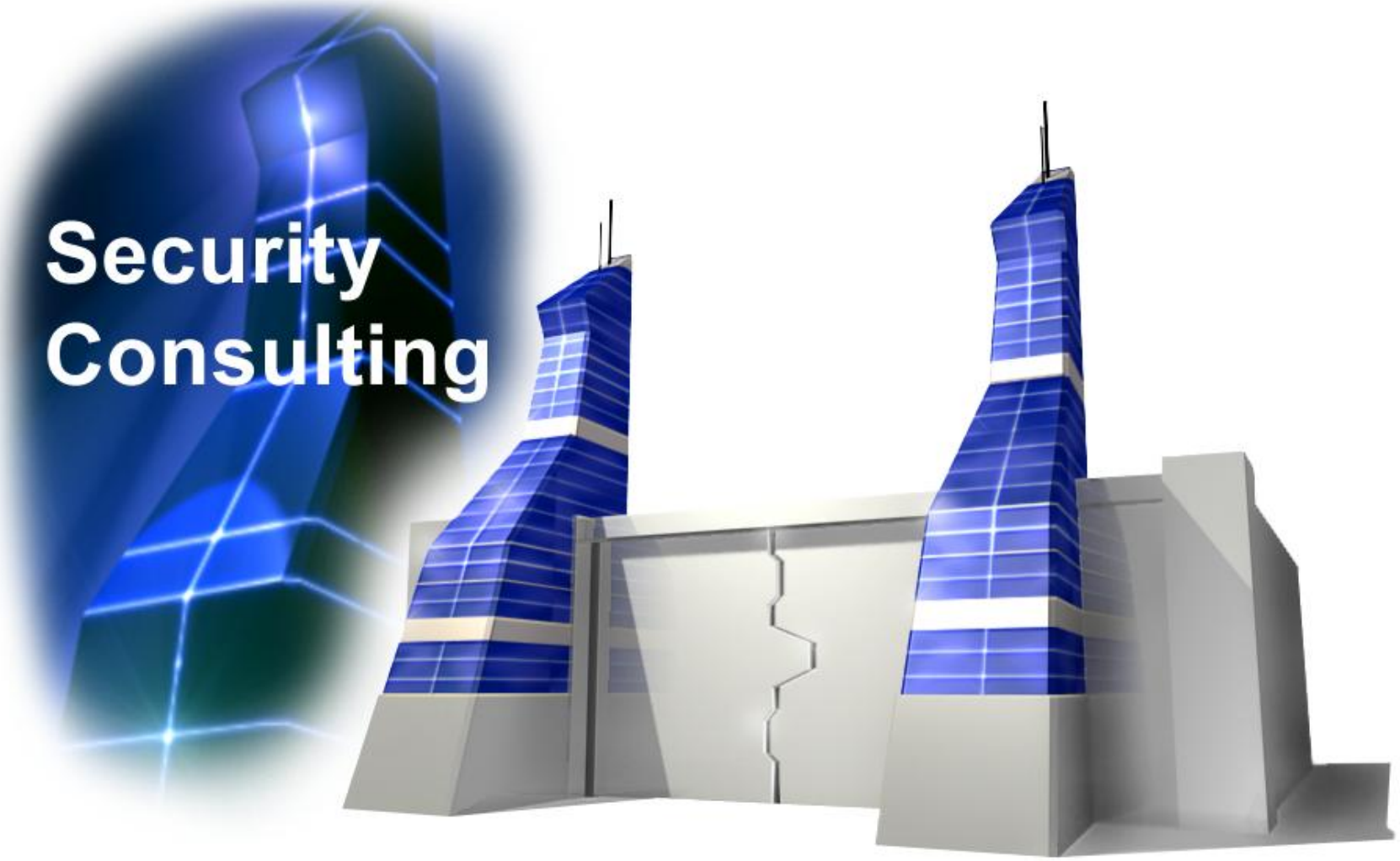
ATEGRA Domino Security Audits



Ausgangslage

- Ihre Organisation hat Sicherheitsbedürfnisse
- Sie führen evtl. bereits periodische Security Audits durch
- Oft wird der Teil Lotus Domino technisch ausgelassen

