DUTCH
SAFETY BOARD

Press release

The Hague, 16 December 2021

Fundamental intervention is needed to ensure Dutch digital safety and security

The Netherlands' approach to digital safety and security needs to change rapidly and fundamentally to prevent Dutch society from being disrupted by cyber-attacks. This is the conclusion reached by the Dutch Safety Board in its report '*Vulnerable through software'* published today. The Board investigated security breaches that occurred in thousands of organizations due to vulnerabilities in Citrix software. Jeroen Dijsselbloem, Chairman of the Dutch Safety Board, commented, "These incidents show that Dutch government organizations and businesses are highly vulnerable to cyber-attacks. They highlight the lack of a national structure capable of alerting all potential victims of cyber-attacks in a timely manner."

Attacks via Citrix

On 17 December 2019, Citrix disclosed a vulnerability in its software and took temporary measures to mitigate the risks. But before the thousands of organizations using Citrix could be made aware of the acute risks and install the temporary measures, attackers had penetrated some systems. The National Cyber Security Centre (NCSC) issued a direct alert to the Dutch national government and vital operators, for which it considers itself responsible. Other organizations and the wider business community were not alerted directly by the NCSC, leaving the attackers free to infiltrate digital systems on a large scale. To this day, attackers have illegal access to systems and data in organizations. They can use this capability at any time to disrupt business processes and services, and affect privacy and security.

Manufacturers' responsibility

Secure software is primarily the responsibility of the manufacturer. The Dutch Safety Board argues that manufacturers should invest greater resources on a more continuous basis to improve software security. At present, manufacturers inundate software users with patches and updates to fix flaws in their software without coming up with structural solutions. There are no instruments to provide software purchasers with independent insights into the security of the product they are buying. In addition, customers often lack the expertise and power to demand more secure software from the manufacturers. Some customers do not recognize the importance of doing so.

Limited government approach

As things stand, early warning systems do not reach all organizations that use software and are therefore potential victims of cyber-attacks. The NCSC sees no legal mandate for itself in terms of warning organizations beyond national government and vital operators. The Dutch Safety Board believes it is essential that the government should adopt a centralized approach to identifying threats and issuing quick and direct warnings to all potential cyber-attack victims, backed by a sufficient mandate and legal safeguards.

Contact
Spokesperson: Simone Klein Haneveld +31 6 86 65 46 59
E-mail: press@safetyboard.nl Website: safetyboard.nl Twitter: @onderzoeksraad

Recommendations of the Dutch Safety Board
Society is becoming increasingly dependent on digital systems. Manufacturers, governments and organizations will have to work together to come up with an effective approach that will make the Netherlands more resilient to cybercrime. This requires manufacturers to improve the security of their software on a fundamental and continuous basis. The Dutch Safety Board recommends that software quality requirements be set at a European level to compel software manufacturers to take responsibility for the security of their products. The Board advises the relevant government bodies and the business community to join forces. By working together, they can strengthen their position in relation to the software manufacturers and make better use of their limited expertise.

Within government, the monitoring of digital safety and security can be regulated in the same way as the monitoring of prudent fiscal policy as laid down in relevant legislature. Such legislation requires a single government official and a central service to oversee the relevant processes, to intervene where necessary and to be held accountable. The Board also recommends that larger companies and organizations be held legally accountable for how they manage their digital safety and security.

Note to editors: For more information, please contact Simone Klein Haneveld, spokesperson for the Dutch Safety Board, by telephone on +31 6 86 654 659 or by email at s.kleinhaneveld@onderzoeksraad.nl.