Cyber Observatory Report May 2024

A review of significant recent developments relating to the cyber domain.

3 May 2024: Statement by the High Representative on behalf of the EU on continued malicious behaviour in cyberspace by the Russian Federation

The European Union and its Member States, together with international partners, strongly condemn the malicious cyber campaign conducted by the Russia-controlled Advanced Persistent Threat Actor 28 (APT28) against Germany and Czechia. Today, Germany has shared publicly its assessment on APT28 compromise of various e-mail accounts of the German Social Democratic Party executive. At the same time, Czechia announced its institutions have been a target of this cyber campaign. State institutions, agencies and entities in Member States, including in Poland, Lithuania, Slovakia and Sweden have been targeted by the same threat actor before. In 2020, the EU imposed sanctions on individuals and entities responsible for the APT28 attacks targeting the German Federal Parliament in 2015.

The malicious cyber campaign shows Russia's continuous pattern of irresponsible behaviour in cyberspace, by targeting democratic institutions, government entities and critical infrastructure providers across the European Union and beyond. This type of behaviour is contrary to the UN norms of responsible state behaviour in cyberspace, such as impairing the use and operation of critical infrastructure. Disregarding international security and stability, Russia has repeatedly leveraged APT28 to conduct malicious cyber activities against the EU, its Member States and international partners, most notably Ukraine.

The EU will not tolerate such malicious behaviour, particularly activities that aim to degrade our critical infrastructure, weaken societal cohesion and influence democratic processes, mindful of this year's elections in the EU and in more than 60 countries around the world. The EU and its Member States will continue to cooperate with our international partners to promote an open, free, stable and secure cyberspace. The EU is determined to make use of the full spectrum of measures to prevent, deter and respond to Russia's malicious behaviour in cyberspace.

06 Mar 24: EU Cyber Solidarity Act

To strengthen EU's solidarity and capacities to detect, prepare for and respond to cybersecurity threats and incidents and enhance its cyber resilience, the Council presidency and European Parliament's negotiators reached a provisional agreement on the so-called 'cyber solidarity act', as well as on a targeted amendment to the cybersecurity act (CSA).

"Today's agreements set new milestones for Europe's cyber resilience. These rules will strengthen the EU's and member states' capabilities to prepare, prevent, respond, and recover from large-scale cyber threats or incidents. Moreover, creating the possibility for the certification of managed security services will help to ensure a high common level of these cybersecurity services across the EU by facilitating their cross-border provision to the benefit of our citizens and businesses."

Mathieu Michel, Belgian Secretary of State for digitisation, administrative simplification, privacy protection and the building regulation

Main elements of the cyber solidarity act

The new regulation establishes EU capabilities to make Europe more resilient and reactive in front of cyber threats, while strengthening cooperation mechanisms. It mainly aims to:

- support detection and awareness of significant or large-scale cybersecurity threats and incidents
- bolster preparedness and protect critical entities and essential services, such as hospital and public utilities
- strengthen solidarity at EU level, concerted crisis management and response capabilities across member states
- contribute to ensuring a safe and secure digital landscape for citizens and businesses

To detect major cyber threats quickly and effectively, the new regulation establishes a 'cyber security alert system', which is a pan-European infrastructure composed of national and cross-border cyber hubs across the EU. These are entities in charge of sharing information and tasked with detecting and acting on cyber threats. They will strengthen the existing European framework and in turn, authorities and relevant entities will be able to respond more efficiently and effectively to major incidents.

The new regulation also provides for the creation of a cybersecurity emergency mechanism to increase preparedness and enhance incident response capabilities in the EU. It will support:

- preparedness actions, including testing entities in highly critical sectors (healthcare, transport, energy, etc.) for potential vulnerabilities, based on common risk scenarios and methodologies
- a new EU cybersecurity reserve consisting of incident response services from the private sector ready to intervene at the request of a member state or EU institutions, bodies, and agencies as well as associated third countries in case of a significant or large-scale cybersecurity incident
- mutual assistance in financial terms

Finally, the new regulation establishes an evaluation and review mechanism to assess, amongst others, the effectiveness of the actions under the cyber emergency mechanism and the use of the cyber security reserve, as well as the contribution of this regulation to strengthening the competitive position of the industry and service sectors.

The targeted amendment to the cybersecurity act of 2019

This targeted amendment aims to enhance EU's cyber resilience by enabling the future adoption of European certification schemes for 'managed security services'. Managed security services, provided to customers by specialised companies, are crucial for the prevention, detection, response, and recovery

from cybersecurity incidents. They can consist of, for example, incident handling, penetration testing, security audits, and consulting related to technical support.

The amendment will enable the establishment of European certification schemes for managed security services. It will help to increase their quality and comparability, foster the emergence of trusted cybersecurity service providers, and avoid fragmentation of the internal market given that some member states have already started the adoption of national certification schemes for managed security services. Awaiting the regular review of the CSA, due by 28 June 2024, the provisional agreement:

- clarifies the definition of 'managed security services' and ensures alignment with the revised network information systems ('NIS 2') directive

- aligns the security objectives of these certification schemes with the security objectives of other schemes under the current CSA regulation

- includes modifications in the annex to the CSA, which contains a list of requirements to be met by conformity assessment bodies

- specifies that ENISA's consultation of all relevant actors should be carried in a timely manner and provides a possibility for quarterly briefings by ENISA or by the Commission to the co-legislators on the functioning of the certification schemes.

Comment / Background

On 18 April 2023, the Commission adopted the proposal for a regulation laying down measures to strengthen solidarity and capacities in the EU to detect, prepare for and respond to cybersecurity threats and incidents, the so-called 'Cyber solidarity act'.

The origin of such a legislative proposal is multiple. The EU cybersecurity strategy adopted in December 2020 mentioned the creation of a European cyber shield, reinforcing the cyber threat detection and information sharing capabilities in the EU. On 8 and 9 March 2022, ministers of EU member states in charge of telecommunications met informally in Nevers and expressed the wish for the EU to fully prepare to face large-scale cyberattacks. The Council conclusions of May 2022 on the cyber posture highlighted the need to address gaps in terms of response and preparedness to cyber-attacks, by calling for the Commission to present a proposal on a new emergency response fund for cybersecurity.

The Commission proposal therefore introduces a 'European cyber shield', composed of operations centres (SOCs), and brought together in several multi-country SOC platforms financed by the Digital Europe programme. The total budget for all actions under the EU cyber solidarity act is of EUR 1.1 billion, of which about 2/3 will be financed by the EU through the Digital Europe programme.

NPW 06 05 24