NEW EU CYBER STRATEGY AIMS TO CUT CRIME AND RAISE RESILIENCE

-

20.09.2017

Deutsche Welle (19 September 2017)

The European Commission has said it will upgrade its existing cyber agency as part of an effort to add EU-wide standards to boost resilience against increasing online aggression. But will the plan work?

There are more than 4,000 ransomware attacks every day Europe-wide, according to the European Commission, with 80 percent of European companieshaving experienced at least one cybersecurity "incident." The cost of these intrusions? An estimated 265 billion euros ($318 billion) per year.

Introducing the new package of initiatives on Tuesday, European Commission Vice President Andrus Ansip made it sound even more dramatic than that. "There are two types of companies," Ansip quipped. "Those that were cyberattacked and those that don't know yet that they were attacked."

Ansip, along with fellow commissioners on security, Julian King, and digital affairs, Mariya Gabriel, detailed the plan to improve EU citizens' and companies' abilities to fight back against web-based exploitation by upgrading the EU's existing cybersecurity agency and encouraging even certifying – companies to improve their own defenses.

King pointed out the EU has had a "cybersecurity strategy" since 2013, but that the increase in attacks especially with ransomware like WannaCry makes clear the bloc's resilience, deterrence and defense policies are not up to par.

"Better late than never," Piret Pernik, a research fellow in cybersecurity at Tallinn's International Centre for Defence and Security (ICDS), told DW. She applauded the commission's proposal to turn the current European Agency for Network and Information Security (ENISA), whose mandate would otherwise end in 2020, into a permanent structure. Its annual budget will be doubled to 23 million euros, with staff increased from 84 to 125 people.

Safety in sharing

"I think it is a step in the right direction," Pernik said, "by, among other things, establishing information-sharing and analysis centers in critical sectors, organizing annual exercises" and supporting the implementation of other information-security directives.

That said, the commission's call to speed up information sharing may not bear fruit, as governments and businesses are always reluctant to do so, and Pernik believes there's no way

around having to change the thinking on this. "I think that we should stop speaking about the need to share information," she said, "and determine modalities of information exchange, working out how that information will be used in order to prevent cybersecurity incidents and respond in a timely manner."

Certification scheme gets mixed reviews

With the aim of prevention, another tenet of the plan involves creating a "Cybersecurity Certification Framework," which will set out EU-wide technical standards and national authorities will recognize those companies that meet them.

Pernik commended the intention to apply the scheme to consumer devices as well as to critical infrastructure relating to finance, energy and transport, and to defense capabilities, where she thinks the certification program should be mandatory, not voluntary as envisioned.

The Software Alliance, BSA, takes a different, albeit preliminary, view. "We believe that a certification framework will only work if it is based on international standards along with being voluntary, consensus-based, and industry-led," BSA Policy Director Thomas Boue told DW. He recommends the envisioned certification schemes "should be enabled through market-driven incentives rather than through legislation, shaping insurance markets or legal liability. Such an approach would have the unintended consequence of impeding flexible, outcome-oriented standards."

The group, which represents a wide range of industry giants including Apple, IBM, Microsoft and Siemens, warned that if Europe opts only for regional standards, "it will not effectively address the shortcomings and vulnerabilities of a fragmented approach to cyber threats."

Half of German companies hit by cybercrime

Threat perceptions, responses need harmonization

EU defense ministers tested those vulnerabilities last week in Tallinn when they conducted their first "tabletop exercise," a simulation of a hacker attack on the bloc's naval mission in the Mediterranean. One of the basic but complicated questions posed to the ministers was how the imaginary situation should be treated: as an "attack," an "incident" or a "threat."

Pernik says the great variation in answers to questions like that adds another layer of difficulty to an already "cumbersome" potential EU response. "A cybersecurity incident that in one member state would be considered as a use of force that could trigger a collective response or even kinetic countermeasures may be considered in another member state as 'business as usual,'" she explained. She hopes the new EU strategy will improve that.

BSA's Boue echoes that call. "Europe must present a united front by harmonizing and streamlining its approach, not only within the EU, but, more importantly, also at a global level," he said. "Without working together and sharing information on threats and how to mitigate them, Europe will not achieve the cyber resilience that it is seeking to reach."

Raj Samani, Chief Scientist and Fellow at cybersecurity firm McAfee, said there is already a model for good public-private cooperation with Europol's European CyberCrime Centre (EC3), set up in 2013 to battle and prosecute online crime. "Such initiatives as demonstrated by [EC3] show how collaborative efforts between public and private sectors can begin to address the global

cyberattacks by establishing relationships with expertise across the globe," he told DW. "Any measures that promote better security are to be applauded, in particular the incorporation of initiatives to support collaboration is integral toward the development of a safer society."

Kaynak/Source: