APPROVED
by Order No. 1-79 of the Director of
NCSC under the MND
of 8 December 2021

PUBLIC REPORT OF THE NATIONAL CYBERSECURITY EXERCISE "CYBER SHIELD 2021"

KIBERNETINIS SKYDAS 2021

TLP: WHITE

Content

1. SUMMARY

The National Cyber Security Centre under the Ministry of National Defence (hereinafter referred to as the NCSC), in cooperation with Kaunas University of Technology, organised an annual national cybersecurity exercise, "Cyber Shield 2021" (hereinafter referred to as the Exercise), on 19-21 October 2021. The aim of the Exercise was to develop the practical cybersecurity skills of participants in the exercise, to verify cyber incident management procedures, and to improve cooperation among cybersecurity entities and the authorities managing and/or investigating cyber incidents.

In total, more than 670 people from 92 organisations participated in the Exercise. The majority of the organisations involved in the Exercise, 87 organisations, are managers or handlers of state information resources or critical information resources. Compared to the previous year, the number of managers or handlers of state information resources or critical information resources participating in the Exercise increased by 35% (64 such participants in 2020). However, 87 organisations represent only 21.7% of all managers or handlers of state information resources or critical information resources, so the number of participants this year was insufficient to achieve the 60% target (200 organisations) specified in the Strategic Action Plan for the years 2021–2023 for the areas overseen by the Minister of National Defence, approved by Order No. V-187 of the Minister of National Defence of 17 March 2021.

The most popular story lines (hereinafter referred to as the SL) chosen by the participating organisations concerned incidents involving Windows workstations (SL1 and SL2) and the sending of fake letters (SL7). The more frequent selection of SL1 is likely due to the activity of the Emotet malware in recent years, and the more frequent selection of SL2 is likely due to organisations' concerns about the risks accompanying the need to organise work remotely due to the Covid-19 pandemic. SL7 allowed organisations to realistically evaluate the resilience of personnel to fake (*phishing*) emails.

For the first time, the coordination meeting for the management of a dangerous incident, as provided for in the National Cyber Incident Management Plan, was held during the Exercise. The Exercise's strategic scenario gameplay showed that due to the location of infrastructure abroad, the NCSC would have limited capacity to assume the management of cyber incidents, and such management would be based on coordination among the responsible CSIRT services in different countries. The coordination meeting also came to the conclusion that in order to have reliable access to state or other electronic services, users need to have more than one authentication method.

The lessons identified in the Exercise have been documented and will be evaluated during the process of improving cybersecurity regulation.

96% of the local trainers agreed that the Exercise had been useful for their organisation.

2. REFERENCES

A. Law on Cyber Security of the Republic of Lithuania (No. XII-1428 of 11 December 2014).

B. Resolution No. 818 of the Government of the Republic of Lithuania of 13 August 2018, "On implementation of the Law on Cyber Security of the Republic of Lithuania".

C. Resolution No. 709 of the Government of the Republic of Lithuania of 3 July 2019, "On approval of the inter-institutional plan for implementation of the national cybersecurity strategy".

D. Order of the Minister of National Defence of the Republic of Lithuania, "On approval of the Strategic Action Plan 2021-2023 for the areas overseen by the Minister of National Defence of the Republic of Lithuania".

3. INTRODUCTION

The National Cyber Security Centre under the Ministry of National Defence (hereinafter referred to as the NCSC), in cooperation with Kaunas University of Technology (KTU), organised an annual national cybersecurity exercise, "Cyber Shield 2021" (hereinafter referred to as the Exercise), on 19–21 October 2021. The preparation of national cybersecurity exercises is provided for in resolutions of the Government of the Republic of Lithuania and in an order of the Minister of National Defence of the Republic of Lithuania (references B, C, D).

This report aims to present to the public, Exercise participants and senior management the concept and course of the Exercise, the results achieved and the feedback received from participants. The statistics presented in the report can also serve as a useful input for future assessment of progress in developing the practical cybersecurity skills of information infrastructure managers.

