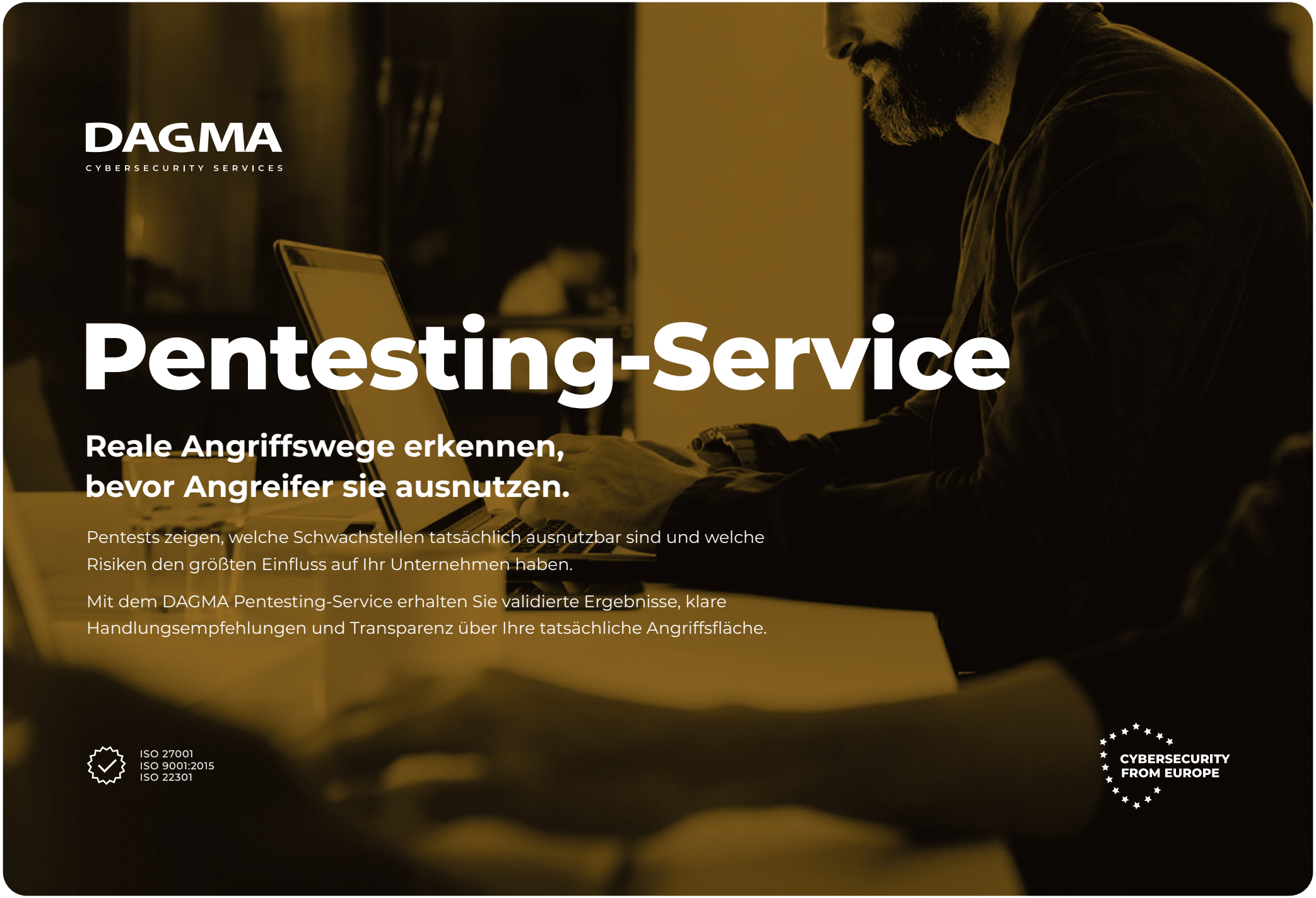

DAGMA
CYBERSECURITY SERVICES

Pentesting-Service

Reale Angriffswege erkennen, bevor Angreifer sie ausnutzen.

