Towards the impact of the operational environment on the security of e-voting

Axel Schmidt, Melanie Volkamer, Lucie Langer, Johannes Buchmann

Technische Universität Darmstadt
CASED
{axel, langer, buchmann}@cdc.informatik.tu-darmstadt.de
volkamer@cased.de

Our paper deals with the security of operational environments for e-voting and its importance for the security of electronic elections. We provide a comprehensive catalogue of organizational and technical requirements which have to be satisfied by the operational environment to carry out secure remote electronic elections. Our findings provide a basis for the design and the evaluation of a secure operational environment for e-voting. Consequently our results are of great value for all institutions which want to perform secure remote electronic elections. So far the security of electronic voting was focused on secure voting protocols and software systems. We show that the security of electronic elections requires a secure operational environment as well. The operational environment has to fulfill many organizational and technical requirements to be able to securely operate an electronic voting system. For example, in most electronic election scenarios the operational environment has to provide secure communication channels, it must ensure the system availability, it must protect the server computers from unauthorized access and provide secure auditing and emergency measures. There are many more requirements of that kind. Security requirements for electronic voting have been defined in several catalogues. Among the most important ones are the catalogue on "Legal, Operational and Technical Standards for E-voting" from the Council of Europe and the catalogue of requirements for online elections in non-governmental organizations of the German Informatics Society. Moreover, two Common Criteria Protection Profiles for the evaluation of electronic voting systems have been released by the German Federal Office of Information Security. The first one is the "Common Criteria Protection Profile for Basic set of security requirements for Online Voting Products", which is intended to be a mandatory prerequisite for online voting systems deployed in Germany, while the second one is a Protection Profile for Digital Voting Pen systems. We deeply analyzed these catalogues and Protection Profiles to derive the organizational and technical requirements they include for the operational environment in which the electronic voting system is implemented. We categorized our results in families of requirements like Trusted Communication, Trusted Components, Trusted Organization or Trusted personnel. We then propose how to use our findings for the evaluation and certification of the operational environment thereby improving trustworthiness and security of electronic elections. We give recommendations for an evaluation procedure based on IT-Grundschutz/ISO27001 methodology. Finally we show how the concept of the Voting Service Provider can facilitate providing a secure operational environment for secure electronic elections.