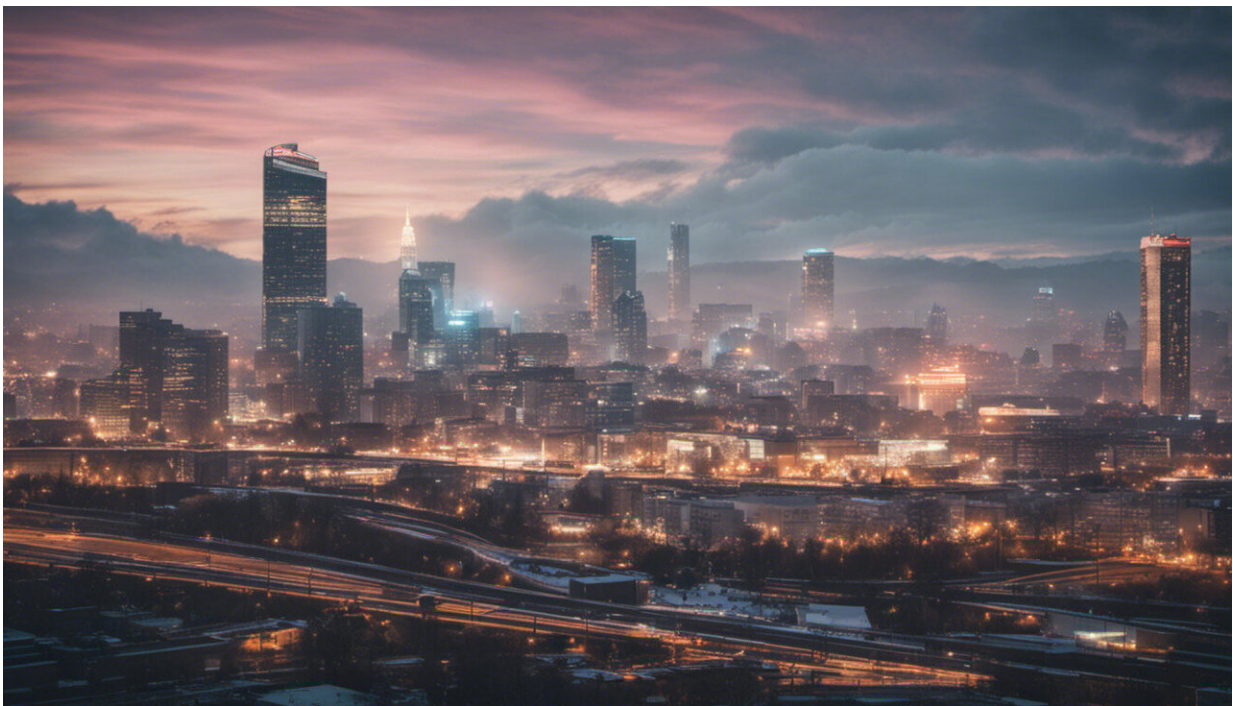# Many Dutch municipalities do not yet respond adequately to security vulnerabilities, research finds

October 4 2023

Credit: AI-generated image (disclaimer)

Many local authorities respond too slowly or inadequately to reports about security vulnerabilities. These coordinated vulnerability disclosures (CVD reports) are often made by ethical hackers who aim to make the internet safer. While this process has improved in recent years,

the study by the University of Twente and the Dutch Institute for Vulnerability Disclosure (DIVD) indicates that there is still much room for improvement for local authorities.

Out of 114 Dutch municipalities, it was tracked whether the issue was resolved in 89 of them. Among these 89 contacted municipalities, 44 did not respond within 90 days—the period specified by the University of Twente in its Coordinated Vulnerability Disclosure for research—regarding the security notification. In 49 of the responding municipalities, the problem was found to remain unresolved. In 10 municipalities, the security [vulnerability](#) was fixed, but this was not communicated back to the notifier.

However, there are reasons for optimism, as there were municipalities that proactively responded to the notifications. In 19 municipalities, the report was handled appropriately, and there was a response to the notification.

The research was conducted by Koen van Hove, a Ph.D. candidate at the University of Twente, a software and research engineer at NLnet Labs, and a researcher at the volunteer organization Dutch Institute of Vulnerability Disclosure (DIVD). He initiated the research out of curiosity about the functioning of CVD procedures in Dutch municipalities.

Between 30 August 2022, and 23 February 2023, Van Hove reported a security vulnerability in commonly used software to municipalities. Where possible, he used the CVD procedure on the municipalities' websites. In total, he contacted 114 Dutch municipalities. The security vulnerability involved the ability to send emails through the infrastructure used by municipalities that were indistinguishable from legitimate municipal correspondence.

During the reporting process, there were challenges, including malfunctioning forms and email addresses, and confusing reporting methods. Notably, many reporting forms were only accessible after logging in via DigiD, making anonymous reporting impossible. Additionally, it was observed that in 11 out of 114 cases, an automated process started after the report.

Personal information such as date of birth, marriage date, financial status, residence permit for both the notifier and partner, parents, and children were requested from the Personal Records Database (BRP). This occurred without the responsible parties at the municipalities being informed.

Since January 1, 2019, the government has introduced the Baseline Information Security Government (BIO), which makes it mandatory to have and publicly disclose a procedure for reporting security issues (CVD procedure). The research indicates that there is room for improvement, as more than half (60) of the 114 contacted municipalities have not yet published or enforced a clear CVD procedure.

The importance of reporting through the CVD system for municipalities is evident, as illustrated in 2020 during a ransomware attack on the municipality of Hof van Twente. Volunteers making these reports are not legally obliged to do so, but they contribute due to their awareness of its significance. Therefore, keeping the threshold for making such reports as low as possible is crucial.

This can be achieved by publishing a clear and accessible reporting procedure on municipal websites, preferably also anonymously and without unnecessarily requesting personal data. Furthermore, the research emphasizes the importance of timely and informative communication with the notifier.