Government of the Netherlands

Grapperhaus: growing digital threat to the Netherlands gives cause for concern

News item | 29-06-2020 | 10:13

Once again, the National Coordinator for Security and Counterterrorism (NCTV)'s annual Cyber Security Assessment Netherlands (CSAN) paints a worrying picture. In the view of the NCTV, cybercrime incidents have the potential to cause significant damage and even social disruption in extreme cases.

> “
> ‘It should hardly come as a surprise that the digital threat to the Netherlands has not diminished. Although we have so far been spared, it is conceivable that cyberattacks or large-scale outages will cause disruption in the Netherlands. For instance, ransomware attacks continue to be an attractive earnings model for criminals. It therefore remains as important as ever that we increase our resilience against digital threats as well as tackle cybercrime more broadly. This demands our permanent vigilance.’

according to Minister of Justice and Security Ferd Grapperhaus.

Preventing social disruption

Preventing social disruption caused by incidents affecting critical processes is at the top of the National Cyber Security Agenda. The government is working on an ‘apply or explain’ approach for critical providers and the national government. Once adopted, these organisations will have to apply measures to address serious vulnerabilities or explain their reasons for not doing so. If a situation similar to the issues affecting the Citrix software arises, organisations will be compelled to take action.

Improving the exchange of threat information

To protect themselves adequately against cybercrime incidents and outages, organisations must have access to timely and accurate threat information. As revealed in the CSAN, there are signs that hostile nation-state actors have abused the COVID-19 pandemic to carry out cyberattacks on sites such as hospitals, pharmaceutical companies and research centres. For this reason, the government has introduced emergency legislation to direct the National Cyber Security Centre (NCSC) to assist these organisations in the event of digital threats and incidents during the pandemic.

Digital dependence

The threat posed by cybercrime to Dutch businesses and citizens remains unrelenting, particularly now that the coronavirus has led to an increased dependence on digital technology. Examples include working from home, taking courses online and more frequent orders from web shops. The coronavirus has shown once more that hostile nation-state actors and criminals will not hesitate to respond quickly to developments in society and abuse this increased dependence. In 2019, the police and the Public Prosecution Service launched a joint approach to supraregional cybercrime phenomena.

Prevention and information activities will continue, for example in the form of campaigns organised jointly by the government and private-sector parties.

See also

- National Coordinator for Security and Counterterrorism (NCTV)
- Cybercrime
- Coronavirus COVID-19

Ministry responsible

- Ministry of Justice and Security