The Cyber Security Package

Policy Brief

May 2023

Summary: The EU strives to have an open, secure and stable cyberspace which works to the benefit of its citizens and businesses. This Cyber Security Package announced in April 2023 consists of the proposed Cyber Solidarity Act, the Cyber Security Skills Academy and a targeted amendment to the Cybersecurity Act.

Key Words: ***Cybersecurity, resilience, Cybersecurity Reserve, trusted private companies***

Introduction

The EU strives to have an open, secure and stable cyberspace which works to the benefit of its citizens and businesses. However, the EU has been subject to an increased frequency and serious cybersecurity incidents which are exacerbated by the geopolitical tensions at the EU's borders.

Through this package, it is aimed to continue to build on the existent strategic, policy and legislative frameworks by enhancing the capacity for the detection of cyber threats, in making the EU better prepared and more resilient to threats. Existent policy frameworks include the Directive on measures for a high common level of cybersecurity across the Union (NIS 2) and the Cybersecurity Act.

This so-called Cyber Security Package consists of:

1. The Cyber Solidarity Act
2. The Cyber Security Skills Academy and

3. A targeted amendment to the Cybersecurity Act - the certification schemes for ‘managed security services'

The Cyber Solidarity Act

This Act aims to strengthen the EU’s cyber resilience. The EU aims to do so by emphasising cybersecurity which includes risk assessments for potential vulnerabilities and monitoring actions taken in advance. It aims to do so in a coordinated manner across the Member States by providing the latter with the support for testing and assessing entities operating in highly critical sectors. The sectors or subsectors will be selected at the EU level to ensure coordinated action. Sectors which are not deemed as highly critical will be supported through various types of other national preparedness activities.

The EU Cyber Solidarity Act includes a series of actions to strengthen solidarity and enhance coordinated EU detection and situational awareness to threats. It also aims to support Member States' preparedness and response capabilities to significant or large-scale cybersecurity incidents, through:

1. The European Cyber Shield

The Shield will constitute of a pan-European infrastructure of Security Operation Centers (SOCs) whose purpose is to build and enhance coordinated detection and situational awareness capabilities by analysing, detecting, preventing and cyber threats, as well as producing high-quality intelligence on cyber threats. National SOCs will be public bodies designated by Member States and artificial intelligence and advanced data analytics are be utilised as tools. The European Cyber Shield will consist of several cross-border SOC platforms, with each platform grouping national SOCs from at least three Member States. The European Cyber Shield will complement the work of existing SOCs, Computer Security Incident Response Teams (CSIRTs), and other relevant actors.

2. The Cybersecurity Emergency Mechanism

This mechanism aims to support Member States in preparing for and responding to large-scale cybersecurity incidents. It complements national resources and other forms of support available at the Union level. The mechanism includes preparedness actions to identify and address potential vulnerabilities in critical sectors and sub-sectors. It also provides support for incident response and recovery from significant and large-scale cybersecurity incidents through the EU Cybersecurity Reserve. Additionally, the mechanism allows for mutual assistance between national authorities when a Member State dispatches experts to assist another Member State in mitigating a cybersecurity incident.

Trusted private providers which are private companies will offer services such as incident analysis and coordination. Their role would be to provide managed security services, such as incident analysis or incident response coordination services. The mechanism establishes that these companies are to be ready and can be mobilized to support Member States in case of significant and large-scale cybersecurity incidents affecting entities covered by the NIS2

Directive. The providers will be selected in a procurement procedure and the selection criteria are also listed in the Cyber Solidarity Act.

3. The Cybersecurity Incident Review Mechanism

The second mechanism within this act, aims to review and assess significant or large-scale incidents. The European Union Agency for Cybersecurity (ENISA) according to the Act will be requested to review and assesses a specific potential, ongoing or large-scale cybersecurity incident. When reviewing and assessing a specific incident, ENISA shall collaborate with relevant stakeholders, including representatives from the private sector, Member States and the Commission. ENISA will also consult managed security services providers, entities affected by cybersecurity incidents, and other relevant entities. ENISA's reports shall address main causes and vulnerabilities of cybersecurity incidents, as well as lessons learned and, where appropriate, recommendations to improve Union's cyber posture.

