# Security Penetration Testing

**For many organizations, IT teams operate on a reactive stance towards security events. However, there are a number of proactive approaches that can be taken in order to enhance the security posture at an organization. One of the most effective approaches is cyber security penetration testing where boundary infrastructure and internal security measures are tested for vulnerabilities.**

## Business Challenges

With cyber-attacks continuing to increase in both complexity and frequency, the challenge for many organizations is knowing what preventative measures to put in place and what budget scope is required. To do this effectively, IT security teams need a clear understanding of exactly where the vulnerabilities are in the infrastructure which could be at the perimeter of the organization, or inside the organization where systems and applications may be at risk. While many IT departments are skilled in the day-to-day running of the infrastructure, understanding how it might be attacked is not within their skill set or remit.

## Solution

RUAG Cyber Security Services provides certified analysts who, with full agreement from the customer, can carry out thorough vulnerability scans and penetration testing on an organization. The use of military grade tools and a proven process ensures the testing high. A high quality report on vulnerabilities and risks is delivered as part of the service along with a comprehensive set of mitigation recommendations.

The report can be used as proof of compliance with various standards, including ISO 27001, or as part of a wider report which forms the basis for prioritization of security projects and investment.

### Key Features and Benefits

- Independent, Certified Analysts with top security clearances provide objective testing and results
- Fully scalable service in both scope and depth from single application to full perimeter and internal network
- Vulnerability scan will highlight all major and minor risks
- Full penetration test with a view to compromising security using (white-hat) hacker techniques and tools
- Social engineering campaign
- Measurement of efficacy of existing cyber defence measures and configurations
- Use of standard and bespoke military grade monitoring and analysis tools
- Compliance with standards (including ISO 27001), including documented proof
- Full risk assessment
- Comprehensive Analysis Report, including recommendations for security improvements
- Documentation for use in security architecture improvement programmes

### About RUAG

RUAG develops trailblazing innovations and internationally sought after cutting-edge technology in the fields of aerospace and defence. By combining outstanding technological expertise with a high degree of foresight and responsibility, it creates the foundations for security and progress within society.

For more information:
**www.ruag.com**

### Other Relevant Services

- Incident Response and eForensics
- Cyber Academy Training
- IT Emergency Planning
- Security Health Check

### Primary Offices

**RUAG Cyber Security**
RUAG Schweiz AG
Stauffacherstrasse 65
3000 Bern 22
Switzerland
T: +41 31 376 68 42

**RUAG Cyber Security**
Repräsentanz Berlin
Leipziger Platz 14
10117 Berlin
Germany
T: +49 3020 61 68810

**RUAG Cyber Security (Clearswift)**
1310 Waterside
Arlington Business Park
Theale
Reading
Berkshire RG7 4SA
United Kingdom
T: +44 118 903 8300

Email for more information:
**info@ruagcybersecurity.com**

## Scenarios

### Regular Testing

Cyber-attacks are, unfortunately, a matter of 'when' not 'if'. Forward thinking organizations prepare by using regular Cyber Security Penetration Testing to check for vulnerabilities. Often mistakes are made in the configuration of systems which then leaves the organization open to attack. Regular testing ensures that cyber risks are minimized and helps with prioritizing security projects.

### Compliance with ISO 27001

For many organizations, compliance with ISO 27001 is a necessity in order to work with other organizations. As part of ISO 27001, a vulnerability scan need to have taken place and a report showing compliance created.

### Security Project Prioritization

A penetration test will help identify the areas within IT infrastructure when investment is required to reduce business risk. This can be carried out from the 'outside in' or the 'inside out', highlighting where vulnerabilities exist and what should be done to mitigate them.

### New Application

When a new application is commissioned, especially if can be accessed by third parties such as customers and suppliers, a penetration test can be carried out to ensure the application and its environment is secure. This provides peace of mind to the business that they are not opening up new vulnerabilities as a project moves from 'test' to 'production'.

## Pricing

Pricing depends on the extent and complexity required testing. A basic vulnerability scan starts from €5,000 which includes a comprehensive report into the findings and improvement recommendations.

## Why RUAG Cyber Security Services

RUAG Cyber Security Services have grown out of high profile engagements with the Swiss Government, operating in highly secure environments with specialist personnel. A consistent approach to projects of all sizes ensures a high-quality, on-time, on-budget deliverable which is tailored to the customer's specific needs.

RUAG Cyber Security Services Customers include government departments, manufacturers, engineering services, telecommunication providers, software development businesses and energy providers.

RUAG Cyber Security