Report of the State Comptroller of Israel | March 2022

Cyber Security

Cyber Security in the Israel Electric Corporation Ltd.

Cyber Security in the Israel Electric Corporation Ltd.

Background

Cyberspace includes computers, mechanized systems and networks, software, computerized data, digital content, and traffic and control data. A cyberattack is a sequence of actions performed by an adversary in cyberspace. With the growth of cyberspace, cyber threats are ever-increasing and could lead to harm in both cyberspace and the physical world, such as in power stations and production lines. This damage could cause economic harm as well as physical injuries and fatalities. In recent years the level of the stated threat gradually increased, in both the frequency of events and their severity, in Israel and worldwide. Israel Electric Corporation Ltd. (IEC) generates, transmits, and supplies the electricity. IEC is in charge of some of the most critical infrastructure in Israel. Damage to the Information and communication technology (ICT) systems supporting the generation, transformation, transmission, and distribution processes might shut them down and disrupt the regular supply of electric power for periods that may be critical for the economy, especially in times of emergency.

Key figures

USD 100 million

the insurance policy limit for coverage of cyberattack damage in 2021, with the deductibles of millions of USD

NIS 527 million

execution of IT budget in the IEC in 2019. In 2018, budget execution totaled NIS 521 million

19%

employees number reduction in the ICT division in the years 2015–2019

Audit actions

From May to December 2020, the State Comptroller's Office audited cyber security in the IEC and the activities of the IEC and the Israel National Cyber Directorate (INCD) to improve the cyber security of critical processes and systems in the Electric Corporation. The audits were performed in IEC, INCD, and the Ministry of Energy.

The report was submitted to the Prime Minister and the Knesset's State Control Committee on 29.07.2021, with the duty of confidentiality imposed on it until discussion in the subcommittee of the State Control Committee.

By the authority given to the State Comptroller's Office under Section 17(c) of the State Comptroller Law 1958 [Consolidated Version], after considering the government's arguments, consulting with the protection of national security information bodies, and coordinating with the Chairman of the Knesset, and as the stated subcommittee failed to convene, it was decided to publish this report while imposing confidentiality on sections of it. These sections shall not be submitted to the Knesset, nor shall they be published.

The findings of the audit and its recommendations are valid as of the completion of the above audit.

Key findings

Uniformity of the guiding body and guidance in the energy sector – according to the division of work between INCD and the Ministry of Energy, IEC power stations sold to private entrepreneurs were transferred from INCD guidance to Ministry of Energy guidance, according to the regulation determined by the Ministry of Energy (professionally guided by INCD). When comparing the guidance provided by INCD to IEC and guidance provided by the Ministry of Energy to the private producers, several differences were found.

Supervision and tracking by INCD of the implementation of guidelines given to the Electric Corporation – it was found that INCD did not regulate the IEC's reports to enable it to track the implementation of its guidelines and rectify the deficiencies it raised. It was found that INCD has not fully tracked and supervised the implementation of all its guidelines by the IEC. Regarding some of the guidelines the INCD presented to

the State Comptroller audit team, INCD stated that it received no information written or verbal regarding the guidance status.

- **Preparation of multi-annual and annual work plans for implementation of INCD guidelines (assimilation plans)** – as of the audit end date, the IEC did not submit a multi-year plan, and the annual work plans it presented for 2019–2021 did not include full details regarding their implementation.

- **Performing risk analyses and penetration tests** – from IEC documents, it was raised that in July 2019, it did not form a multi-annual or annual plan for performing risk analyses and penetration tests. In practice, gaps arose regarding performing risk analyses and penetration tests. Nevertheless, in May 2020, IEC prepared a triennial work plan for performing risk analyses and penetration tests.

- **Separation of system operator unit from the IEC as part of the reform** – at the audit end date, IEC had not completed its plan for separation of the system operator unit from IEC regarding cyber aspects, nor had it submitted such a plan to INCD. This, even though at the audit end date, in June 2021, the system operator unit was supposed to move to the system operator company.

Establishment of a cybernetic center – the Ministry of Energy has established the Sectorial Cybernetic Center, which monitors all energy infrastructure, coordinates data received from it, and presents a status update concerning the cyber security of the energy economy.

This report examined additional topics, such as the level of resilience, intra-organizational security policy, work plans, annual and multi-annual assimilation, and cyber security and information protection controls. The findings were communicated to the relevant parties.

Key recommendations

- It is recommended that the INCD, as a regulator, will regulate procedures for reporting and control of the IEC. Including written reports regarding the rectifications of deficiencies raised by the INCD or by others in external or internal audits and the accompanying explanations required in the reporting. In addition, it is recommended that the INCD set a timetable for submitting the above written reports, including periodic and immediate reports, and the details IEC is required to provide in its reports. It is further recommended that INCD receive information from IEC regularly concerning implementing all its previous years' guidelines and that INCD establishes an online reporting and control system for IEC and all organizations under its guidance.

IEC is recommended to prepare a detailed multi-annual work plan in the cyber field according to the work order on the matter, including all necessary details. Furthermore, it is recommended that IEC prepare detailed annual plans as stated.

Summary

The Israel Electric Corporation is in charge of critical national infrastructure. The compromise of the electric power supply might damage the Israeli economy. The report contains deficiencies in the Electric Corporation's cyber security. This report has presented the status report concerning cyber security in the Israel Electric Corporation and oversight thereof by the INCD. Among other things, deficiencies were found in INCD's tracking of the implementation of its guidelines.