Follow-up audit of the cantons' implementation of the network security policy of the Swiss Conference on Informatics
Federal Office of Information Technology, Systems and Telecommunication

Key facts

In 2009, the Swiss Federal Audit Office (SFAO) carried out an audit on the extent to which the cantons had implemented the network security policy (NSP) prescribed by the Swiss Conference on Informatics (SIK/CSI)[1]. Based on the results, the Federal Office of Information Technology, Systems and Telecommunication (FOITT) was given a recommendation, and this has not yet been implemented in the SFAO's view. Security elements were supposed to be added to the contracts between the FOITT and the cantons. The cantons were also to be obliged to provide evidence of the implementation of the agreed security requirements in their networks. If they failed to comply with these agreements, the FOITT or a third party instructed by it was to carry out corresponding security audits.

The FOITT implemented this recommendation insofar as possible in the *Service Level Agreement* (SLA) with the cantons. However, it sees itself neither in a position nor under an obligation to carry out audits in security-related areas in the cantons. There is no legal basis for this in Switzerland's federalist system that would give a federal office the right to interfere with the cantons' authority or vice versa. Consequently, the SFAO will class the still outstanding recommendation as settled.

Each party has to protect its own networks from threats

The threat situation and the ensuing risk potential have deteriorated since the SFAO's report. Earlier, there was a tendency towards mutual trust within network structures. Now, it is paramount for the administrative units' sensitive data to be protected in a very targeted manner. Therefore, not only are the highest possible barriers installed at a network's external borders, data traffic is also monitored constantly within the network.

The transport network between the cantons' networks and the federal one (KOMBV-KTV) is an external network from the Confederation's viewpoint. It gives the cantons a highly available and fast connection in order to access federal applications within the framework of their statutory tasks. The first security barrier for access is two-factor authentication. Because of the associated personalised profile, the second security component consists of access rights to applications being activated only for people who are entitled to them. Encryption ensures the confidentiality of the data transferred.

The cantons are responsible for the implementation of network security

Because of their own interests in protecting their data at a similar level, the security of the cantons' networks was to be handled in the same way as in the case of the Confederation. Aside from the NSP of the Swiss Conference on Informatics, there are further basic principles and specifications that enable each canton to take the minimum security precautions. There is also cooperation be-

[1] "Audit of the cantons' implementation of the network security policy of the Swiss Conference on Informatics", 8421, 2009

tween federal and cantonal representatives in various SIK/CSI bodies with the invariable aim of ensuring a uniform approach. However, there is no superior body that can regularly check the implementation of binding specifications and also implement them. Greater attention should be paid to these requirements when preparing the NSP of the Swiss Conference on Informatics, which is welcomed by the SFAO.

Original text in German