ATEGRA Security Dienstleistungen

1. Periodische Security Audits
   - ATEGRA prüft Ihre Systeme nach Ihren Anforderungen und Ihrem Bedarf
2. IT Security Policy Audit
   - auch als Teil der periodischen Security Audits
3. Periodische Prüfungen auf bekannte Sicherheitslücken
   - ATEGRA prüft Ihre Systeme periodisch auf publizierte Sicherheitslücken (sog. Exploits)
4. Einmalige Penetration-Tests
   - ATEGRA prüft Ihre Systeme nach einem vorbestimmten Szenario auf Schwachstellen
5. Security Newsletter
   - ATEGRA sammelt die bekanntesten und renommiertesten Security-Newsletter. Sie bekommen ein massgeschneidertes Newsletter das nach Ihren Bedürfnissen gefiltert wurde.

Security

- CIA & N
  - C = Confidentiality
  - I = Integrity
  - A = Availablity
  - N = Non-Repudiation

ISO 17799

- ATEGRA orientiert sich an ISO 17799
- Elemente ISO 17799
  1. Business Continuity Planning
  2. System Access Control
  3. System Development and Maintenance
  4. Physical and Environmental Security
  5. Compliance
  6. Personnel Security
  7. Security Organisation
  8. Computer & Network Management
  9. Asset Classification and Control
  10. Security Policy
- Anmerkung zu BS7799: ISO/IEC 17799 wandelt den britischen Standard BS 7799, der in vielen Ländern übernommen wurde, in einen internationalen Standard um. Man geht davon aus, dass der ISO/IEC 17799 Standard in Zukunft das Referenzdokument für sicheren und zuverlässigen e-commerce sein wird. ATEGRA bietet Ihre Dienste in Übereinstimmung mit diesem Standard an

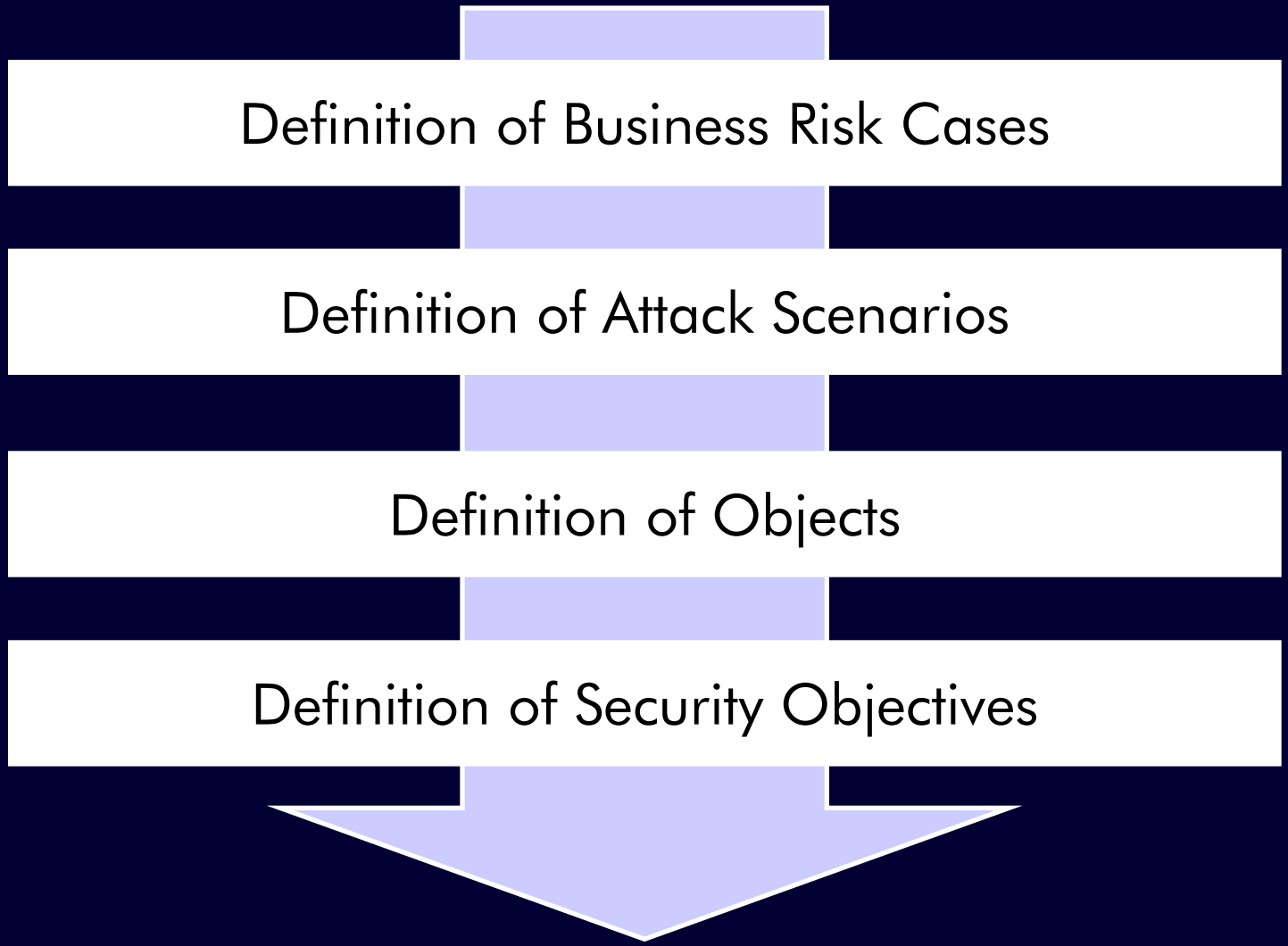
CobiT- Control objectives for information and related Technology

