March 14, 2022

Russia / Ukraine war – Cyber Impacts

Dear Sebastian,
Following our discussion, I am happy to share additional information provided by the Israeli national cyber CERT:

The Israeli cyber CERT is in contact with the German Ministry of Finance, working on scenarios for financial leadership at the country level.
The State of Israel and the Ministry of Finance recently led such an exercise - ten foreign finance ministries, including the United States and England, participated as observers, including the Central Bank and the World Bank, and in this exercise, Germany was very active.

Simulations and exercises that corresponded to the Russia/Ukraine crisis were performed.
As a result, the level of alertness of the Israeli Cyber CERT has increased.
Currently, we are at the stage of conducting situation and status assessments in Israel. We have raised the issue with attention and are conducting ongoing assessments, and we are sharing general information broadly between the two countries.

Because Germany is dependent on Russian energy sources, Germany is on the Russian target. For example, the wind energy farms used for electricity generation in Germany were attacked by Russian hackers.
An attack was conducted on a server network (Modems) connected to the Internet via satellite. Physical replacement of the devices was required at all stations. Consequently, most wind turbines in Germany could not be controlled!
We are not seeing attacks on the financial system yet, but as time progresses, we will begin to see these as well, and due to the move to the Chinese Swift, attacks on the financial system are also expected to be more frequent and intense.

Please also read this:
https://www.reuters.com/markets/europe/exclusive-imf-10-countries-simulate-cyber-attack-global-financial-system-2021-12-09/

As of now, the situation is being handled at the country level with the assistance of the Israeli national cyber CERT.

Gil Arazi