
Steinitz: Israel's Electric Authority hit by 'severe' cyber-attack

Some computers shut down since Monday, says energy minister; ministry and cyber authority 'handling it,' but problem not yet solved

BY TIMES OF ISRAEL STAFF | January 26, 2016, 10:05 pm |

Israel's Electric Authority is currently being targeted by a "severe cyber-attack," Energy Minister Yuval Steinitz said Tuesday, adding that steps are being taken to counter the assault.

Addressing the Cybertech Conference in Tel Aviv, Steinitz said the attack was discovered on Monday, and that his ministry was "already handling it," along with the Israel National Cyber Bureau.

"The virus was already identified and the right software was already prepared to neutralize it," he said. "We had to paralyze many of the computers of the Israeli Electricity Authority. We are handling the situation and I hope that soon, this very serious event will be over ... but as of now, computer systems are still not working as they should."

"This is a fresh example of the sensitivity of infrastructure to cyberattacks, and the importance of preparing ourselves in order to defend ourselves against such attacks," he said.

Steinitz did not say whether Israel has identified any suspects behind the attack.

The Electricity Authority is a department in the Ministry of Energy, and is a separate entity to the Israel Electric Corporation, the country's state-owned utility company.

In mid-July, the Israel's [National Cyber Authority](#) warned that the country would be targeted by a massive cyberattack.

Government ministries and security agencies were alerted to look for any changes in their computer systems, and security officials were instructed to prepare for "any possible scenario," the Israeli daily Haaretz reported.

The warning went into effect immediately and included computer systems and cellular phones, according to the report.

Over the last two years, Israel has been targeted by a number of cyberattacks. Officials estimated hackers affiliated with Hezbollah and the Iranian government were behind the infiltration attempts.

In April, members of the Anonymous hacking group [defaced dozens of Israeli websites](#) in what it warned would be an "electronic holocaust." Dubbed OplIsrael, the anti-Israel hackers targeted websites of the Israeli government and organizations, Facebook pages and gained access to

personal emails. The annual attacks have thus far not caused disruption of Internet services in Israel, and failed to bring down any major governmental websites.

In response, Israel has invested resources to streamline its offensive and defensive cyber capabilities, and announced last month the [establishment of a new IDF corps](#) responsible for all such cyber activity.

Israel has also become a center of cybersecurity research and development, with multinationals from the US, Europe and Asia setting up R&D labs to develop better and more effective cyberdefense strategies and technologies.

Israeli cybersecurity firms are said to export \$3 billion in knowledge, services and solutions each year, developing many of the technologies the world will need in the coming years to protect banks, infrastructure and government servers.

© 2015 THE TIMES OF ISRAEL, ALL RIGHTS RESERVED