- ATEGRA orientiert sich an CobiT
- CobiT liefert die Rahmenbedingungen für die Implementierung von Zielvorgaben für die Steuerung und Überwachung der gesamten IT.
- Das CobiT-Projekt wird von einem Projektteam bestehend aus internationalen Vertretern aus Industrie, Bildungswesen, Regierung und aus der Sicherheits- und Kontrollbranche beaufsichtigt. Das Projektteam war bei der Entwicklung des CobiT-Framework und in der Verwendung der Forschungsresultate behilflich. Internationale Arbeitsgruppen wurden zum Zweck der Qualitätssicherung und zur professionellen Überprüfung der vorläufigen Forschungs- und Entwicklungsergebnisse etabliert. Für die übergreifende Projektleitung ist das IT Governance Institute verantwortlich.
- Siehe http://www.isaca.org/cobit.htm
- http://de.wikipedia.org/wiki/Cobit

Typische Sicherheitsrisiken in Lotus Domino-Umgebungen

1. Offene ACL (Access Control List) in Datenbanken
   - Interne Mitarbeiter können zugreifen wo sie nicht dürfen
   - Externe können Daten abrufen, wo sie nicht dürfen
2. ACL des Domino-Directory und anderer System-Datenbanken wie log.nsf, admin4.nsf
3. Web-Zugang
   - Ist offen für Millionen von neugierigen Internauten
4. Domino-Server-IDs und deren Passwörter
   - Kann die Server-ID entwendet/kopiert werden?
5. User-ID-Security: Passwörter-Qualität
6. Ihre System-Administratoren haben viel zu tun und oft reicht die Zeit nicht für Prüf-Vorgänge → Delegation an Externe ist sinnvoll

Methodik


Definition of Business Risk Cases
Definition of Attack Scenarios
Definition of Objects
Definition of Security Objectives

