MEMBER OF
CANCOM GROUP

K - Businesscom Deutschland

// we transform for the better

Agenda

- Einleitung
- FAQ und Wichtige Informationen
- Security Services
- Consulting Services

Die Auditoren

Henning Knobloch, MSc

- Security Consultant - Teamleader
- Master of Science
- NSE4 und NSE7 OT-Security
- IT-Grundschutz-Praktiker TÜV

Tobias Brisach

- Security Auditor
- DSB (TÜV)
- ISB
- NSE8
- CISSP
- IT-Grundschutz-Praktiker TÜV
- Prüfverfahrenskompetenz für § 8a BSIG
- ISO/IEC 27001:2022 Lead Auditor CQI IRCA

Einleitung

Fragen zur Ermittlung des Scopes für ein Audit

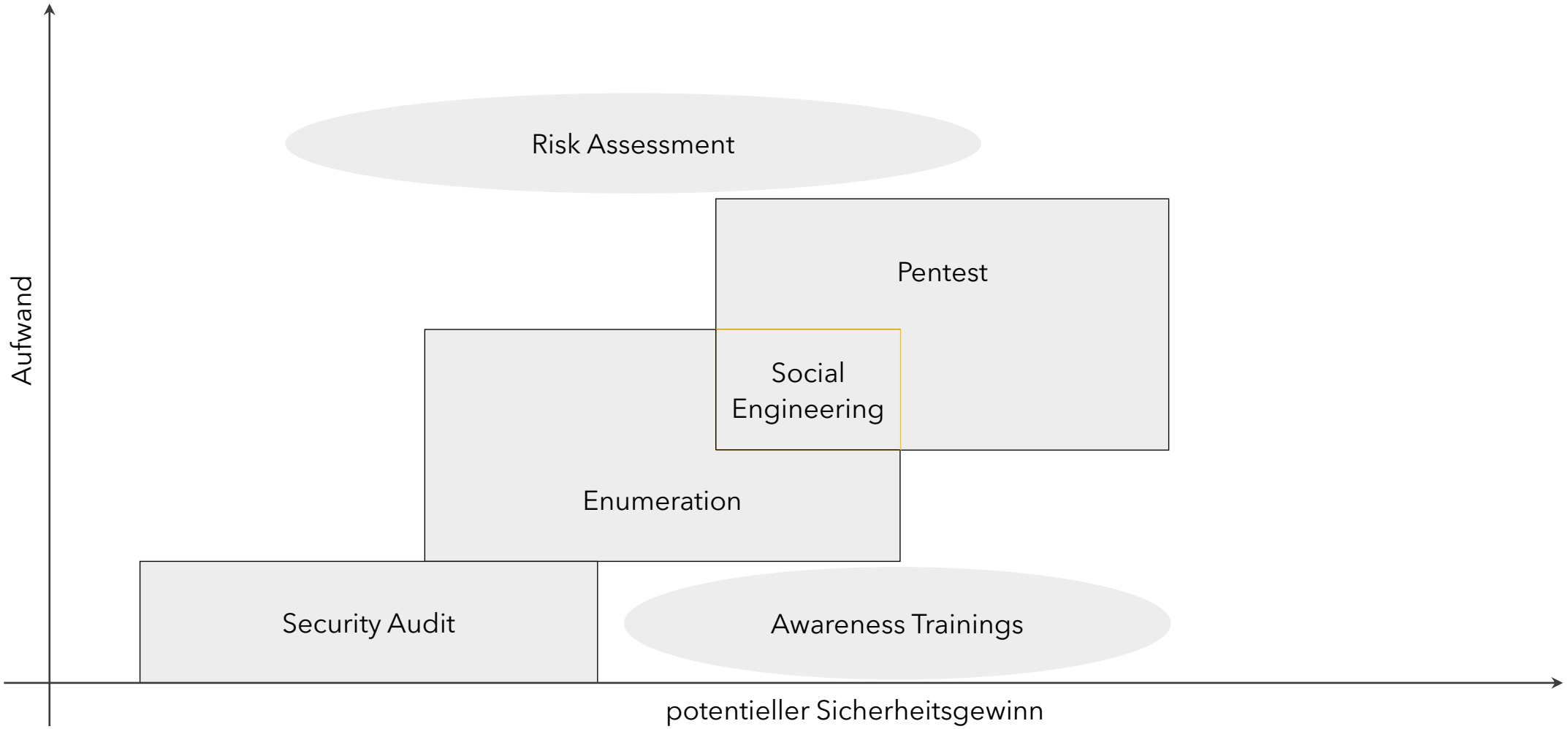
- **Was wird Auditiert ?**
- **Was wird nicht Auditiert ?**
- **Wie viele Assets sollen überprüft werden ?**
- **Wie finden die Audits statt ?**
    - Remote oder vor Ort ?
- **In welchem Zeitraum soll das Audit stattfinden ?**

