

# AUDIT MODULE 2009/2010

## 1. Extern

### Modul 1.1 - externer Audit

- Information Gathering
- Portscan – Feststellen der erreichbaren Dienste
- Dienstidentifikation
- manuelle Identifikation konfigurationsabhängiger Schwachstellen
- teilautomatisierte Identifikation von bekannten Schwachstellen
- Angriffsversuche auf Managementinterfaces

### Modul 1.2 – Webapplikationsaudit

- Information Gathering
- Session-ID Analyse
- Testen auf sichere Parametervalidierung
  - Cross Site Scripting
  - SQL Injection
  - XML/XPath Injection (bei WeBservices)
  - Inclusion Attacks
  - Fuzzing
- Cookie-Diebstahl (Session Hopping, Session Fixation, etc.)
- Testen der Authentifizierungsmethoden (Managementinterfaces, etc.)
- unauthorisierte Uploadversuche
- Angriffsszenarien bei denen Angriffsmethoden kombiniert werden
- Prüfung der Webserverkonfiguration
- teilautomatisierte Identifikation von bekannten Schwachstellen in der Serversoftware



### Modul 1.3 - Social Engineering

- Informationsbeschaffung und Vorbereitung
- Vortäuschen falscher Identitäten und Kompetenzen, um an geheime Daten zu gelangen oder Services zu erschleichen
- Durchführung per Telefon oder Email
- genaue Vorgehensweise wird an Kundenwünschen und organisations-spezifische Gegebenheiten angepasst



## 2. Intern

### Modul 2.1 - interner Audit

- Blackbox Teil:
  - Überprüfung des Zugangsschutzes zum Netzwerk
  - Schwachstellenanalyse in Server-, Benutzer- und Außenstellennetzwerken
  - Angriffe auf Netzwerkkomponenten, Server und Clients
  - Versuch Berechtigungen im Netzwerk zu erlangen und diese auf domänenweite Administratorberechtigungen auszubauen
  - Schwachstellenanalyse der vorhandenen Datenbanken
  - Schwachstellenanalyse der vorhandenen Intranetserver
  - Prüfung auf Konfigurationsschwachstellen in Netzwerkkomponenten und Servern
  - Erhebung des Verbesserungspotenzials
- White-Box Teil:
  - Topologie Audit: Überprüfung des Netzwerkaufbaues, Trennung
  - Schwachstellenanalyse und Erhebung des Verbesserungspotenzials

### Modul 2.2 – WLAN Audit

- Überprüfung der implementierten Verschlüsselung
- Prüfung von Abschottung und Filterung des WLANs
- Wardriving/Warwalking
- Identifikation unternehmensfremder Funknetzwerke

### Modul 2.3 - VoIP

- Überprüfung der VoIP-Basisinfrastruktur auf OS und Applikationsebene
- Überprüfung der eingesetzten Protokolle und Sicherheitsmechanismen
- Abhörversuch (in Abstimmung)
- Aufbereiten des Verbesserungspotenzials

### Modul 2.4 - Social Engineering

- Informationsbeschaffung und Vorbereitung
- Prüfung der physischen Zugangssicherheit
- Physikalische Sicherheit von Servern und Netzwerkkomponenten
- Vortäuschen falscher Identitäten und Kompetenzen, um an geheime Daten oder kostenlose Services zu gelangen
- Durchführung vor Ort
- genaue Vorgehensweise wird an Kundenwünschen und organisationsspezifische Gegebenheiten angepasst

# AUDIT MODULE 2009/2010

## Modul 2.5 - Organisations-Audit

Überprüfung der IT Sicherheitspolitik und Statusdokumentation unter folgenden Aspekten:

- Verantwortlichkeiten
- IT Organisation
- Sicherheits-Management Team
- Risikoanalyse
- Datenklassifizierung
- Datenintegrität
- Reporting

## Modul 2.6 - Verfügbarkeits- und Infrastruktur-Audit

- Bauliche Maßnahmen
- Feuerschutz
- Zugangsschutz
- Netzwerktopologie
- SAN Infrastruktur
- Server Infrastruktur
- Client Infrastruktur
- Basisdienste (DHCP, DNS, AD, ...)
- Wartungsverträge
- SLA Überprüfungen
- Datensicherung
- Schatten-EDV



## Modul 2.7 - Security Coaching

- Erhebung der Ist-Situation im Workshop
- Definition und Gewichtung von Zielen
- Entwicklung von Sicherheitsmaßnahmen nach Best Practices
- Empfehlungen zu technischen und strategischen Maßnahmen
- Planung langfristiger Strategien
- Projektbegleitung



# AUDIT MODULE 2009/2010

## Modul 3 - Code Audit

- Kick-Off Workshop
- Überprüfung von Eigenentwicklungen (Webapplikationen, Client- und Serversoftware)
- teilautomatisierte Prüfung des Sourcecodes auf Schwachstellen
- Durchspielen von Angriffsszenarien am Testsystem

## Modul 4 - Managementpräsentation

- Aufbereitung der Ergebnisse für das Management
- Präsentation und Diskussion

## VERTRAUEN IST GUT, ANTARES IST BESSER!

In den letzten acht Jahren hat sich Antares NetlogiX als kompetenter IT Dienstleister bewährt. Vom Schwerpunkt **Netzwerk und System Management** kommend, wurde der Fokus zunehmend um **Hoch-Sicherheitslösungen** erweitert. Der stark wachsende Dienstleistungsbereich, und hier vor allem Managed Services, IT Projekt Management Unterstützung sowie Schulungen, sind nun ein weiteres Standbein des ambitionierten Unternehmens mit seinen 25 Mitarbeitern.

Unter anderem ist Antares NetlogiX ein permanent **geschulter** und **zertifizierter Projektpartner** von marktführenden Herstellern. Integrative Lösungen und erfahrene Mitarbeiter mit fundierter Ausbildung sorgen für einen reibungslosen IT Ablauf. Falls dennoch Fragen auftreten, steht der eigene **Help-Desk mit 6 Mitarbeitern** stets als Ansprechpartner zur Verfügung – ohne Zusatzkosten. Antares NetlogiX erreichte 2008 über 3,8 Mill. Euro Umsatz und ist österreichweit sowie im angrenzenden Ausland (Deutschland, Schweiz, Slowakei, Tschechien, Südtirol) tätig.

Umfassende **Projektbegleitungen**, von der **Ausschreibungsunterstützung** bis hin zu komplexen **Netzwerk- und Sicherheitsberatungen**, führten dazu, dass **IT Managementmethoden** eingeführt wurden und auch für Kunden angeboten werden.

Viele der größten IT Infrastrukturen in Österreich vertrauen bereits seit mehreren Jahren auf die Betreuung durch Antares. ITK Unternehmen, Systemhäuser, internationale Konzerne aller Branchen sowie Ministerien und andere öffentliche Einrichtungen (vor allem im Gesundheitswesen) setzen auf eine kompetente und flexible Beratung.