4. INVOLVEMENT OF CYBERSECURITY ENTITIES

Cybersecurity entities managing and/or handling state information resources, critical information infrastructure managers, providers of public communications networks and/or public electronic communications services, electronic information hosting services and digital services (collectively referred to as cybersecurity entities, abbreviated CSE), as well as authorities managing and/or investigating cyber incidents and the authorities coordinating the management of a dangerous cyber incident, were invited to participate in the Exercise. In addition, the NCSC invited organisations belonging to the Association of Lithuanian Banks as well as other organisations to participate in the Exercise. All participants in the Exercise are collectively referred to below as the Exercise audience.

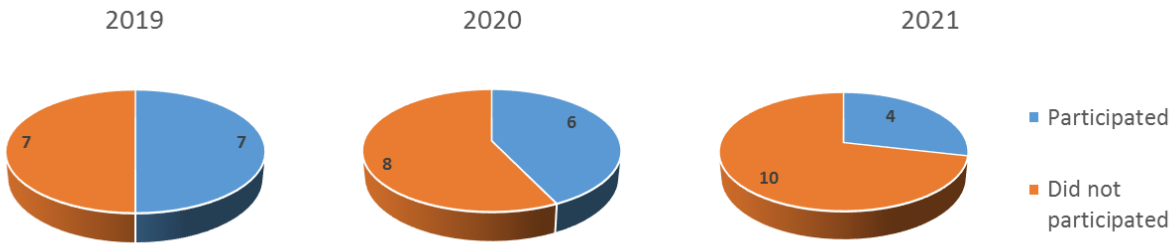
A total of more than 670 people from 92 organisations participated in the Exercise (760 people from 73 organisations participated in Cyber Shield 2020). 87 of the participating organisations are state information resources managers and critical information resources managers or handlers (the number in Cyber Shield 2020 was 64). The majority of the organisations participating in the Exercise were state institutions (ministries and subordinate

bodies). Health care institutions, energy companies, financial institutions, universities and other organisations also participated.

The number of participants in the Exercise was insufficient to reach the assessment criteria set out in the Strategic Action Plan for 2021–2023 for areas overseen by the Minister of National Defence, approved by Order No. V-187 of the Minister of National Defence of 17 March 2021. Criterion R-02-01-03-04, "4. Percentage of critical information infrastructure managers and state information infrastructure managers and state information resources managers participating in national cybersecurity exercises", was set at 60 %, but in fact only reached 21.7%. (The percentage of participants in Cyber Shield 2020 was 19.8%). Criterion P-02-01-03-06-03, "3. Number of critical information infrastructure managers and state information resources managers and/or handlers participating in national cybersecurity exercises", was set at 200, but in fact only reached 87. (The number in Cyber Shield 2020 was 64).

For example, only four of the 14 ministries of the Republic of Lithuania participated, that is, 29%. Given the low level of involvement of ministries, their subordinate bodies also choose not to participate in the Exercise. In order to meet the established criterion, it is necessary to find ways to encourage CSE to participate in national cybersecurity exercises in the future.

Participation of ministries of the Republic of Lithuania in the exercise "Cyber Shield":



5. AIM AND OBJECTIVES OF THE EXERCISE

Aim of the Exercise

Improving the practical cybersecurity skills of participants in the Exercise.

Exercise objectives

(1) Verify and train the capacity of authorities managing and/or investigating cyber incidents and of CSE to carry out the actions set out in the Cyber Incident Management Plan; identify areas for improvement in the Cyber Incident Management Plan.

(2) Verify the internal cyber incident management procedures of authorities managing and/or investigating cyber incidents and of CSE.

(3) Train the Exercise audience to detect and analyse cyber incidents.

(4) Train the Exercise audience to share cyber incident information, improve cooperation, use the services of the Cyber Security Information Network.

6. CONCEPT OF THE EXERCISE

In organizing Cyber Shield 2021, the NATO cyber defence exercise Cyber Coalition was used as a model. One of its main principles is *to train as you fight*. The aim was for the Exercise to take place in an environment that is as close as possible to the everyday environment of the Exercise audience. In other words, the organisation had to participate using the capacity, personnel and procedures that it actually has. Temporary staff structures specifically designed for exercises, which do not exist on a regular basis, were not formed, equipment specifically designed for use in exercises was not purchased. The Exercise took place on the premises of the organisations, staff participated from their everyday workstations, managed incidents, and investigated using the tools they ordinarily have at their disposal, in accordance with their everyday procedures.