MEMBER OF CANCOM GROUP

Hinweise und Abhängigkeiten, FAQ

- Dies sind keine Zertifizierungen
- Ihre Mitarbeit ist wichtig
- Der Scope wird für das Angebot benötigt
  - Zu Ihrer Sicherheit halten wir uns streng an den Scope
  - Gerne formulieren wir den Scope gemeinsam
- Der Report schlägt i.d.R. Lösungsansätze vor
  - Projektplanung im Detail im Nachgang auf Anfrage
- Vorlaufzeit mindestens 3 Wochen

Übersicht Security Services



MEMBER OF CANCOM GROUP

Enumeration

Einstieg zur Sicherheit

Ziel Enumeration:

- Sammlung aller zugänglichen Informationen
- Beschaffung von öffentlich Informationen
  - Internetzugänge
  - Onlineauftritte
  - Personendaten
- Beleuchtung der öffentlichen Zugänge
  - Zertifikatsauswertung
  - Suche nach Schwachstellen
  - **WICHTIG Kein Ausnutzen der Schwachstellen**
- Bild vom Kunden in der Öffentlichkeit
- Informationsauswertung und Erstellung des Berichtes

Durchführung:

- Identifizierung der Assets und User
- Identifizierung der Services pro Asset
- Untersuchung von Assets
- Reaktion auf Ergebnisse
  - Unmittelbare Gefahr -> Kunde informieren
  - Identifizierung neuer Assets
  - Aufnahme in Report
- Zusammenfassung in Report
- 2 Auditoren

MEMBER OF CANCOM GROUP

Awareness Training

Sicherheit der Mitarbeiter

Ziel Awareness:

- Schulung von Mitarbeitern
- Social Engineering
- Richtiges Verhalten
- Interne Richtlinien
- Aktuelle Gefahren
- Datenschutz
- Blick auf privates Verhalten

Durchführung:

- Gemeinsame Planung
- Integration lokaler Belange
- Erstellung der Präsentation
- Train the Trainer
- Durchführung Remote oder vor Ort
- 1 Auditor

MEMBER OF CANCOM GROUP

Security Audit

Sicherheit der Konfiguration und Konzepte

Ziel Security Audit:

- Internes Audit
  - Aufnehmen der internen Infrastruktur
  - Überprüfen des Userverhalten
- Identifizierung akuten Schwachstellen
- **Quelle**:
  - Konfiguration
  - Interviews
  - Rundgang
- Bewertung der gefundenen Informationen
- Im Bericht mögliche Verbesserungen
- Grobe Abschätzung Risiko
- **NDA und AVV sind zwingend notwendig !**

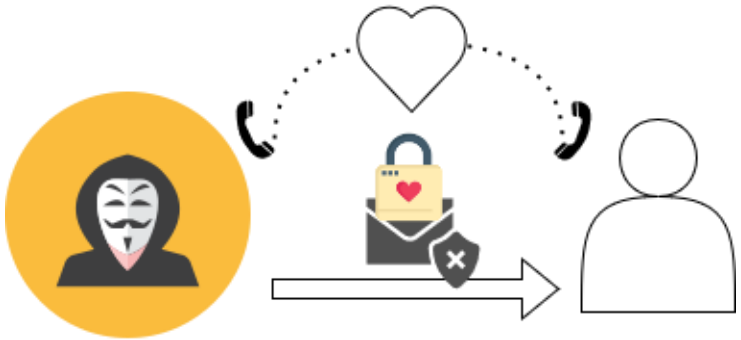
Durchführung:

