Course description:

The aim of the course is to present different aspects of application security. Will discuss common security vulnerabilities along with ways to avoid them, application components critical in terms of safety and additional security items, such as. Testing or ISO. All issues will be presented supported the practical side, the review of the products available on the market along with sample code in your favorite programming language.

Program

1. application Security
    - introduction to the issues
    - an overview of frequently encountered threats ...
    - … and ways to avoid them
    - OWASP and CWE rankings
    - base CVE, CVSS calculator
2. Certificates, electronic signatures, time stamps
    - theoretical basis, PKI, certificate application
    - certificates available on the market, the role of the National Certification Center, qualified services
    - Practical page, review solutions, create your own certification authorities
3. Authentication and authorization
    - Hardware solutions components and their role
    - meanings in different network layers
    - review of protocols and solutions available on the market, including NTLM and Kerberos
    - access control mechanisms, including RBAC & ABAC
    - processes related to the management of identity and access
4. Federation of identity and authentication delegation
    - OAuth2 protocols, OpenID Connect and XACML
    - safety in different types of architecture
    - integration with third-party services: SMS, payment systems, Auth0, Google, Facebook
5. Database Security
    - eg solutions proposed by Microsoft SQL Server
6. Safety of infrastructure
    - security application servers
    - overview of components such as firewalls, proxy IDS / IPS, WAF
    - the importance of monitoring, the role of SIEM
7. security Architecture
    - the importance of good requirements
    - types of controls and their application
    - and an overview of the importance of basic safety rules (called. security Principles)
    - an overview of the architecture layers and their role

- the so-called concept. security domains

8. threat modeling
    - methodology STRIDE
    - the use of tools to support
9. Information Safety
    - basic concepts and terms
    - information flows and their protection
    - use threat modeling
10. security testing
    - penetration testing and vulnerability scans, types, methodology
    - an overview of tools for testing
    - introduction to hacking
11. Security in the software development process
    - overview of the process, an overview of the main stages
    - an overview of the most important activities, including requirements gathering, risk analysis, threat modeling.
12. The importance of establishing and maintaining security policies