OSA Case Study: Applying OSA to Construct a High-Security B2C Internet Service

by Tobias Christen, CTO DSwiss Ltd.

Problem at hand

When DSwiss set out to construct its high-security internet data safe called DataInherit, a well modeled security architecture was regarded a high priority, because the security architecture helps to focus the implementation and operations team and lays the foundations for maintainability and operability. After a comparison of the available architectural standards and frameworks, OSA was chosen because it is based on a widely accepted controls catalogue and features pattern visualizations that helped when talking to software developers and other stakeholders.

Project & Service Needs

DSwiss invested around 40% of the development effort into security for its internet facing B2C data safe. The service is targeted to the general consumer of age 35-65, consequently the selection of security controls also needed to support the highest usability.

The project team consisted of experienced software developers and architects that required a quick start to understand what security (and other non-functional) requirements were to be prioritized. The project used the Scrum approach for iteration planning and security experts were advising and training the team on a daily basis.

Security Baseline

NIST 800-53 was chosen as the starting point for creating a security baseline that is targeted to a lean organization and that is focused on running a secure internet service. Change management, incident management, patch management as well secure development were chosen to be the high priority processes.

Functional Security Requirements

Functional security requirements were influenced by the need for usability as well as by the increasing threat exposure for internet users.

Solution Approach

The DSwiss team found it easy to apply the OSA security architecture approach as it is described out on the OSA homepage.

Process & Patterns

The team worked in fast iterations with the system architects to draft a system architecture that reflects the structure and controls of the selected OSA patterns. The patterns were selected based on the nature of the application.

The pattern "Public Webserver" helped to focus on the strongest threats and make sure all involved parties understood which controls are their responsibility. The pattern "Data Security" helped to identify the principles that then guided the definition of the terms of service and the privacy statement. The module "Server" assisted understanding the array of responsibilities that apply to the operations manager.

Experience and Lessons Learned

The strongly visual approach of OSA helped in the early phases of the design to jump start and then settle on a commonly accepted architectural overview.

The strong controls catalog and consistent actor model helped to structure the security architecture of DataInherit.

However our efforts in selecting the right technologies needed to go beyond OSA since OSA is technology agnostic.

We had to challenge the value of each of the considered technologies and frameworks against the prioritized risk scenarios. We learned that less is more because every additional control even it mitigates an important risk it also increases the most prominent risk "system complexity".