are not spreading their detection nets as widely as possible and are failing fully to share their information with one another.

In computer terminology, a honeypot is a trap set to detect or deflect attempts at unauthorised use of information systems.

Generally it consists of a computer, data, or a network site that appears to be part of a network, but is actually isolated and monitored, and which seems to contain information or a resource of value to attackers.

It therefore lulls in attackers and then records who they are and is able to monitor their activities.

More CERTs

The establishment of CERTs in every EU member state was one of the first responses to cybersecurity by the EU executive. More than 100 CERTs have now been set up around Europe, including those focusing on the private sector and the EU executive has established its own dedicated team.

These are now being beefed up as part of the Commission’s cybersecurity strategy and ENISA will encourage further CERTs to be set up, with additional efforts being made to create networks binding the public and private sector.

Two reports completed by ENISA last month highlighted shortcomings in CERTS operations and recommended new methods of operation.

In “Proactive Detection of Network Security Incidents”, ENISA identified 16 shortcomings in the process of detection of incidents including problems with data quality, slow delivery, lack of contextual information.

The report also claimed that data privacy rules might be hampering the activities of CERTS, saying: “The most important legal problem involves privacy regulations and data protection laws that often hinder the exchange of information – an obstacle faced by CERTS but unfortunately not by miscreants responsible for network attacks.”

Luring hackers with honeypots

A separate report, also published by ENISA in February looked at the CERTs use of ‘honeypot’ traps.

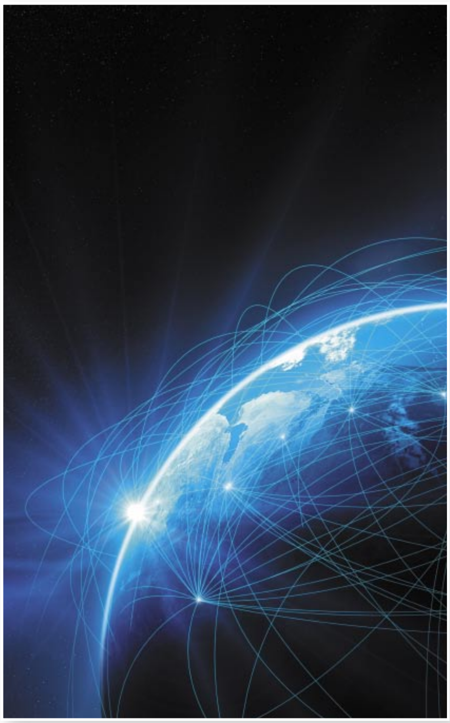
The report said that these traps offer “great insights into malicious activity in a CERT’s constituency, providing early warning of malware infections, new exploits, vulnerabilities and malware behaviour as well as an excellent opportunity to learn about changes in attacker tactics.”

To combat the increasing cyber threat, the report says: “CERTs need to cooperate and develop large-scale inter-connected sensor networks in order to collect threat intelligence from multiple distributed geographic areas.”

CERTs and honeypot researchers should work more closely together, the report recommended.

Cybersecurity directive faces uncertain fate in Parliament

EU attempts to introduce comprehensive new cybersecurity rules risk failure in the European Parliament, where senior administrators doubt the package will pass before the legislature's mandate expires, EurActiv has learned.



In addition to the launch of its new over-arching Cybersecurity Strategy, the European Commission last month proposed a Directive with measures to ensure harmonised network and information security across the EU.

The proposed legislation will oblige companies to be audited for preparedness and to notify national authorities of cyber incidents with a "significant impact."

The directive also suggests that market operators will be liable regardless of whether or not they carry out the maintenance of their network internally or if they outsource it.

The EU singled out a number of sectors which it claimed require more action on cybersecurity including "critical" infrastructure operators in energy, transport, banking and healthcare services.

Parliamentary manouevering

Key internet companies including payment services, social networks, search engines, cloud services, apps providers, e-commerce platforms, video sharing platforms and voice-over-Internet providers were also earmarked by the EU strategy.

The Commission has sent the proposal to the Parliament, where it is awaiting distribution amongst the committees likely to play a key role in the debate.

These include committees for Civil Liberties, Justice and Home Affairs, for Industry Research and Energy, for the Internal Market and Consumer Protection and for Legal Affairs.

Which committee should lead the process remains to be decided, whilst rapporteurs and shadow rapporteurs – the MEPs responsible for the content of committee reports – will also need to be appointed.

The mandate of the current Parliament expires next year, and with elections set for May 2014, MEPs are likely to cease considering legislative matters weeks before as they prepare to canvass for votes.

