Is Latvia facing cyber warfare? What are we supposed to do? 1/30/24

Director, IT Consulting, PwC Latvia
Dr.dat. Baiba Apine

Dr.dat. Baiba Apine, CISA, PMP, Director, PwC Latvia IT Consulting
Photo: Gatis Dieziņš, Ministry of Defence, Republic of Latvia

The media have been actively using the term 'cyber warfare'. At this year's 'Lampa' Conversation Festival, I took part in 'Are we ready for cyber warfare?', a discussion held by the Ministry of Defence. At the moment we are unable to draw a clear line between the kind of cyber warfare that calls for a military response and the sort of cyber warfare that qualifies as an attack under the Criminal Code. Yet cyber warfare is definitely going on in Latvia and companies should be monitoring their cyber security carefully.

In its 2023 report, CERT.LV finds that following Russia's full-scale invasion of Ukraine in 2022, DDoS attacks on Latvia as well as other EU and NATO member states are commonly run by groups of hacktivists associated with Russia. Their activities are probably coordinated and financed to achieve Russia's domestic and foreign policy goals. Whether successful or not, these attacks are being widely advertised as a big success, because the Internet tolerates anything.

Companies are typically unable to tell if the cyber attacker is a military hacktivist or an ordinary fraudster – any attack should be treated as a crime.

From 2019 to spring 2023, I headed up the council of Oschadbank, a national bank, the second largest in Ukraine, a universal bank serving businesses and individuals across all channels. The bank experienced warfare involving extremely powerful cyber attacks on 15 February. We knew the world was planning to launch sanctions, and we called for those to begin. Yet we did not succeed because cyber warfare is not visible. It's designed to wreak havoc and facilitate land warfare. The type of hacktivist attacks changed quite rapidly: the autumn 2022 saw a resurgence of fraudsters and thieves, according to the regulator. If land warfare drags on, it's difficult to finance powerful cyber warfare.

Latvian companies should be ready to continue working under cyber warfare conditions. I suggest a simple list of minimum steps:

1. You have a centralised architecture of corporate information systems in place, with data stored centrally.
2. Your data and software have backups. Your IT professionals have tried restoring your systems from backups at least once.
3. You need a clearly defined group of critical staff for work in a crisis situation, and they need to be aware of their business continuity role.
4. You need to get rid of any accounting software, geospatial information processing software, etc. developed and maintained in Russia or Belarus.

PwC's IT professionals are happy to examine your corporate IT infrastructure and governance for threats to business continuity, to devise a precise action plan for risk mitigation, and to ensure your investment in cyber security is optimal.