SECURITY • NETWORKING • MANAGEMENT

Security Audit of IT Systems

Safety of IT systems can not be bought as a product. Safety is a state achieved using technical and organizational means. Ensuring safety of IT systems' resources requires elaboration of an appropriate security policy, design and deployment of adequate safeguards that enforce the policy, maintenance of the protections by educated IT staff as well as *regular auditing of an entire security system*.

Based on many years experience in IT security, CLICO Professional Services (PS) offers the customers and partners complete auditing services. The customers issued for CLICO written references that acknowledge the highest quality of conducted IT systems' security audits.

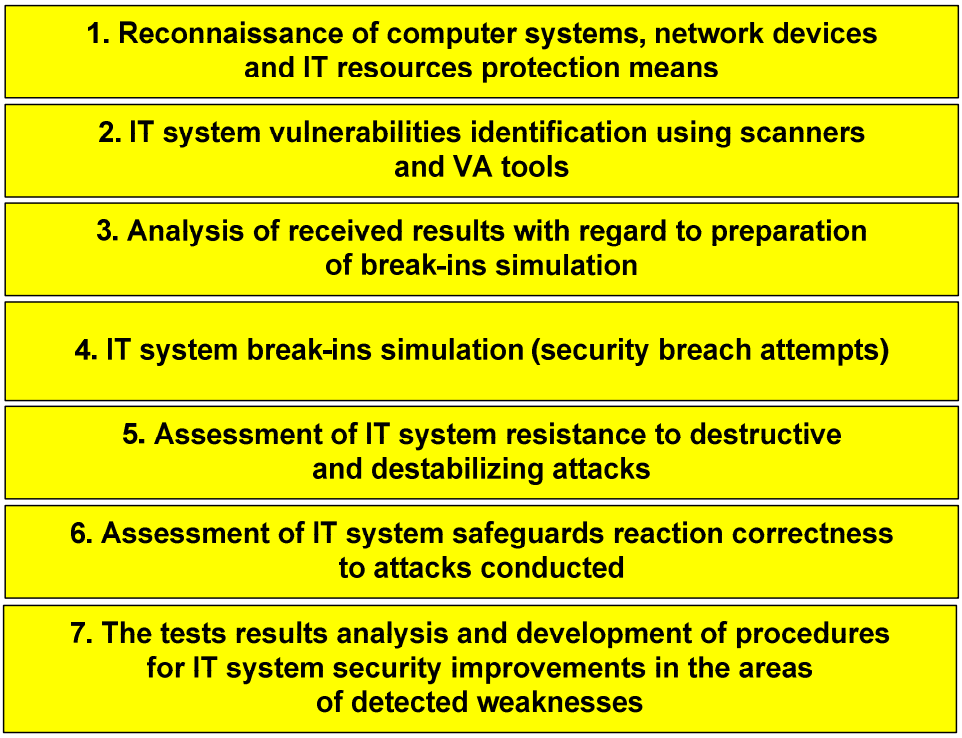
- **Knowledge and competence**
  Audit services are conducted by a team of experienced specialists from CLICO PS department that for many years had been working in IT security (first penetration tests were conducted in 1998). Analysts and security engineers engaged in the audit works have achieved the highest levels in professional certification of IT security, i.e. Certified Information Systems Security Professional (CISSP), Check Point Certified Security Expert Plus (CCSE+), Juniper Networks Certified Internet Specialist (JNCIS).
- **Complete audit services scope**
  CLICO PS offers complete range of IT security audit services - from practical penetration tests with the elements of controlled break-in simulation, analysis of the security design and configuration, etc. to verification of the companies' security policy compliance with low regulations and security standards (i.e. ISO/IEC-27001).
- **Proven audit methodologies**
  Audit works are conducted according to the penetration tests and internal security audits methodologies, elaborated by CLICO PS based on widely approved standards (e.g. ISO/IEC 27001), guidelines (e.g. OWASP Testing Guide), requirements of Polish and international low (e.g. Dz.U.29.08.97, Dz.U.08.02.99) and IT security theory (e.g. "Defense-in-Depth", "Least Privilege" and other principles). The methodologies with accurate description are provided to the customers before the audit starts for proper cooperation with the customers' staff. CLICO Education Services department organizes the trainings that cover theoretical (methodology) and practical aspects of the IT security auditing.
- **Documentation of security audit**
  Results of the security audit are provided in the form of reports describing real safety status of the companies' IT systems. Two reports are elaborated - general report for the company's management and detailed technical report for IT staff. Documentation of the audit works includes accurate description of all conducted tests and analysis (i.e. objectives and scope of the tests, techniques and tools used during the tests, output of the tests, conclusions and recommendations).
- **Recommendations for IT system's security strengthening**
  The audit reports provide clear remarks to the status of IT systems' safety and the description of discovered weaknesses and potential vulnerabilities usages by the intruders as well as the recommendations for security strengthening. The remarks are presented with the priority for IT system's resources safety (scale: critical, high, medium, low) as well as proposed by the auditor deployment time of the security strengthening recommendations.
- **Education of customer's IT staff**
  During the audit, CLICO Education Services can provide training for the customer's IT staff. It is recommended to conducts practical security tests (i.e. exploits, DoS) in the close cooperation with administrators of IT systems being tested. It is particularly important when performing tests of the systems resistance to destructive attacks and break-ins as well as verification of the safeguards reaction correctness to the attacks conducted. Also IT staff knowledge and skills are in the tests scope. Proper security system operations depend on the technology and people responsible for the management, maintenance and governance.

