THE DUTCH SAFETY BOARD

PRESS RELEASE

The Hague, June 28th 2012

DigiNotar investigation: the digital security of public authorities must improve substantially

Public authorities do not always properly organise their digital security and are therefore unable to safeguard that security. This is one of the conclusions of the Dutch Safety Board's report, published today, on the 'DigiNotar incident'. Secure electronic data traffic is a basic condition for the proper functioning and continuity of many administrative organisations and is therefore a direct responsibility of public executives.[1] Public executives are often unable to properly fulfil this responsibility, however, as a result of which the subject is not discussed at the top levels of public administration and public executives do not exercise enough control. Public executives are at far too great a distance from the problems that must be overcome to ensure digital security.

The hacking of DigiNotar in the summer of 2011 made clear that the Dutch government was not prepared for a breach of its digital security. DigiNotar supplied digital certificates that were used to protect electronic data traffic. The Dutch government also made use of the certificates supplied by this company. The security breach meant that the data of private individuals and companies could be intercepted and possibly misused. To the surprise of many, it proved impossible to effect a rapid switch to a different supplier without seriously endangering the continuity of various essential data flows with and within the government. The potential consequences of a rapid switch included the cessation of data flows within the judiciary or the Tax and Customs Administration, which would have caused considerable social disruption and economic damage. Ultimately, it took the government months to replace all DigiNotar certificates.

The Dutch Safety Board focused on the question as to how public authorities safeguard digital security in administrative and organisational terms. Among other things, the Dutch Safety Board investigated the actions of the parties involved following the hacking of DigiNotar. The investigation did not focus on the technical specifications of security at DigiNotar and the hacking itself was also not considered.

Risks

The hacking of DigiNotar could have such potentially drastic consequences because public authorities had not anticipated the possibility of a certificate service provider becoming unreliable. More generally, the Dutch Safety Board concludes that, because of the way PKIgovernment certificates intended for public authorities are currently used, such certificates do not have enough added value relative to other certificates. This is because the central government has placed itself at too great a distance and does not really carry out its own checks to verify compliance with the applicable rules.

Investigation into a number of municipalities revealed that, also at this level of government, there is insufficient understanding of the risks that pose a threat to digital security. Risk awareness is mainly present at ICT departments. It is virtually non-existent at the top level of administrative organisations or in Municipal Executives. With the exception of the municipal personal records database, digital security in the data processing of municipalities is not always systematically safeguarded.

The Dutch Safety Board concludes that the public executives of many administrative organisations do not exercise sufficient control to ensure proper digital security, among other reasons because they are insufficiently aware of the threats to digital security and the potential consequences of digital security breaches. Risks are the rule with respect to digital security, not the exception. The government must remain aware of this fact and act accordingly. Public executives of administrative organisations often lack the knowledge required to guide their respective organisations in this area. Public executives are better able to exercise control with respect to digital security when they are aware that such security is a condition for the continuity of their services. The Social Insurance Bank and the Tax and Customs Administration are examples in this regard.

[1] The term 'public executives' refers to both political executives and executive directors of administrative organisations.

Recommendations
Public executives of administrative organisations must exercise active control with respect to digital security. A public obligation to render account similar to the obligations that apply in the field of finance could contribute to achieving such control. Administrative supervision must be tightened and the government must ensure that public executives become better informed about exercising control and providing guidance with respect to digital security.

Public authorities must also develop a more systematic approach to safeguarding digital security. Although agreements for this purpose have been in place for some time already, they are observed only to a limited extent. The risks associated with data processing must explicitly be weighed against the benefits of such processing at the highest level of the administrative organisation. In addition, public authorities must systematically identify risks to digital security and take the appropriate measures to counter these risks. Since it is unrealistic to expect security that is infallible at all times, these measures must relate to both prevention and recovery following incidents.

Contact: Press officers Sandra Groenendal +31 623 175 701 and Wim van der Weegen +31 623 464 277
or +31 70 333 7000. E-mail: communicatie@onderzoeksraad.nl