Local trainers at their own discretion chose the degree of involvement of their organisation, which had to investigate and manage the cyber incidents prepared by the Exercise organisers. Depending on this choice, the organisation's structure and its procedures, the local trainer had to adapt the typical Exercise scenario to the trainer's organisation.

Cyber incidents were carried out in the infrastructure for the Exercise prepared by Kaunas University of Technology (KTU), and artefacts were presented to participants (images of work stations, servers and mobile phones as well as logs, pcap and NetFlow data). Information about events and incidents in the Exercise space was provided by the local trainer to the Exercise audience by email. Participants assumed that cyber incidents were occurring in their organisation's IT infrastructure.

7. EXERCISE EVENTS AND PARTICIPANTS

An invitation to participate in the Exercise and to designate a representative of their organisation (a local trainer) was sent by the NCSC to 401 managers and handlers of critical information infrastructure and state information resources.

A total of 195 organisations responded to the NCSC invitation and designated a representative (a local trainer) for Exercise planning.

The majority of organisations which had expressed an intention to participate in the Exercise but subsequently ceased to participate in the preparations did not inform the Exercise organisers of their decision. Those organisations which informed the Exercise organisers about their decision to cease participating in the preparations usually identified obstacles caused by the COVID-19 pandemic as the reason for their decision.

In March and June, Exercise planning conferences were organised online for local trainers. Three scenario-writing conferences were held in September. These events presented the typical Exercise scenario and cyber incidents, and explained the responsibilities of the local trainer and the work required during the preparation of the Exercise. Local trainers adapted the typical Exercise scenario to their organisation.

The Exercise was followed by trainings for cybersecurity practitioners who had taken part in the Exercise. 400 specialists from the CSE registered for the trainings, and during the trainings it was demonstrated how cyber incidents developed for the Cyber Shield 2021 Exercise could be investigated.

A total of 92 organisations participated in the Exercise on 19-21 October. According to a survey completed by 86 local trainers, an average of 8 staff members from the organisation (median: 6 employees) participated in the cyber incident management Exercise, including not only cybersecurity professionals and IT administrators, but also public-relations professionals, lawyers, and top and mid-level managers.

8. EXERCISE SCENARIO

The scenario prepared for the Exercise consisted of 7 parts, the story lines (hereinafter SL). The local trainers, taking into account the relevance of the SL and the organisation's objectives, selected the SL in which the organisation would participate. The local trainer adapted the selected SL to the organisation's structure, procedures and needs. The following SL were prepared for the Exercise:

1. A fake (phishing) email with a malicious attachment gives access to a workspace at the organisation.

2. When a USB flash drive is connected to a laptop, files containing employees' personal data are leaked.

3. Hacking into a Windows IIS server. Placement of a phishing webpage on the organisation's website.

4. Hacking into a Windows RDP server as a user. Privileges escalation. *Active Directory* data leakage.

5. Hacking into a Linux web server by exploiting a plug-in vulnerability. Leakage of a database.

6. After installing a malicious app on a mobile phone (*Android*), photos are leaked.

7. The local trainer sends phishing emails to the staff of the organisation with an attached Excel file, from which a macro initiates contact with a server registering events during the Exercise, or sends emails with a link, which when clicked on contacts a server registering events during the Exercise. The opening of the Excel file with the enabling macro and the opening of the link is logged on the server registering events during the Exercise. These events, illustrating the level of cybersecurity awareness of staff, are given to the local trainer for further assessment.