CLICO Sp. z o.o., ul. Oleandry 2, 30-063 Kraków; Tel: 12 6325166; 12 2927522 ... 24 ; Fax: 12 6323698;
Oddział Warszawa, ul. Kijowska 1, 03-738 Warszawa; Tel: 22 5180270 .. 72; Fax: 22 5180273
E-mail: support@Clico.PL, orders@Clico.PL.; http://www.clico.pl

Penetration tests of IT systems and infrastructure

Main goal of the penetration tests is reliable assessment of IT system security tightness and effectiveness. These tests are performed in the form of practical evaluation focused on the verification if deployed safeguards properly react to the attacks conducted and IT systems are resilient to real threats (i.e. penetration attempts, unauthorized access and break-ins, DoS attacks, malicious code propagation, network eavesdropping, etc.).

To be reliable the tests should be performed with real hacking techniques and tools (i.e. VA scanners are not enough). For this purpose the auditor's stations must be properly prepared and protected, so that the tests results would not be revealed to unauthorized persons (i.e. hacking tools downloaded from Internet can contain Trojans). The stages of typical penetration test were presented in figure bellow.



Security analysis of Web applications

Web is a standard for IT systems applications access. It is convenient and cost-effective, because the users do not need to install, configure and upgrade any client software - standard Web browser can be used for this purpose. Web technologies are growing rapidly. The developers use new, sophisticated programming methods, libraries and components (e.g. AJAX, SOAP, ASP .NET, PHP, etc.).

During the penetration tests of Web applications, new specific application threats should be taken into consideration, i.e.:

- tampering of Web application elements like URLs, form fields, cookies and other parameters,
- SQL-injection (including blind SQL-injection),
- CLI-injection and LDAP-injection,
- Cross Site Scripting (XSS),
- Cross Site Request Forgery (CSRF),
- fuzzing, illegal encoding, cookie poisoning, Web brute force logins, etc.

The security tests of Web applications are conducted according to the methodology based on *Open Web Application Security Project (OWASP) Testing Guide* completed by the tests designed by CLICO PS.

Analysis of security policy and safeguards design correctness

Deployment of the security products in the network (e.g. firewall, intrusion prevention system) in practice not always improves IT system resources safety. Due to the design and configuration errors, the safeguards do not perform their tasks properly and cause an illusive sense of security. Analysis of IT systems' security policy and safeguards design correctness is performed based on proven theory of IT systems' security as well as engineering good practices, i.e.:

- **The principles of security design**
  (i.e. „Defense-in-Depth", „Defense Through Diversification", „Compartmentalization", „Least Privilege", „Adequate protection", „Weakest link in the chain")
- **Standards in IT systems security designing and management**
  (i.e. IETF RFC 2196, ISO/IEC 27001:2005 - formerly BS 7799-2, ISO/IEC 27002:2005- redesignation of ISO/IEC 17799:2005, ISO/IEC 18028-1,2,3,4,5)
- **Good practices in security and network engineering**
  (i.e. CERT, IETF/RFC, ISO/IEC, ISSA, NIST, NSA, SANS, security vendors guidelines)

During the analysis the risk assessment is conducted. Security policy and safeguards design should be based on the risk assessment results and additional requirements formulated by the Company (e.g. low and other regulations that the Company should fulfill). Conducting risk assessment allows the verification if IT system's protections were deployed in a cost-effective way - IT system security means should be built according to the business needs (i.e. the risk and business impact analysis).

Telecommunication systems and networks are crucial for IT systems proper operations as most of the applications work in the networking environment and closely depend on its performance, reliability and security. During the analysis the following elements of IT systems are verified:

- Performance and overload resilience (i.e. suitable communication links and devices throughput, and appropriate systems memory and processing power).
- Reliability, network bandwidth management and the systems and traffic optimization (i.e. ability to fulfill SLA).
- Safety of the network devices and administrator's authentication and authorization processes.
- Scalability and ability for the security system expansion by new elements and protection mechanisms in the area of its size (additional protection points), performance (higher network throughput and increased traffic) and reliability (redundancy configurations).
- Security and control of virtualized systems, etc.

For more information about IT systems security audits and other security services offered by CLICO please contact: psw@clico.pl

About CLICO

CLICO Sp. z o.o. (formerly CLICO Hi-Tech Software promotion Center) is a private company founded on October 1991. The company has HQ in Kraków and its offices in Warszawa, Katowice, Wrocław and Sofia (Bulgaria). In Poland CLICO is the biggest specialized distributor of advanced security and networking products as well as both pre and post-deployment technical support provider. Main companies' interest is security audits and other IT services requiring deep knowledge, competence and experience.
Since its foundation CLICO has been interested in advanced IT solutions, especially designated for network and multiuser systems. As the first company on Polish market CLICO introduced TCP/IP tools for Windows and as the only company in Poland included in its offer the multiuser, award-winning Interactive UNIX system.
One of the most important company's strategies is a care of offer's completeness and compatibility, the subject which has been cultivated since the very beginning. It brought specially visible and positive results when the company's activity was focused on computer system and network security. CLICO as the first company introduced to Polish market a commercial firewall solution (Check Point FireWall-1 in 1995), an intrusion detection system (ISS RealSecure in 1996), and recently next-generation firewall (Palo Alto Networks).
Currently, CLICO Ltd. acts on Polish market as specialized software and network devices supplier with strong focus on systems and computer networks security issues as well as topics related to e-commerce. Company's offer includes products of leading vendors in the branch supplying such products as: firewall systems, VPN solutions, encryptors, digital identification and authorizations systems, PKI systems, solutions for reliable network services operation, anti-virus and anti-vandal systems, Internet access policy creation solutions, comprehensive e-commerce infrastructure tools (mail, catalogue systems, portal servers, B2B, etc.), advanced terminal emulators, tools for heterogenic operating systems integration and more.
The company achieved quality certification according to PN-EN ISO 9001:2001 and WSK criteria.