Risk Cases

- Die Angriffe basieren auf gemeinsam spezifizierten Szenarien. Ausgangslage für die Angriffsszenarien sind Risk-Cases. Beispiele für Risk-Cases sind:
  - Nicht-Verfügbarkeit einer Web-Site (z.B. Ausfall Web-Server On-Line-Shop)
  - Ausfall „mySAP XXX“
  - Einspeisen von falschen Bestelldaten
  - illegale Mutationen im Artikelstamm
  - Erschleichen von Leistungen
  - Ausfall Incoming-Mail
  - Ausfall Outgoing-Mail
  - Ausfall POS-System

Angriffs-Szenarien

- Aufgrund der Risk-Cases werden gemeinsam kundenspezifische Angriffsszenarien spezifiziert und anschliessend gemäss Risiko R priorisiert (R = grob geschätzte Eintretenswahrscheinlichkeit x grob geschätzte Schadenskosten).
- Ein Angriffsszenario enthält
  1. eine Vorgeschichte
  2. den Risk-Case und
  3. eine Beschreibung der Folgen

Objekte

- Die Angriffe werden auf gemeinsam vereinbarte Objekte gefahren. Dazu werden alle Objekte, die für einen Angriff in Frage kommen, zusammengestellt.
- Potentielle Objekte sind:
  - Aktive Netzwerk-Komponenten (Firewall, Router, Gateway, Proxy Server, Modem)
  - Dienste (Software-Services, z.B. HTTP, SMTP, LDAP, ftp)
  - Rechner mit deren File-Systemen und Hauptspeichern (Server, Workstations, Notebooks, PDA)
  - Personen (Anwender, Kader, System-Administratoren, Entwickler, interne und externe Fachpersonen)
  - Prozesse/Abläufe (z.B. Betreten von Gebäuden und Räumlichkeiten, Support-Request bei Passwort-Verlust)

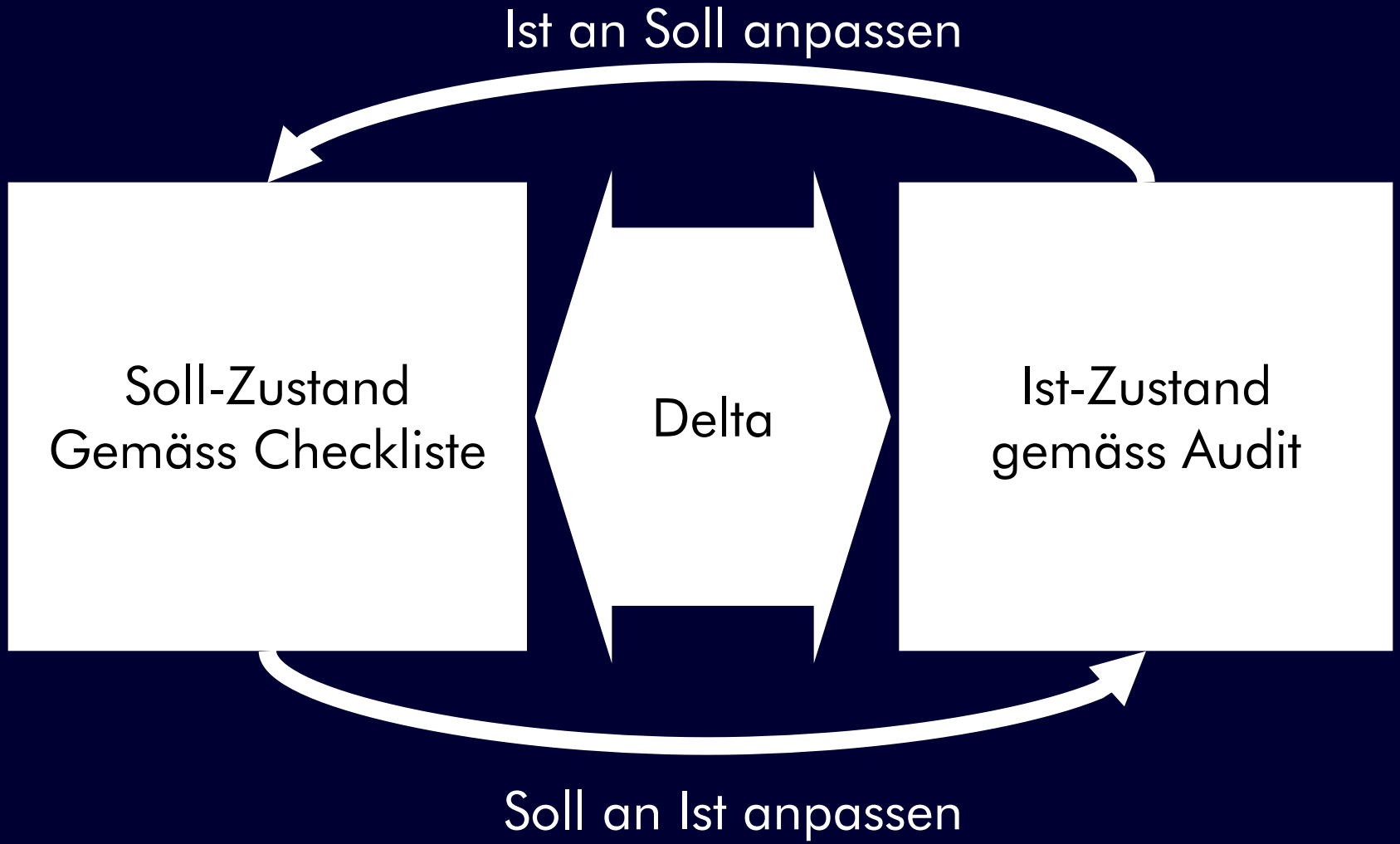
Security Objectives und Angriffs-Aktionen