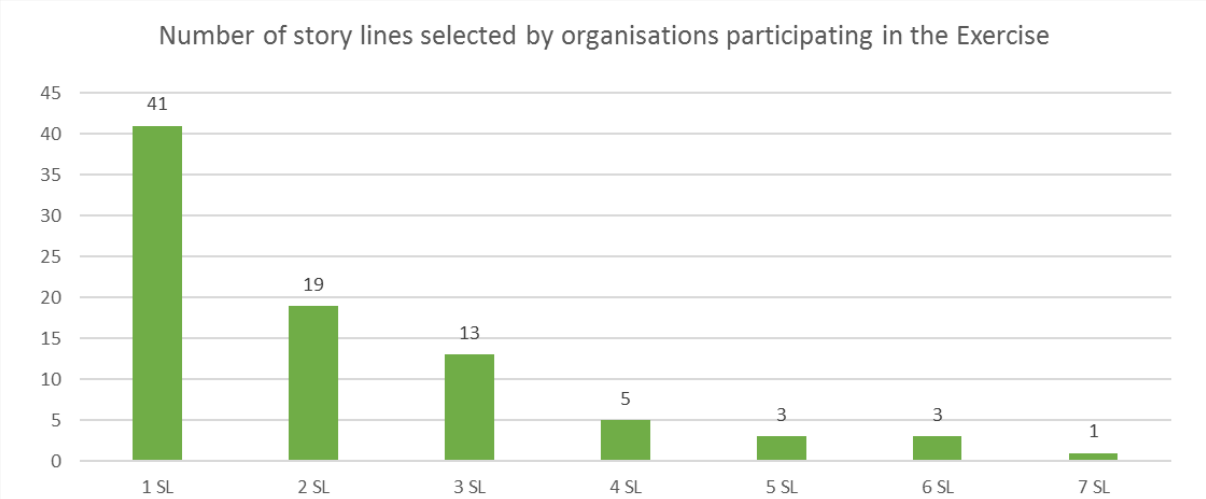
For all SL, technical artefacts were prepared, which participants could investigate and, in accordance with the internal procedures of the organization, submit the results of their investigation to their organisation's security staff, which in turn had to inform the NCSC, the State Data Protection Inspectorate and the Police.

Examples of emails for all SL were also provided, which local trainers could use to initiate the management and investigation of cyber incidents within their organisations.

Local trainers mostly selected Exercise story lines related to incidents involving Windows workstations (SL1 and SL2) and sending fake emails (SL7). The choice to manage the SL1 incident is likely a consequence of the Emotet virus activity observed in recent years, which this SL simulates. The choice of SL2 could have been motivated by organisations' concerns about the risks associated with the need to organise work remotely during the Covid-19

pandemic. SL7 gave local trainers the opportunity under realistic conditions to check the resilience of the organisation's staff to phishing emails. Local trainers sent more than 12,000 such emails to employees in their organisation, the opening of which was logged on the Exercise server. The Exercise organisers are not in a position to provide precise statistics on the opening of the links or attachments contained in such emails, but the partial data provided by local trainers suggests that users' resistance to attacks of this type is poor.

Explanation: 57 organisations selected SL1 , 28 organisations selected SL2, etc.



Explanation: 41 organisations participated in one SL, 19 organizations participated in two SLs, etc.

The role of the media was actively simulated during the Exercise. Personnel of the 8th Territorial Unit of the National Defence Volunteer Forces of the Lithuanian Armed Forces performed this function during the Exercise, calling the organisations managing the cyber incident and requesting information of interest to the public.

9. STRATEGIC-LEVEL SCENARIO

For the first time, the Exercise included a strategic-level scenario. According to the scenario, one of the banks operating in Lithuania suffered a large-scale cyber attack, which makes electronic banking services unavailable to the bank's clients. Simultaneously, provision of the

State's e-services to the bank's customers was also disrupted, because most customers use e-banking to authenticate their identity when accessing such State-provided e-services.

To manage this incident, the NCSC convened a coordination meeting, making use of its right to do so in accordance with the Cyber Incident Management Plan.

The gameplay of the strategic-level scenario revealed that, due to the location of infrastructure in other countries, the NCSC would have limited capacity to take over the management of cyber incidents, and that the management of the incident would be based on coordination among the responsible CSIRT services in different countries.

The coordination meeting also concluded that in order to have reliable access to State or other electronic services, users need to have more than one method for authentication of identity.

The lessons identified in both the coordination meeting and in the rest of the Exercise have been documented and will be evaluated during the process of improving cybersecurity regulation.