InfoGuard
SWISS CYBER SECURITY

PENETRATION TESTING UND ETHICAL HACKING

Ihre technischen Sicherheitssysteme auf hartem Prüfstand.

PENETRATION TEST – GEZIELT, EXAKT, BEWÄHRT UND HILFREICH.

Die Risikoreduktion, gesetzliche Bestimmungen und die Sorge um das eigene Image sind die am häufigsten erwähnten Gründe für Investitionen in die Informationssicherheit. Informationssicherheit ist aber bei weitem mehr als «nur» die Vermeidung von Missständen. Dies erst ist die Voraussetzung, dass die heutigen Technologien zuverlässig und problemlos genutzt werden können, um die Qualität des Unternehmens zu steigern.

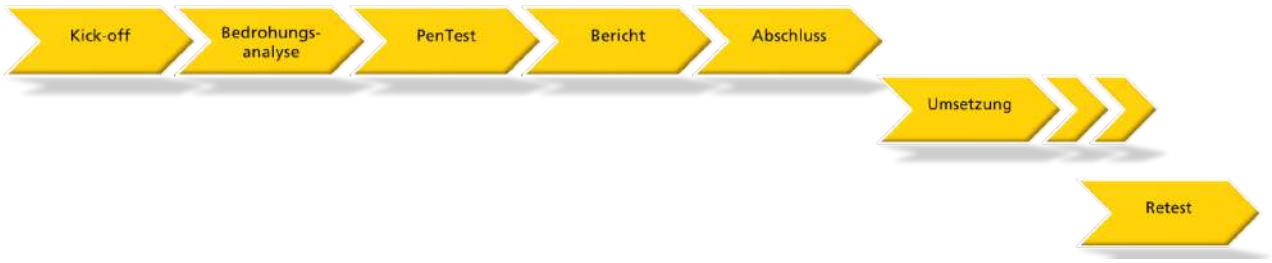
Mit einem Penetration-Test führen unsere Sicherheitsexperten einen echten Angriff durch. Dabei zeigt sich, ob die Infrastruktur gegenüber Angriffen von aussen und innen ausreichend geschützt ist und mit den akzeptierten Restrisiken im Einklang steht.

Das Ziel von Penetration-Tests ist eine Überprüfung der IT-Sicherheit. Durch die kontrollierte Durchführung eines Angriffs werden besonders realitätsnah Schwachstellen aufgedeckt. Die Bandbreite der getesteten Systeme erstreckt sich dabei von Netzwerkdiensten und Online-Shops, über komplexe Unternehmensnetzwerke bis hin zum Benutzer der Infrastruktur.

Um diese entscheidenden Faktoren eingehend zu prüfen, bieten wir modulare Penetration-Tests an. Sie reichen von passiver Informationsgewinnung, über gezielte externe Penetration-Tests aus dem Internet bis hin zur Identifikation von Schwachstellen, die nur vor Ort festgestellt werden können. Unser Vorgehen orientiert sich dabei an den anerkannte Methoden OWASP, OSSTMM und ISO 27001.

Unsere Dienstleistungen beinhalten:

- Deckt potentielle Schwachstellen in Sicherheitskonzepten, Systemen und Anwendungen auf.
- Analysiert die IT-Infrastruktur und wertet die vorhandenen Schutzmassnahmen aus.
- Erhöht die Integrität, Vertraulichkeit und Verfügbarkeit von Daten, Anwendungen und Systemen durch erprobte Sicherheitsmassnahmen.
- Unterstützt bei der Erfüllung gesetzlicher Bestimmungen und weiterer Compliance-Anforderungen.



1 Planung der Angriffs-Szenarien

Der Penetration-Test findet in der Regel in mehreren Schritten statt. Zunächst gilt es, die Ziele der Überprüfung zu definieren und den Einsatz der gewählten Technologien und Methoden abzustimmen. Auf das Kick-off-Meeting folgt eine eingehende Bedrohungsanalyse. Damit erhalten wir ein erstes Bild der vorhandenen Topologie, das heisst der Infrastruktur, Systeme und Applikationen, ohne bereits in die erkannten Systeme einzubrechen (Blackbox-Ansatz).

Anhand der Resultate dieser ersten Phase werden die eigentlichen Angriffs-Szenarien mit dem Kunden diskutiert und definiert. Das Ergebnis ist ein individueller Penetration-Test, welcher der Bedrohungslage des Kunden umfassend gerecht wird.

Die Infrastruktur wird mit den abgestimmten Angriffsarten überprüft. Dabei wird geklärt, ob das Firmennetzwerk tatsächlich gegen gezielte Attacken ausreichend geschützt ist. Bei diesem Testlauf werden zunächst gefundenen Schwachstellen gezielt ausgenutzt und dazu verwendet, weitere Systeme zu attackieren, um so tiefer in das Netzwerk vordringen zu können. Finden unsere Spezialisten kritische Sicherheitslücken, werden diese umgehend gemeldet und vorrangig behandelt. Im Rahmen unseres Penetration-Tests setzen wir verschiedene Angriffstechniken ein.