Parliamentary sources told EurActiv that the body has already signalled to the Commission that it will not be in a position to manage the debate of new legislative measures proposed by the EU executive after April this year.

Paper is complicated, controversial

That puts the cybersecurity directive in a precarious position as it is a complicated paper requiring scrutiny from the different political groups.

One key issue is the extent to which the private sector will be compelled to make official notifications indicating when they have been cyberattacked under the new rules.

This issue marks a clear line of difference between the levels of cybersecurity vigilance the EU and United States aim to implement, since the US is likely to opt for a much more voluntary approach to such notifications.

"The European Parliament will have a very close look on the Commission's proposal and we will carefully elaborate the impact of the directive. Ensuring the security of our citizens, granting shareholder as well as consumer protection will be at the core of the discussions in the coming months," said German MEP Christian Ehler (European People's Party), a member of the committee on industry research and energy.

Race against time

Two senior administrators in the Parliament, speaking on condition of anonymity, doubted the body would be able to conclude deliberations before its mandate finishes next year.

"It is complex, and even deciding who should take the lead on the process is clearly not going to be easy," said one.

Even if the Parliamentary process works at top speed, negotiations with the Council and the Commission are likely to be "extremely difficult", another administrator said.

"The Commission will also be coming to the end of its mandate, and political pressures between the EU executive and the Parliament will make the atmosphere less amenable," he added.

If the legislation fails to pass the Parliament, a fresh proposal may be needed since "only legislation which has reached an advanced stage of agreement can usually be held over for the next elected Parliament to consider," one administrator said.

That would mean a considerable delay to Europe's adoption of harmonised cybersecurity measures.

Cybersecurity offers commercial opportunity, but also stokes trade tensions

The European Commission wants new cybersecurity rules to spur industrial growth by turning Europe into a showcase for lucrative security products, but the use of cybersecurity as a proxy for protectionism is also stymieing trade.

The European Commission last month launched its over-arching Cybersecurity Strategy, including measures to ensure harmonised network and information security across the EU.

Whilst consultations were under way on this last June the EU executive simultaneously launched an action plan for the security industry.

The programme intends to empower the industry to stay in Europe and to continue producing high quality security products.

The Commission action plan includes proposals to harmonise standards and certification procedures for security technologies and exploit synergies between security and defence research.

Next month the EU executive is organising workshops in Ispra, Warsaw and Edinburgh, to set roadmaps for standardisation in the general security sector as part of the action plan.

The current fragmented market weakens the competitiveness of Europe's security industry, said European Commission Vice President Antonio Tajani, responsible for enterprise and entrepreneurship.

"This lack of an "EU brand" is especially critical as the future key markets for security technologies will not be in Europe but in emerging countries," Tajani said.

Standisation under way

Talks are under way behind the scenes to agree standardisation on cybersecurity issues too, as a part of the plan, according to industry sources.

The EU security industry is valued between €26 billion and €36.5 billion with around 180,000 employees. It includes the manufacture of counter-terror intelligence and crisis management products, both of which include strong cyber security and communication.

European companies are still among the world leaders in the majority of the security sector's market segments.

The strategy also aims to strengthen cooperation between the public and private sectors, encourage the development of public-private partnerships, and take advantage of other initiatives, such as the European Public-Private Partnership for Resilience (EP3R).

UK-India seal deal on cybersecurity

Meanwhile, cybersecurity remains a key issue in trade negotiations involving member states and the EU executive.

An agreement between the UK and India signed last month (25 February) paved the way for close co-operation between the two countries on cybersecurity including creating a joint task force to exchange and share information about identifying and countering threats.

In addition to academic and security cooperation, however, the deal heralded greater use of offshoring and outsourcing of UK state information and communications technology (ICT) work to India, acting as a lubricant for trade between the two nations.

Cybersecurity is also acting as a block on trade, however. Chinese companies have been frozen out of public contracts with US public authorities on national security grounds, details of which remain hazy.

Meanwhile Hibernia – a network cable provider – has reportedly delayed work on a new trans-Atlantic submarine cable, called Project Express, over cybersecurity issues.

US service providers allegedly said they would not be able to use the network over concerns that they would lose contracts with their federal government customers, because Hibernia was working with Chinese partner companies.

For information on EurActiv Special Reports...

Contact us

Delia Nicolaescu
events@euractiv.com
tel. +32(0)2 788 36 72

Ross Melzer
publicaffairs@euractiv.com
tel. +32(0)2 226 58 17

Other relevant contacts:

Rick Zedník
ceo@euractiv.com
tel. +32(0)2 226 58 12

Frédéric Simon
executiveeditor@euractiv.com
tel. +32(0)2 788 36 78