EDA Live Cyber Exercise for Military CERTs in its Second Edition

WRITTEN BY GABRIELA-CORINA TANASA

The second live-fire cyber exercise of the European Defence Agency (EDA), specifically dedicated to improving European cooperation between member states' national military Computer Emergency Response Teams (CERTs) has reached and concluded its second edition in the last days of January 2022. Even though European countries have established mechanisms and processes to exchange information between civilians of the CERTs over time, cooperation and communication channels are much less developed in the military domain due to the high sensitivity of the information. Therefore, many stakeholders have decided to extend the information sharing practices used in civilian circles to military CERT and their operations. Through this Info flash, we will briefly investigate the birth of this project, the two editions carried out and conclude with a perspective on the future.

Introducing the new EU Cybersecurity Strategy: towards increasing cooperation among the member states

In December 2020, the Commission unveiled the new EU Cybersecurity Strategy. Its goals are bolstering Europe's collective resilience against cyber threats, and allowing the EU to step up leadership on international norms and standards in cyberspace and to strengthen cooperation with partners around the world to promote a global, open, stable, and secure cyberspace, which is grounded in the rule of law, human rights, fundamental freedoms and democratic values.

The EU MilCERT Interoperability Conference 2021

In this respect, the European Defence Agency (EDA) organised the EU MilCERT Interoperability Conference in 2021(MIC) to improve European cooperation between member states' national Military Computer Emergency Response Teams (MilCERTs). The MIC sought to establish a permanent forum for discussing information sharing within the EU Network of MilCERTs. Its aspirations were, in fact, creating a more detailed understanding of the challenges and ultimately laying the groundwork to improve information-sharing without undermining the strategic importance of classification.

The EU MilCERT Interoperability Conference 2021 was organised in two tracks: technical and strategic. The first technical track took place on 16/18 February 2021 and focused on a 3-days cyber defence live-fire exercise, intending to establish a collaboration channel between technical teams of the interested member states. The exercise brought up more than 200 experts from 17 EDA member states and Switzerland, all of them connecting remotely from their working locations. The objective of the first-ever live-fire exercise was to bring together military CERTs and observe incident management dynamics with a particular focus on information-sharing, a key factor in modern cyber defence. In fact, while European countries have come a long way in establishing mechanisms and processes to exchange information between civilian CERTs, such cooperation and communication channels are much less developed in the military domain, also due to the high sensitivity of the information. Therefore, many stakeholders have expressed the need to extend the information sharing practices used in civilian circles also to military CERTs and their operations.

Based on these assumptions, the exercise goal was to experience and observe the dynamics of incident response during realistic live-fire cyber-attacks and identify gaps and opportunities for improvement. The operational environment created for the exercise was based on advanced Cyber Range technology, with professional attackers based in several member states launching live cyberattacks against infrastructure defended by teams from the other member states. This exercise was specifically designed for military CERTs. It included platforms, tools, and technology specific to the military domain, while the entire exercise scenario was conceived in such a way that it used military planning and strategy similar to what is used in real cyber military operations. In addition, to create a realistic scenario, the intent was to push participants out of their comfort zone, asking them to use all tools, processes and procedures possible, even those not directly at hand in the exercise platform.

The second part of the event took place in June 2021and focused on the lessons learnt from the practical exercise and discussed more strategic topics. The strategic track of the second part followed up on the practical part and addressed the heads of the Computer Emergency Response Teams with strategic topics. It consisted of several online events, with keynotes delivered by high-profile stakeholders, interactive incidents, and discussions between the participants. It aimed to build confidence and foster cooperation and information sharing.

Second EDA Live Cyber Exercise for Military CERTs

EDA's second live-fire cyber exercise for military CERTs took place in January 2022, with the exercise kicking off the technical track of the 2022 edition of the EU MilCERT Interoperability Conference. The second phase of it is scheduled to take place in June when the lessons learnt from the exercise and more strategic topics will be discussed with senior military leaders and decision-makers. Opening the exercise, EDA Chief Executive, Jiří Šedivý affirmed, "last year's MIC was the first step to start closing the gap of the absence of a milCERT network with the 2022 edition being a second step in what for sure will be a long journey". Again, the operational environment designed for the exercise was based on the advanced Cyber Range technology, with professional attackers from both the military and industry launching live cyberattacks against infrastructure defended by teams from other member states. The exercise tested fictional cyber-attacks, pitting, and attacking (red) teams against defending (blue) ones. The entire exercise scenario was conceived to use military planning and strategy similar to what is used in real cyber military operations. At the end of the exercise, Finland was awarded overall winner of the 2022 MIC technical track while Hungary (task solving), Austria (situational report) and Italy (information sharing) won for specific categories.

Looking forward

To date, EDA's cyber activities range from defining key priorities at the E.U. level looking at the capability development, R&T and industrial dimensions, including initiatives supporting cyber defence training, education and exercises. To build on the benefits and lessons of the MIC, EDA envisages the possibility of establishing an EU milCERT Operational Network as a new ad hoc project within the Agency, with the member states currently invited to signal their interest in participation. For filling in the gap identified in the E.U. Cyber Defence Policy Framework and the E.U. Cybersecurity Strategy, the project will provide a solution to identify, develop and sustain the establishment of a network of MilCERT, which will facilitate the exchange of information and foster a stronger response to cyber incidents.

Bibliography

EU Commission. "New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient". Press release, December 16, 2020 [online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391. [accessed on February 8, 2022]

European Defence Agency. "Cyber defence exercise brings together military CERTs". European Defence Agency, February 19, 2021 [online]. Available at: https://eda.europa.eu/news-and-events/news/2021/02/19/cyber-defence-exercise-brings-together-military-certs. [accessed on February 8, 2022]

European Defence Agency. "MilCERT Interoperability Conference talks strategy". June 8, 2021 [online]. Available at: https://eda.europa.eu/news-and-events/news/2021/06/08/milcert-interoperability-conference-talks-strategy [accessed on February 8, 2022]

European Defence Agency. "Second EDA Live Cyber Exercise for Military CERTs Concluded". January 26, 2022 [online]. Available at: https://eda.europa.eu/news-and-events/news/2022/01/26/second-eda-live-cyber-exercise-for-military-certs-concluded. [accessed on February 9, 2022]