Cyber Security Skills Academy

This Cyber Security Package also includes a Commission proposal for the Academy which will initially be a European digital infrastructure consortium. The Cybersecurity Skills Academy aims to increase the visibility of cybersecurity skills initiatives and to help boost the numbers of skilled cybersecurity professionals in the EU to tackle the gap in cybersecurity professionals across the Member States. The Academy will:

- Work towards increasing the number of cybersecurity professionals in Europe by launching a pilot project to set up a European attestation system for cybersecurity skills.
- Ensure a better channelling and visibility of the available funding opportunities for cybersecurity skills-related activities to maximise their impact.
- Call on stakeholders (e.g., companies, schools, universities and authorities) to take action by making concrete pledges to initiate specific actions, such as to offer cybersecurity trainings and certifications, as well as integrating cybersecurity skills into their strategies.
- Define indicators to monitor the evolution on the job market to ensure timely adaption of trainings and curricula to the market needs.

The Commission will create a single point of entry to the Academy through the Digital Skills and Jobs Platform, giving access to relevant information, activities and stakeholders within the scope of the Academy. Initially, the Academy will gather existing education and training opportunities and give them visibility on the Digital Skills and Jobs Platform.

Targeted Amendment to the Cyber Security Act

In April 2023, the Commission proposed a targeted amendment to the EU Cyber Security Act.

This aims to enable, by means of Commission implementing acts, the adoption of European cybersecurity certification schemes for 'managed security services'[1], in addition to

[1] Managed security services, which are services consisting of carrying out, or providing assistance for, activities relating to their customers' cybersecurity risk management.

information and technology (ICT) products, ICT services and ICT processes, which are already covered under the Cybersecurity Act. There was a need to such an amendment given that managed security services play an increasingly important role in the prevention and mitigation of cybersecurity incidents.

This proposal aims to improve the quality of managed security services and to increase their comparability. It thereby enables essential and important entities to exercise the increased diligence in selecting a managed security service provider as required under Directive (EU) 2022/2555. Moreover, the definition of 'managed security services' in this proposal is derived from the definition in Directive (EU) 2022/2555 and thus the proposal is highly complementary with the NIS 2 Directive. Finally, this proposal is complementary with the proposed Cyber Solidarity Act. Future certification schemes for managed security services will play a significant role in the implementation of the Cyber Solidarity Act.

Cyber Security in Malta

Businesses in Malta, similar to their European counterparts face a range of cybersecurity threats, including malware, phishing, social engineering, ransomware, and denial-of-service attacks. As a framework, Malta has developed a National Cyber Security Strategy (NCSS) which outlines the country's priorities for cybersecurity.

Currently, Malta also has The National Cyber Security Strategy 2023-2026 which focuses on the need to have Government and society prepared and resilient. The strategy also outlines that there is a need for cyber security to be addressed on a national scale with a planned, collective and systemic effort from all stakeholders. The National Cyber Security Strategy 2023-2026 follows an initial one published in 2016, which laid the foundation blocks for such an approach in Malta. The principles outlined in this Strategy need to be put into practice by the Maltese public administration, the private sector and all Maltese society including a community of cyber security experts and practitioners.

Malta has also established The National Cyber Security Coordination centre which among other things works to actively support the implementation and upkeep of the National Cyber Security Strategy, in collaboration with national and international stakeholders; and to ensure the alignment of communications relayed by MITA with respect to Information Security matters.

Link to more information

Proposed Regulation on the Cyber Solidarity Act

Commission communication on the Cybersecurity Skills Academy

Proposed Regulation on 'managed security services' amendment

For questions or more detailed information please contact EU Affairs Manager Daniel Debono and Policy Executive Christine Said on infobrussels@mbb.org.mt

The Malta Business Bureau is the EU business advisory organisation of;

THE MALTA CHAMBER

MALTA HOTELS & RESTAURANTS ASSOCIATION

and a partner of the Enterprise Europe Network;

enterprise europe network

Business Support on Your Doorstep