EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
SWISS FEDERAL AUDIT OFFICE

Horizontal audit of IT security in the Federal Administration
Report for the attention of the Federal Council

Key facts

As per the Federal Council's decision of 4 June 2010, the Swiss Federal Audit Office (SFAO) received a written request from the "Delegate for Federal IT Strategy" on 24 June 2010 to audit the implementation status of measures to improve IT security. The SFAO accepted the request on 27 August 2010 and agreed to perform a horizontal audit for the year 2011. The audit report was brought to the attention of the Federal Council members on 2 December 2011 in an information memo from the Federal Department of Finance (FDF).

In its audit schedule for 2011, the SFAO set out which measures were to be audited, with which priority and to what extent, and which areas of the Federal Administration were to be covered in the audit. The topics thus selected were "Adherence to password rules", "Timely resolution of security deficiencies" and "Intensified network monitoring". The audit was performed on a total of seven IT service providers within the Federal Administration. In addition, the SFAO conducted a written survey among 71 service users on the areas "Adherence to password rules", "Timely resolution of security deficiencies" and "Improved information management". These areas correspond to the immediate measures set out in the Federal Council's decision of 16 December 2009.

The main findings from the individual audits are as follows:

Only minor deficiencies were revealed in the Windows environment. The audit found a good level of conformity among the audited service providers with regard to the adherence to password rules and the timely resolution of security deficiencies on new Windows systems.

Significant security issues exist in the non-Microsoft environment. The SFAO identified substantial weaknesses in the timely resolution of security deficiencies in non-Microsoft products running on Windows platforms. In some cases, dependencies exist on specialised applications, no longer allowing the relevant components to be updated. Deficiencies were also found in defining responsibilities for maintenance of these products. Other security vulnerabilities were found in legacy systems that cannot conform to the password rules and for which updates are no longer available to resolve the current security shortfalls.

Security deficiencies are accepted by service users; the service providers lack assertiveness. Examples have shown that security matters were often not a priority at the user end:

- Some of the workstation systems give highly privileged user rights (local administrator rights). These were assigned on the basis of user requests submitted.
- The business areas continue to operate legacy applications and systems despite knowing that these present security deficiencies or prevent security-critical components from being updated.
- In one case, password rules were disabled at the department's management level. The escalation mechanisms in place for such an order obviously failed to take effect.

- Responsibility for security-related matters still tends to be regarded by service providers as a purely technical responsibility. There is a lack of understanding of the segregation of tasks and responsibilities between service providers and service users.
- Some service providers maintain that the absence of any binding or sufficiently specific rules often undermines their assertiveness with respect to service users. The security directives need to be more precise in this respect.

Synergies between service providers tend to arise more by coincidence than by design. In the course of its audits, the SFAO found that good solutions had been found in many areas. However, the SFAO believes that this knowledge is not sufficiently shared among service providers and that synergies are not sufficiently exploited. As a result, the individual service providers tend to develop or commission their own solutions.

Numerous activities are underway in the intensification of network monitoring. The service providers concerned have implemented initial projects and are now gathering their experience. Further expansion steps are planned, specifically for the handling and analysis of the data gathered. The required two-year retention period for log files is not supported by all service providers. While measures to improve the security situation are envisaged, no short-term improvements are to be expected.

Security of the cantonal networks remains “the great unknown”. The FOITT still does not have the contractual basis to assess the quality of network security in the cantons connected and to take the necessary countermeasures. This should change with the signing of revised service level agreements (SLAs) with the cantons, planned for the end of the year. For several cantons, the implementation of these SLAs, and thus ensuring and evidencing the security of cantonal networks, will only be possible in the medium term.

Based on the SFAO’s feedback from service users, it would appear that these have not yet fully identified their critical applications in terms of information protection.

The SFAO has made a number of recommendations at the appropriate level to the Federal IT Council (FITC) or the Federal Strategy Unit for IT (FSUIT) and to the various service providers. The recommendations to the FITC or the FSUIT concerned making guidelines more precise, raising the level of cooperation between service providers, and security-related training. The written feedback shows that the SFAO’s recommendations have been accepted.

Original text in German