- Remote oder vor Ort
- Sichtung von Unterlagen und Konfiguration
- Begehung vor Ort
- Reaktion auf Funde
- Sichtung der Richtlinien
- Zusammenfassung in Report
- 1-2 Auditoren

MEMBER OF CANCOM GROUP

Social Engineering Pentest

Angriff auf Mitarbeiter



Ziel Social Engineering Pentest:

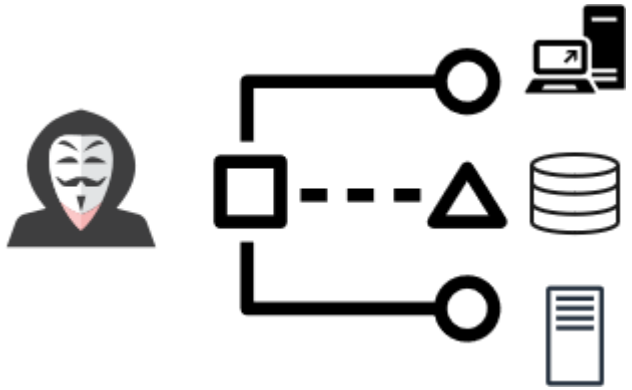
- Überprüfung der Mitarbeiterawareness
- Überprüfung von Prozessen
- Phishing
- Smishing / WHAShing
- Vishing
- Zugang zum Gebäude / Räumen
- Anonymität der Targets, wenn möglich
- Im Bericht mögliche Verbesserungen
- Grobe Abschätzung Risiko
- IdR. nicht ohne Enumeration sinnvoll
- **NDA und AVV sind zwingend notwendig !**

Durchführung:

- Vorbereitung des/der Angriffe
- Remote oder vor Ort
- Ausschluss von Personen und Bereichen
- Zusammenfassung in Report
- 2 Auditoren

Pentest

Angriff auf Kunde



- **Ziel Pentest:**
  - Systeme übernehmen und aktiv Angreifen
- **Erweiterung der Enumeration**
  - Versuchen des Ausnutzen, der bekannten Schwachstellen
- **Zwei Kategorien**
  - extern
    - Mit verschiedenen Tools zum Ausnutzen der Sicherheitslücken
    - Phishing Kampagne zum erhalten von Userdaten
  - intern
    - Versuchen von Zutritt aufs Gelände
    - Versuch von Installation eines Hacking Devices
- **NDA und AVV sind zwingend notwendig !**

Durchführung:

- Drei Varianten:
  - Blackbox – Hoher Aufwand
  - Greybox – Mittlere Aufwand
  - Whitebox – Regulärer Aufwand
- Ausschluss von Personen und Bereichen
- Vorbereitung des/der Angriffe
- Remote oder vor Ort
- Zusammenfassung in Report
- 2 Auditoren

MEMBER OF CANCOM GROUP

Risk Assessment

Angriff auf Kunde

- **Ziel Risk Assessment:**
  - Identifizierung von Risiken
    - Aufnehmen der internen Infrastruktur
  - Identifizierung akuten Schwachstellen
- **Quelle:**
  - Interviews (CRISAM)
- Modellierung der Infrastruktur
- Bewertung durch einfache Fragen
- BIA und RA
- **NDA und AVV sind zwingend notwendig !**

Durchführung:

- Planung der Interviews
- Planung der Softwaremodule
- Remote oder vor Ort
- Zusammenfassung in Report
- 1 Auditor oder Calpana

MEMBER OF CANCOM GROUP

Security Unterstützung/Deinstleistungen

Erhebung der Informationssicherheit in der IT/OT Landschaft

Was machen wir ?