2 Angriffstechniken

Infrastruktur-Tests

Für die Simulation eines konkreten Angriffs verwenden wir eine Vielzahl von manuellen Tests. Unser Team versucht dabei, erkannte Schwachstellen in der Infrastruktur gezielt auszunutzen, um unberechtigten Zugriff auf das Netzwerk oder einzelne Computer zu erhalten, dabei überprüfen wir:

- die Fernzugänge (RAS- oder VPN-Zugänge)
- die Server-Infrastruktur (Domain Controller, DNS-Server, Terminal-Server, etc.)
- den Malware-Filter beim E-Mail-Übergang und dem Internet-Zugang.

Wir führen die Penetration-Tests dabei von intern und extern durch. Zudem überprüfen wir auch wie die Sicherheitssysteme konfiguriert und implementiert wurden.

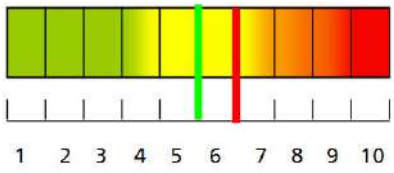
Webapplikations-Tests

Beim Web-Hacking überprüfen wir gezielt Webapplikationen auf Schwachstellen wie z. B. Cross-Site-Scripting oder SQL-Injection, aber auch auf (logische) Fehler in der Authentisierung, resp. Autorisierung oder beim Session-Handling. Die Analyse wird situativ mit insgesamt 25’000 verschiedenen automatisierten und manuellen Einzeltests durchgeführt.

Benutzerverhalten

Um die Sicherheitssysteme zu umgehen, setzen wir auch auf Social-Engineering-Methoden. Dabei überprüfen wir das sicherheitsbewusste Handeln der Mitarbeitenden. Zum Beispiel versuchen wir über Phishing-Mails und mittels DriveBy-Infektionen oder Inside-Out-Attacken sensitive Informationen oder Passwörter zu erhalten.

3 Analyseergebnisse und Testbericht



Zum Schluss erhält der Kunde einen umfangreichen Testbericht Dieser stellt sicher, dass die Ergebnisse stufengerecht präsentiert werden und nachvollziehbar sind. Der Bericht umfasst dazu den detaillierten Ablauf und die Erkenntnisse aus dem Penetration-Test. Zu jeder gefundenen Schwachstelle wird eine ausführliche Dokumentation erstellt, welche beschreibt, was für eine Sicherheitslücke vorliegt und wie diese ausgenutzt werden kann. Dazu wird eine spezifische Risikoanalyse erstellt, welche das Gefahrenpotential der Lücke in den Gesamtkontext des Unternehmens-Netzwerks stellt.

Als Abschluss folgen konstruktive Lösungsvorschläge zu den einzelnen Schwachstellen, um die Sicherheit direkt zu optimieren. Abhängig von den eingesetzten Betriebssystemen und Applikationen werden zudem noch generelle Checklisten zur Erhöhung der Sicherheit abgegeben. In einem abschliessenden Workshop wird der Testbericht mit dem Kunden diskutiert und die weiteren Schritte vereinbart.

Wir verfügen über ausgewiesene Spezialisten der Informationssicherheit mit langjähriger Erfahrung im Lokalisieren und Testen von Schwachstellen in Applikationen, Systemen, Netzwerken und Konfigurationen. Durch die ständige Veränderung der IT-Landschaft kommen fast monatlich neue Lücken hinzu. So halten sich unsere Penetration-Tester immer auf dem aktuellen Stand der Technik um einen realistischen Angriff durchzuführen. Unser breites technisches Know-how in den Bereichen Betriebssysteme, Sicherheitssysteme, Applikationen und Datenbanken können Sie gerne im Rahmen zusätzlicher Services in Anspruch nehmen.

INFOGUARD – IHR QUALIFIZIERTER PARTNER FÜR DIE TECHNISCHE SICHERHEITSÜBERPRÜFUNG

Ihre Geschäftsprozesse funktionieren nur, wenn stets die richtigen Informationen zur richtigen Zeit am richtigen Ort vorzufinden sind. Vertraulichkeit, Integrität und Verfügbarkeit der Informationen spielen dabei eine bedeutsame Rolle.

InfoGuard bietet eine unabhängige Überprüfung Ihrer Informationssicherheit. Dabei zeigen wir auf, welche organisatorischen, technischen und personellen Schwachstellen in Ihrem Unternehmen vorliegen und wie Sie diesen begegnen können.

Unsere Dienstleistungen umfassen die Bereiche:

- Security Audit nach ISO 27001/27002
- GAP-Analyse hinsichtlich einer ISO 27001-Zertifizierung
- System- und Architektur-Review
- Penetration Test nach OSSTMM
- Vulnerability Scan
- Social Engineering Audit

Ihre Sicherheit ist unser Ziel –
wir analysieren und optimieren Ihr Sicherheitssystem!

InfoGuard – Der Schweizer Cyber Security Experte

InfoGuard ist ein Schweizer Experte für umfassende Cyber Security und innovative Netzwerklösungen. Sie profitieren von unserer Erfahrung, Professionalität und Zuverlässigkeit im Audit, in der Beratung, Architektur und Integration führender Netzwerk- und Security-Lösungen. State-of-the-Art Cloud-, Managed- und Cyber Defence-Services erbringen wir aus dem ISO 27001 zertifizierten InfoGuard Cyber Defence Center in der Schweiz.

InfoGuard AG
Lindenstrasse 10
6340 Baar / Schweiz
Telefon +41 41 749 19 00

Office Bern
Stauffacherstrasse 141
3014 Bern / Schweiz
Telefon +41 31 556 19 00

INFOGUARD.CH