

INFORMATION SECURITY CONSULTING

Security Proofing



➤ Moderne Systeme der Informations- und Kommunikationstechnologie (IKT) sind heutzutage sehr komplex und können oft nur mit anderen Systemen oder Systemlandschaften im Verbund betrieben werden. Neben einem störungsfreien Betrieb muss auch die Sicherheit der einzelnen Systeme sowie des Systemverbunds über den gesamten Lebenszyklus sichergestellt werden. Das Information Security Consulting Team von RUAG bietet hierzu von der Beratung, über die Konzeption bis hin zum Security Proofing umfassendes Expertenwissen für zivile und militärische Systeme und insbesondere für sicherheitskritische Infrastrukturen an.

➤ Unsere Dienstleistungen

Es ist unabdingbar, einzelne IKT-Systeme sowie den gesamten Systemverbund regelmässig und detailliert auf Sicherheitslücken zu überprüfen. Oft ist jedoch die Implementierung von Sicherheitsvorkehrungen sehr aufwändig, fehleranfällig und lückenhaft, weshalb eine präzise Kontrolle sehr wichtig ist. Sie attestiert nicht nur die angemessene Sicherheit in Ihren Systemen, sondern deckt auch Schwachstellen auf.

Unser Angebot umfasst vollumfängliche Dienstleistungen im Security Proofing:

- Klassische Beratung inklusive Voralanalysen, Assessments und Audits
- Ausbildung im Security Umfeld
- IT-Security Tests (Testing, Penetrationstesting, Reporting, Massnahmenplanung und Support)

➤ Ihre Vorteile

Der Service Security Proofing verbindet die zwei Gebiete Testing und Security und bündelt das Wissen der einzelnen Spezialisten. Dadurch ist eine ganzheitliche Betrachtung der Systeme, der Funktionalitäten sowie kritischer Abläufe möglich.

Sie profitieren von unserer Ausrichtung wie folgt:

- Penetrationstest sind abgestimmt und angepasst auf das militärische Umfeld
- Vollumfängliche Beratung von einem Partner mit Expertise
- Ein Ansprechpartner (dadurch nur ein Geheimnisträger)
- Langjährige Erfahrung in militärischen Projekten nach ZUVA/HERMES VBS
- Maximale Transparenz und gleichbleibend hohe Qualität bei kosteneffizienter Umsetzung

➤ Lebenszyklus eines Systems

Der Lebenszyklus eines IKT-Systems lässt sich in verschiedene Phasen einteilen (vgl. HERMES). Er beginnt mit der Konzeption und endet mit der Stilllegung oder Entsorgung. Sicherheitserhöhende und oder -erhaltende Massnahmen sollten im Lebenszyklus eines Systems ständige Begleiter sein, um dauerhaft qualitativen Ansprüchen zu genügen. Das RUAG Information Security Consulting berät und unterstützt Sie in den verschiedenen Projektphasen.



Die Qualitätssicherung erfolgt in unterschiedlichen Phasen des Systemzyklus. Wir begleiten Sie bei:

➤ INITIALISIERUNG

- Beratung bei der Kostenplanung für den Testaufwand im Hinblick auf Ressourcen und Infrastruktur
- Beratung bei der Erarbeitung von Sicherheitsanforderungen
- Review der Sicherheitsanforderungen hinsichtlich Vollständigkeit und Testbarkeit
- Erarbeitung erster Testkonzepte und Teststrategien
- Früherkennung von Entwurfsfehlern

➤ KONZEPT

- Wir begleiten Sie bei der Entwicklung von komplexen IKT-Systemen vom Prototypen bis zu den abschliessenden Testaktivitäten:
- Erstellen oder Verfeinern der Teststrategien und Testkonzepte
 - Definieren von Testdesigns/Pentest-Designs und Testfällen
 - Sicherheitsreviews von Architekturen und Entwürfen
 - Früherkennung von Entwurfsfehlern
 - Definition von Massnahmen und Optimierungsvorschlägen
 - Definition, Aufbau und Betrieb von Testinfrastrukturen und Testautomatisierungen
 - Testdurchführung und Testauswertung
 - Erstellen/Führen des Sicherheitsberichtes (Risiken im ISDS-Konzept)

➤ REALISIERUNG

- Wir übernehmen die Testaktivitäten für Validation und Systemabnahme komplexer IKT-Systeme nach Beendigung der Entwicklung oder im Falle von eingekauften Systemen:
- Erstellen der Validierungs- und Abnahmekonzepte
 - Erstellen der Prüfvorschriften (Testfälle in der Regel auf Stufe Szenarien)
 - Aufbau der Validations- und Abnahmeumgebung
 - Durchführung der Validation und Systemabnahme, Schwachstellenerfassung samt Bewertung
 - Erstellen/Führen des Sicherheitsberichtes (Risiken im ISDS-Konzept)