- **Ähnlich eines Security Audits**
    - Rein technische Betrachtung des Bereiches
- **Interviews mit den Administratoren und Verantwortlichen**
- **Abfrage und Bewertung Netzwerkpläne**
- **Abfrage und Bewertung Konfigurationen**
- **Einschätzen Risikopotential**
- **Erstellung eines Reports mit groben Empfehlungen**
    - Keine Projektpläne oder ähnliches
- **Regelmäßige Termine zur Unterstützung**
    - Begleitung im ganzen Prozess

MEMBER OF CANCOM GROUP

Erhebung der Informationssicherheit in Prozessen

Was machen wir ?

- **Ähnlich eines Security Audits**
  - Nur Betrachtung der Prozesse des Bereiches
- **Interviews mit den Administratoren und Verantwortlichen**
- **Interviews mit Usern**
- **Abfrage von Relevanten Prozessen**
  - ZB. Passwortrichtlinien oder User Awareness
- **Abfrage und Bewertung Konfigurationen**
- **Einschätzen Risikopotential**
- **Erstellung eines Reports mit groben Empfehlungen**
  - Keine Projektpläne oder ähnliches
- **Kann für spezielle Prozesse genutzt werden**
  - ZB. Auslieferung von Komponenten oder Inbetriebnahme von neuen Komponenten im eigenen Netzwerk
- **Regelmäßige Termine zur Unterstützung**
  - Begleitung im ganzen Prozess

MEMBER OF CANCOM GROUP

Unterstützung beim Aufbau eines ISMS

Auf Basis der ISO 27001

Was machen wir ?

- **Interviews mit den Administratoren und Verantwortlichen**
- **Interviews mit Usern**
- **Abfrage von Relevanten Prozessen**
    - ZB. Passwortrichtlinien oder User Awareness
- **Unterstützung beim Risk Assessment**
- **Erarbeiten eines gemeinsamen Planes zur Etablierung eines ISMS**
- **Vorbereitung einer ISO Zertifizierung**
    - Bei Bedarf Erstellung der notwendigen Dokumente
    - Beratung zum Best Practice Ansatz
    - Technische Lösungsvorschläge
- **Regelmäßige Termine zur Unterstützung**
    - Begleitung im ganzen Prozess

MEMBER OF CANCOM GROUP

*Unterstützung zum Erreichen der Umsetzungsgrades**

**auf Basis des BSI IT-Grundschutzes*

Was machen wir ?

- **Aufnahme Ist-Stand**
  - Relevante Prozesse und Technische Bereiche
- **Interviews mit den Administratoren und Verantwortlichen**
- **Riskiobewertung**
  - Gemeinsame Klassifizierung der relevanten Assets
  - Erarbeiten einer Priorisierungsliste
  - Erarbeiten von Maßnahmen zum Erreichen des gewünschten Reifegrad
- **Unterstützungsleistung**
  - Technische Beratung
  - Technische Umsetzung
  - Gemeinsame Umsetzung
  - Planung von Netzwerkstrukturen und Assets
  - Erarbeiten von Migrationsplänen
- **Alles Konform dem aktuellen Stand der Technik und IT-SIG**
- **Regelmäßige Termine zur Unterstützung**
  - Begleitung im ganzen Prozess

CANCOM Cyber Security Architektur

(Auszug)

CANCOM Professional Services

(standardisierte Dienstleistungen für **Assess, Analyse, Plan**)

- Security Governance, Policies & Standards
- Security Operations
- Data & Application Security
- Content Security
- Identity Security
- Endpoint Security
- Network & Perimeter Security

Pentest - Ransomware Assurance Assessment „The Ransomware Killer“

IT Sicherheits-audit

Cloud Readiness Workshop

SOC Best-Practice Workshop

Zero-Trust Strategy Workshop

Compliance Suite Starter Pack

Cloud Security Check

PKI Green-/Brownfield Workshops

Zero-Trust Access Assessment

Secure Access Service Edge (SASE) Workshop

Secure Remote Work(shop)

EDR Workshop

Security GAP Analyse

MEMBER OF CANCOM GROUP

Ansprechpartner

Henning Knobloch, M.Sc.
Teamleiter Security Consulting | IT Security Engineer

Henning.Knobloch@k-business.com
+49 2131 9526 123