- Ziel aller Angriffe ist es jeweils, die angegriffenen Objekte in den folgenden Dimensionen (Security Objectives gemäss ISO17799) zu prüfen:
  1. Vertraulichkeit: Kann auf Daten zugegriffen werden, die nicht zugreifbar sein sollten? (Lesezugriffe)
  2. Verfügbarkeit: Kann die Verfügbarkeit von Daten/Diensten beeinflusst/reduziert werden? (Denial of Service)
  3. Integrität: Kann die Integrität von Daten verändert werden? (Schreibzugriffe)

Bericht und Struktur der Befunde

1. Nummer, Bereich und Objekt
2. Befund (Schwachstelle)
3. Informationen für den Nachvollzug des Angriffs (Zeitpunkt, Tool)
4. Potentielle und ggfls. bisherige effektive Auswirkungen (Risiko R = C x P)
5. Empfohlene prophylaktische und/oder Gegen-Massnahmen (konkret)
6. Handlungsbedarf-Priorität 1 (Muss), 2 (Kann) oder 3 (Nice to have) aus der Sicht von ATEGRA (nicht aus der Sicht der Stakeholder des Kunden)

Das Audit-Prinzip



Vorgehen für Domino Security Audit

- Definition des Scope
  - Domänen
  - Server
  - Datenbanken
  - User
- Definition der Business Risk Cases
- Zusammenstellen der Audit Checkliste

Kosten

Variante	Aufwand	Lieferobjekte
Light	1 Tag	Schlussbericht standardisiert
Advanced	2 Tage	Schlussbericht
Professional	4 Tage	Schlussbericht + Präsentation

Andere Audit-Arten in Lotus Domino-Umgebungen

- Anwendungs-Audit
  - Prüfung der Nachvollziehbarkeit
  - Prüfung der Zugriffsrechte Lesen und Schreiben/Mutieren
  - Ist Verschlüsselung angebracht?
    - Auf den Notebook-Festplatten?
    - In den Rich-Text-Feldern?

Weiteres Vorgehen

- Abklären: Wer ist in Ihrer Organisation zuständig?
- Mit ATEGRA Erst-Gespräch führen
  - Umfeld und Ausgangslage
  - Zielsetzungen

Vielen Dank Für Ihr Interesse!