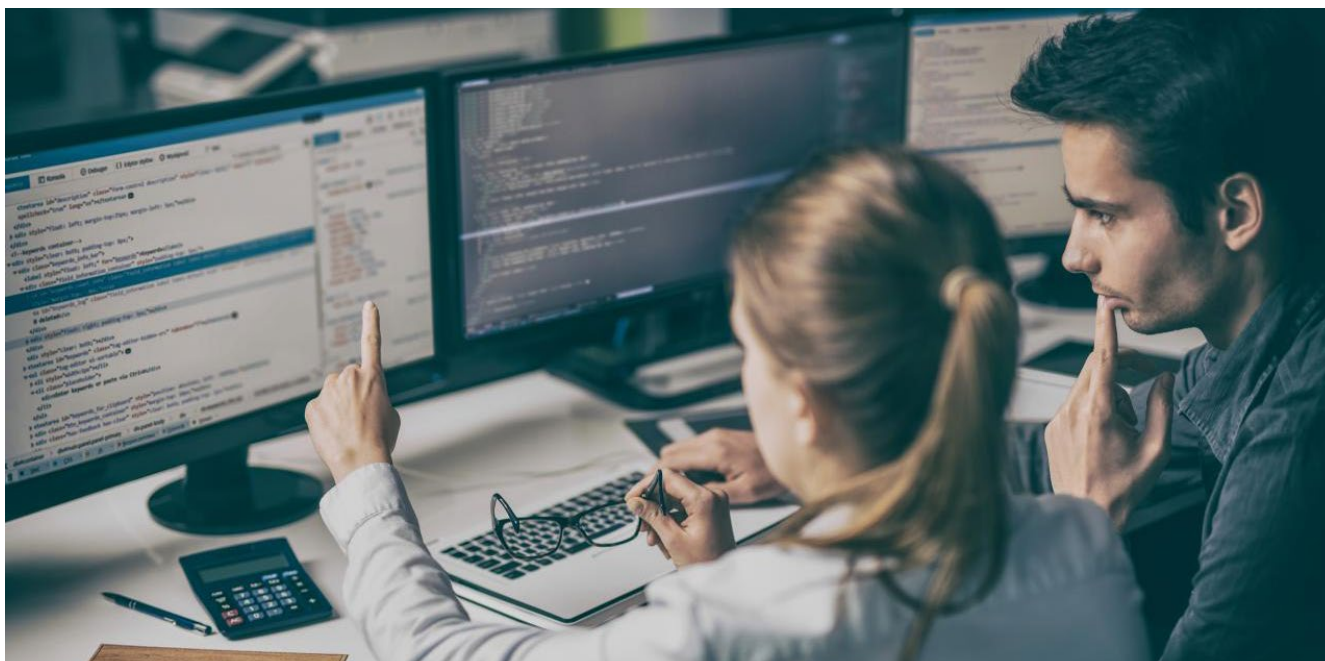
➤ EINFÜHRUNG

- Sicherheitsprüfung von Änderungen im Änderungs- und Konfigurationsmanagement
- Sicherheitsprüfung und Review der Konfigurationen
- Sicherheitsprüfung (Pentests) nach risikobasiertem Ansatz

➤ BETRIEB/NUTZUNG

- Audits gemäss gängigen Normen/Standards (ISO 27001/IKT-Grundschutz Bund)
- Sicherheitsprüfung von Änderungen im Änderungs- und Konfigurationsmanagement
- Periodische Sicherheitsprüfung (Pentests) nach risikobasiertem Ansatz

➤ Angewandte Prüfverfahren



Angewandte Prüfmethoden

- Audits (Interviews/GAP-Analysen)
- Sicherheitstests (Funktion/Integration)
- Penetrationstesting/Angriff-Simulation
- Phishing-Kampagnen und Awareness-Schulungen
- Sicherheitsreviews (Dokumente/Pläne/Architekturen/Prozesse)
- Simulationen

Zertifizierungen

- Das Security Proofing arbeitet nach etablierten Standards
- Zertifiziert nach ISO 9001
- Die Security-Engineers und -Manager sind nach CISSP, CISM, CISA, CEH, ISTQB, IREB, ITIL, HERMES, Scrum Master und Usability zertifiziert
- Das Prüfpersonal ist nach Vorgaben des Bundes in Bezug auf den Zugang zu klassifizierten Informationen, Materialien und Anlagen überprüft (PSP 11, bis Stufe GEHEIM)



➤ KONTAKTIEREN SIE
UNS FÜR IHR PROJEKT: