"T.I.S.P. Community Meeting 2022"

Berlin, 09.-10.11.2022

Gänsehaut garantiert

Die schaurigsten Funde aus dem Leben eines Pentesters

Unser Team - unsere Kompetenz

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Kreativer & professioneller Dienstleister in der IT -Security Branche

Penetrationstests & Sicherheitsuntersuchungen

- Mehr als 200 PT p.a.
- Internationale Kundschaft
- Hohe Expertise

Live Hacking & Cyber Security Shows

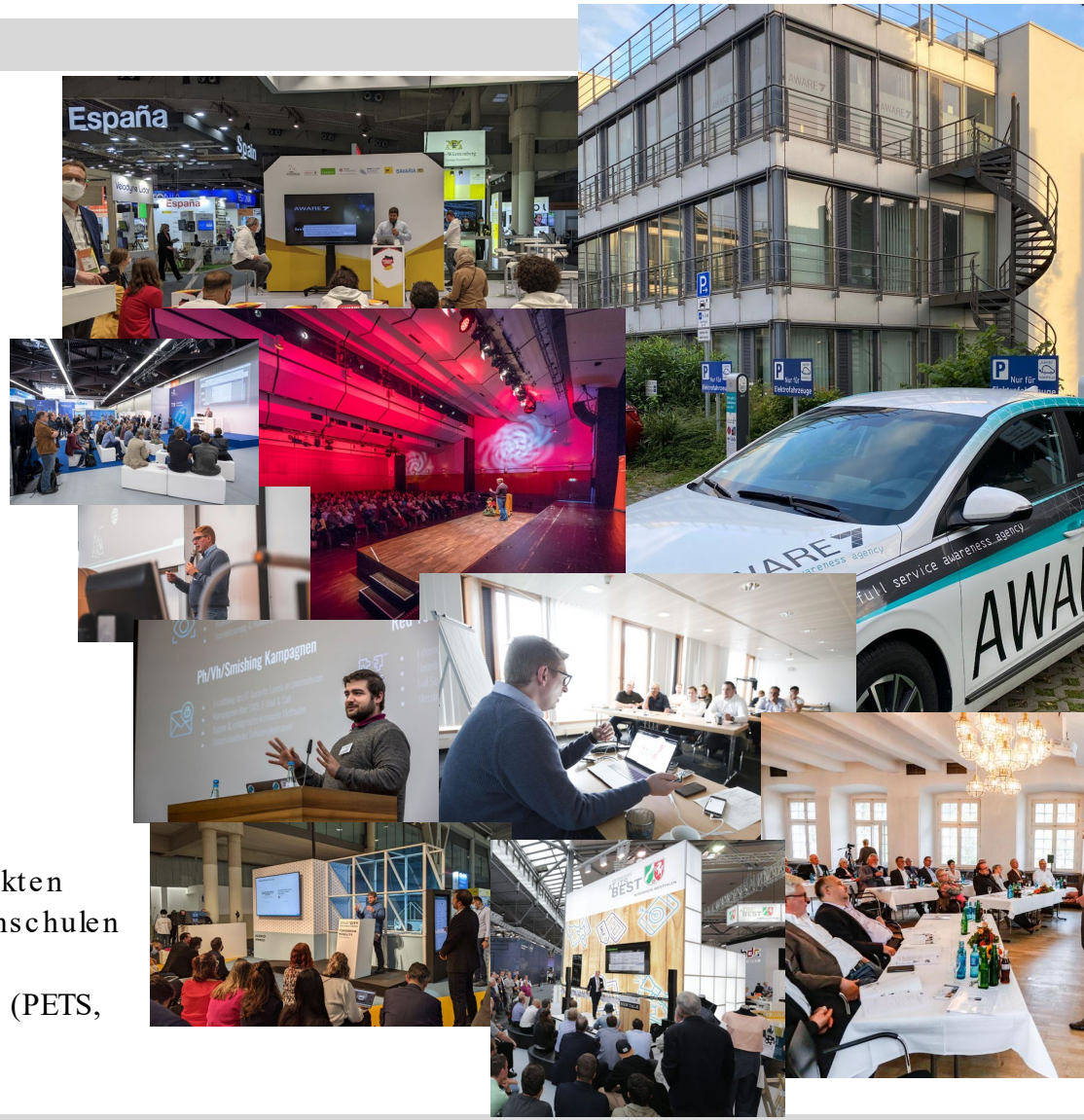
- Projektübergreifender Austausch
- von 30 bis 180 Minuten
- Im Duett und zweisprachig

IT-Sicherheitskonzeption ISO 27001

- Vom Beginn bis zur Zertifizierung
- Partner für internes und zert. Audit
- Bereitstellung von ext. ISBs

Individuelle IT - Security Projekte

- Aus- und Durchführung von individuellen Projekten
- Enge Zusammenarbeit mit Instituten, Fachhochschulen und Universitäten
- Publikationen in Top Konferenzen und Journals (PETS, WWW)



Wer bin ich

M.Sc. Chris Wojzechowski

- **Bachelor of Science**
  Westfälische Hochschule Bocholt
  Wirtschaftsinformatik

- **Master of Science**
  Westfälische Hochschule Gelsenkirchen
  Internet-Sicherheit

- **IT-Grundschutz Praktiker (TÜV)**
  Auf- und Ausbau von ISMS Systemen nach
  ISO 27001 auf Basis des IT-Grundschutzes

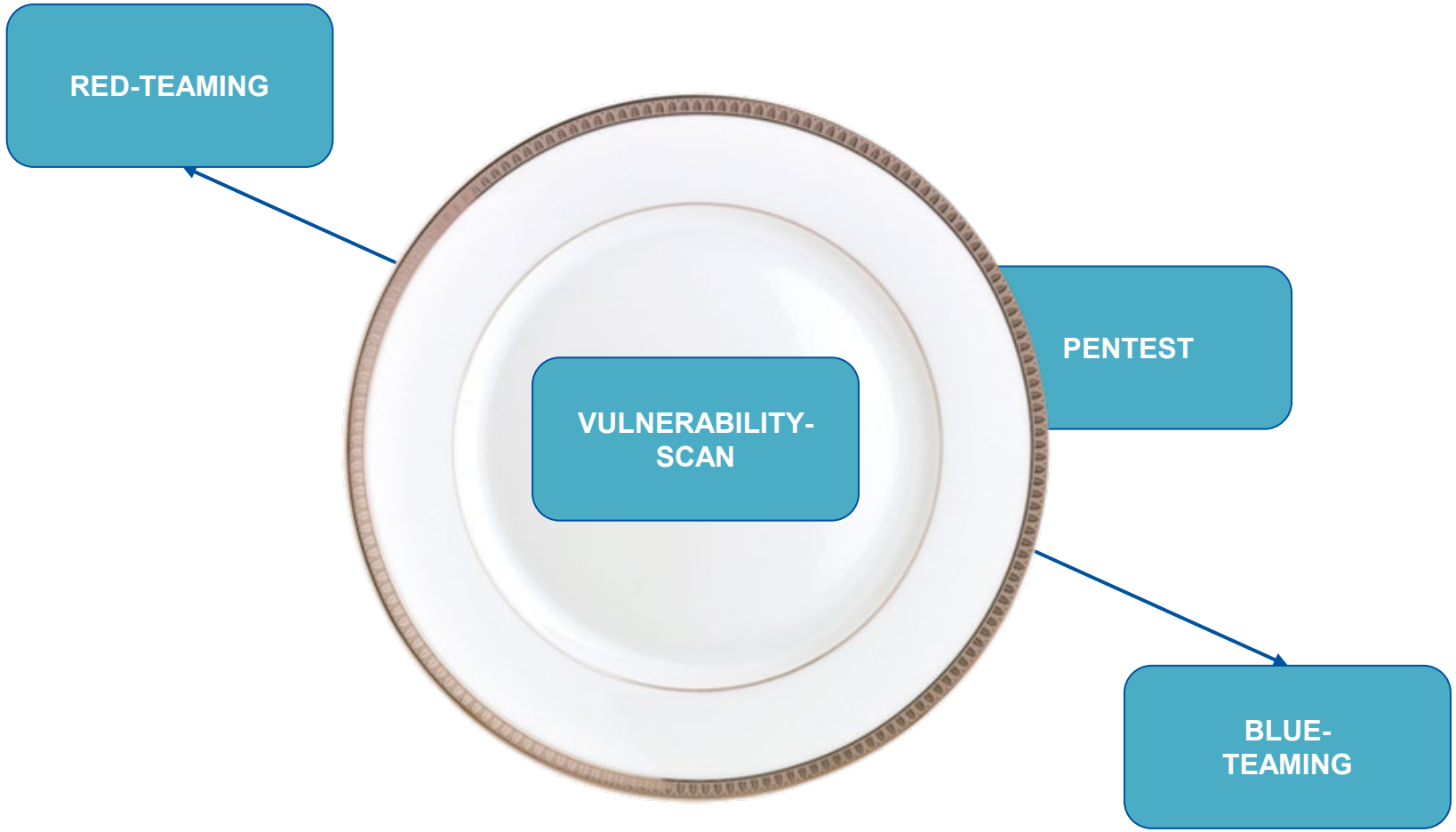
- **IT-Risk Manager (DGI)**
  IT-Risikoanalyse und Bewertung nach ISO 31000

Veröffentlichungen:

Kompass IT-Verschlüsselung
Studie für das Bundesministerium für Wirtschaft und Energie (BMWi)

Meine digitale Sicherheit - Tipps und Tricks für Dummies
Wiley Verlag, 06.10.2021

Einordnung Pentest



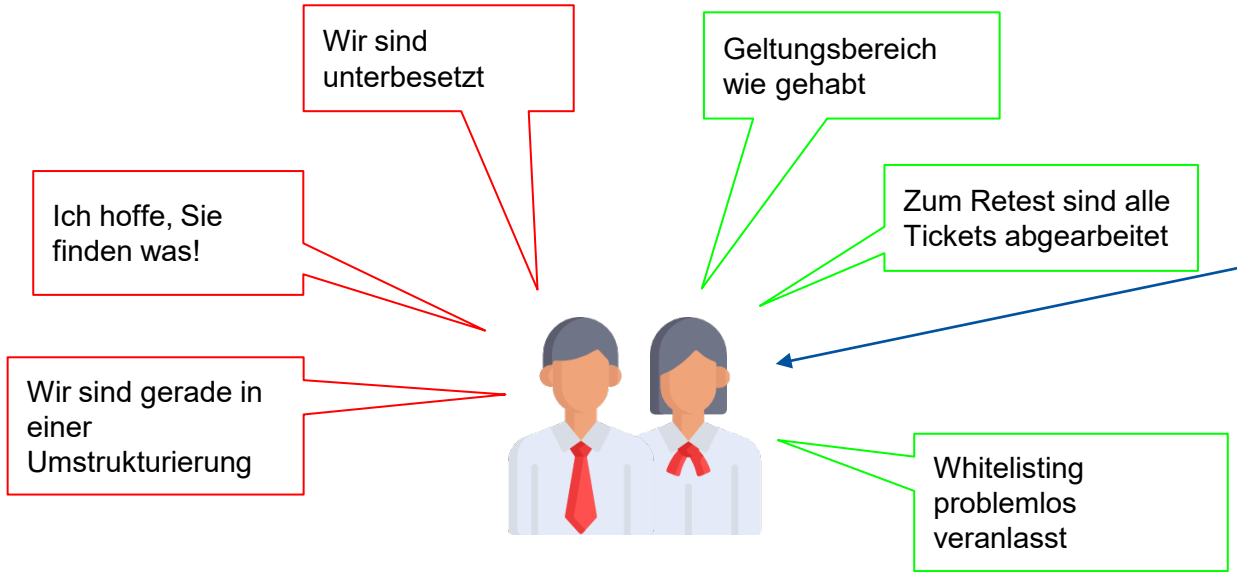
Let’s talk about pentests!

KUNDE
“Wir würden gerne einen Pentest durchführen!”

AWARE7
Erstgespräch, Fragen, Angebot

KUNDE
Rückfragen, Annahme, Kickoff

AWARE7 & KUNDE
Austausch mit Fachabteilung



Finding 1
Wordpress. You’re not alone.

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Viele Webseiten (>70%) laufen auf Wordpress
- Grundsätzlich eine solide Basis
- Gepflegte Systeme sind sicher, ohne menschlichen Faktor

- Personal zur Pflege nötig
- Alternativ dazu ein gewissenhafter Dienstleister

- Durchgeführt wurde ein externer Penetrationstest mit einem Umfang von ca. 5 Tage

Ergebnis: Remote Code Execution im Gallery Plugin

Finding 2
Das Intranet Web Archiv für alle(s) da

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Zugriff auf das Web Archiv im Intranet ohne auth möglich. Gefunden wurde einiges

- Interner Pentest ohne Credentials
- Web Archive waren nur mit Zugang, ohne Auth, für jeden im Netz erreichbar

- “Service” wurde fleißig von ausgewählten Personen genutzt
- Kuriosester Fund: Ein ausgefüllter BAFÖG Antrag eines Admins

Ergebnis: Organisatorische Maßnahmen (z. B. Rechte- und Rollenkonzept)

Finding 3
Die E-Mail ist nicht sicher. Lass Simsem

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Gehacktes SMS Gateway

- Kunde führt Großteil der Kommunikation mit dem Kunden über SMS durch
- Mitarbeiter:innen betreuen Kunden an Workstations
- SMS Gateway schafft Möglichkeiten zur geräteübergreifenden Kommunikation

- Interner Penetrationstest deckt vulnerable Systeme auf
- Darunter auch das eingesetzte SMS Gateway

- Sämtliche Kommunikationsdaten waren mit Standard Admin Zugangsdaten, die in der Dokumentation hinterlegt waren, einsehbar.

Ergebnis: Kommunikation zwischen Kunde und Company im Klartext auffindbar

Finding 4
Unfreiwillige Gastfreundschaft

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Wenn das Active Directory dank menschlicher Bequemlichkeit unsicher ist

- Active Directory ist ein Verzeichnisdienst und der Dreh & Angelpunkt zahlreicher Unternehmen
- Eine Kompromittierung kann zahlreiche Nutzer:innen von Ihren Anwendungen und Zugängen ausschließen

- Die Absicherung des Active Directorys sollte entsprechend hohe Priorität genießen.
- “welcome123” ist dabei zwar leicht zu merken, jedoch nicht sicher.

Ergebnis: Einfache Manipulierung von Benutzern, Daten und Rechten.

Finding 5
In das gemachte Netz will sich keiner setzen

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Ein Netz, wie es keine Spinne spinnen würde. Über 1.000 Systeme erreichbar.

- Interner Pentest im Umfeld einer Behörde
- Zahlreiche Fachanwendungen, (Gäste-) WLAN sowie mehrere Endgeräte im Netz
- Ein Netz, das so groß ist, dass es mehr als 1.000 Systeme zählt.

- Bei der Größe eines solchen Netzes stellt sich nicht die Frage ob, sondern wann die Behörde kompromittiert wird.

Ergebnis: Unverzügliche Maßnahmen zur Isolierung und Netztrennung

Finding 6
Süßes oder Saures zum Schluss…

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

E-Mail-Adresse des Admins in 12 Databreaches gefunden.

- Es wurde ein erweiterter externer Penetrationstest in einem mittelständischen Unternehmen im Lebensmittelsektor durchgeführt
- Im Geltungsbereich waren auch die E-Mail-Adressen der Mitarbeiter:innen, die sich durch Recherchen in Erfahrung bringen ließen

- Über den LinkedIn Account eines Administrators, der dem Unternehmen zugeordnet war, konnte die Corporate E-Mail-Adresse hergeleitet werden
- Datenlecks konnten gegen eine geringe Gebühr (ca. 8 USD) erworben werden.
- Erlangte Informationen konnten beim internen Test genutzt werden um den PC zu entsperren
- “Liebingspasswort” zeichnete sich ab

Ergebnis: Intensive Schulung des Admin-Personals

Vielen Dank für Ihre Aufmerksamkeit

Munscheidstrasse 14, Im Wissenschaftspark 45886 Gelsenkirchen

49 (0) 209 8830 6760

info@aware7.de