



bw digitronik ganzheitlicher Ansatz:
Informationssicherheit =
Organisation + Mensch + Technologie.



Organisation: Unterstützung bei der Erstellung von Strategien, Richtlinien und Konzepten für die Informationssicherheit. Aufbau und Betrieb eines ISMS.



Mensch: Analyse der Informationssicherheitskultur. Unterstützung bei Awareness-Massnahmen für das Management und die Mitarbeitenden.



Technologie: Beratung, Engineering, Lieferung, Integration und Support von IT-Security-Lösungen.

Security Audits & Penetration Testing nach OSSTMM.

bw digitronik, seit 1994 in der Informationssicherheit tätig, gehört zu den Schweizer Pionieren auf diesem Gebiet. Unser Ansatz für ganzheitliche Informationssicherheit basiert auf erprobten und international anerkannten Standards wie BSI 100-1 bis 100-4 und ISO 27001/2:

Informationssicherheit = Organisation + Mensch + Technologie.

Ihre Herausforderung

Täglich werden neue Sicherheitslücken in Betriebssystemen und Applikationen bekannt. Häufig ist die Hacker-Gemeinschaft rascher mit dem Bereitstellen von Tools zur Ausnutzung der Lücken, als die Hersteller mit der Lieferung von entsprechenden Patches. Es entsteht das sog. „Window of Vulnerability“. In dieser Zeit ist ein Unternehmen potentiell verwundbar gegen externe oder interne Angriffe. Alle Lücken zeitgerecht zu schliessen, ist ein unmögliches Unterfangen. Daher lohnt es sich, neben technischen Massnahmen, auch periodische Sicherheitsüberprüfungen der Infrastruktur und der kritischen Applikationen vorzunehmen. So können Sie das Sicherheitsniveau überprüfen lassen und sich optimal vor Angriffen schützen.

Unsere Dienstleistungen

- ▶ **Security Audit** (teilautomatisierte, gezielte Sicherheitsüberprüfung)
- ▶ **Penetration Testing** (intensive Sicherheitsüberprüfung aus der Angreifer-Optik)
- ▶ **Application Security Audit** (gezielte Sicherheitsüberprüfung einer Applikation)

Um eine ganzheitliche Sicherheitsüberprüfung vorzunehmen, empfehlen wir ein Security Audit, welches die organisatorische und die technische Ebene berücksichtigt. Je nach Anforderung empfehlen wir bei den technischen Aspekten verschiedene Stufen der Überprüfung: Ein Security Audit, um eine gezielte Sicherheitsüberprüfung von kritischen Systemen oder Netzwerk-Komponenten durchzuführen. Ein Penetration Testing, um einen realitätsnahen Hacker-Angriff zu simulieren. Hier kommen verschiedene Tools und die aktuellsten Methoden zum Einsatz, um mögliche Lücken aufzuspüren. Für Datenbanken, Web Applikationen (z. B. eCommerce, Online-Shops) oder Multi Tier Applikationen empfehlen wir unser Application Security Audit. So können Sie das Sicherheitsniveau des überprüften Objekts eruiieren und allfällige Massnahmen zur Erhöhung der Sicherheit einleiten.

Unsere Methode: OSSTMM

Unser IT Security Team verwendet für sämtliche technischen Security Audits den OSSTMM-Standard. Dieser wird von der unabhängigen Organisation ISECOM herausgegeben und permanent weiterentwickelt. Das Open Source Security Testing Methodology Manual (OSSTMM) definiert eine umfassende, sehr praxisbezogene und zu diversen Standards (z. B. ISO 27001/2) kompatible Methodik zur Planung, Durchführung, Dokumentation von technischen Audits und der Bewertung der Ergebnisse (Sicherheitsniveau als objektiver Zahlenwert). Die Security Consultants von bw digitronik sind nach OSSTMM-Standard als OPST und OPSA zertifiziert.

Fordern Sie uns heraus für Ihre Informationssicherheit!

Unsere Spezialisten stehen Ihnen gerne zur Verfügung: 044 905 48 50