Pentests zeigen, welche Schwachstellen tatsächlich ausnutzbar sind und welche Risiken den größten Einfluss auf Ihr Unternehmen haben.

Mit dem DAGMA Pentesting-Service erhalten Sie validierte Ergebnisse, klare Handlungsempfehlungen und Transparenz über Ihre tatsächliche Angriffsfläche.

ISO 27001
ISO 9001:2015
ISO 22301

CYBERSECURITY FROM EUROPE

Vorteile mit DAGMA Pentesting

Sicherheitsrisiken frühzeitig erkennen

Reale Schwachstellen sichtbar machen, bevor sie ausgenutzt werden.

Investitionen gezielt priorisieren

Fokus auf Risiken mit dem größten Handlungsbedarf.

Compliance-Anforderungen unterstützen

Technische Sicherheitsprüfungen zur Unterstützung von NIS2, DORA, ISO 27001, PCI DSS und weiteren regulatorischen Anforderungen.

Sicherheitsniveau objektiv bewerten

Unabhängige Sicht auf die eigene Angriffsfläche.

Warum DAGMA?

6 Monate Retest-Zeitraum

MANUELLE TIEFENANALYSE INKL. RETESTS

Keine automatisierten Scan-Berichte. Jede Schwachstelle wird durch erfahrene Pentester manuell analysiert, validiert und dokumentiert. Ein optionaler Retest (ca. 1-3 Tage) überprüft die erfolgreiche Behebung identifizierter Schwachstellen.

100% validierte Findings

KEINE FALSE POSITIVES

Wir dokumentieren ausschließlich reproduzierbare Findings. Jede dokumentierte Schwachstelle wurde durch einen Pentester validiert und nachvollziehbar nachgewiesen.

OSCP, CEH, CISSP & weitere anerkannte Pentesting-Zertifizierungen

PRAXISERFAHRUNG AUS UNTERSCHIEDLICHEN BRANCHEN

Unsere zertifizierten Pentest-Experten verfügen über langjährige Projekterfahrung in verschiedenen Branchen, u.a. Finanzwesen, Gesundheitswesen, Industrie sowie Handel und öffentliche Einrichtungen.

1 Woche bis zum Abschlussbericht

STRUKTURIERTE BERICHTE MIT HANDLUNGSEMPFEHLUNGEN

Sie erhalten innerhalb von ca. einer Woche einen strukturierten Abschlussbericht mit validierten Findings, Risikobewertungen und konkreten Handlungsempfehlungen.

Mehr als ein automatischer Schwachstellenscan

Jede Organisation verfügt über unterschiedliche Systeme, Anwendungen und Sicherheitsanforderungen. Deshalb folgen unsere Pentests einem strukturierten und bewährten Vorgehen, das den individuellen Prüfungsumfang ebenso berücksichtigt wie die Qualität und Nachvollziehbarkeit der Ergebnisse.

1 SCOPE & ZIELSETZUNG

Gemeinsame Definition von Prüfungsumfang, Sicherheitszielen und Rahmenbedingungen als Grundlage für die Sicherheitsprüfung.

2 VORBEREITUNGEN

Erfassung relevanter Informationen zu Infrastruktur, Anwendungen und organisatorischen Rahmenbedingungen mithilfe eines strukturierten Fragebogens.

3 SICHERHEITS-PRÜFUNG

Durchführung automatisierter Analysen und manueller Tests zur Identifikation von Schwachstellen und potenziellen Angriffspfaden.

4 VALIDIERUNG & RISIKOBEWERTUNG

Verifizierung identifizierter Schwachstellen sowie Bewertung ihrer Ausnutzbarkeit und ihres Risikopotenzials durch unsere erfahrenen Pentest-Experten.

5 REPORTING

Erstellung eines strukturierten Abschlussberichts mit Management Summary, technischen Details und konkreten Handlungs-Empfehlungen.

6 RETEST & NACHBETREUUNG

Überprüfung umgesetzter Maßnahmen sowie Unterstützung bei Rückfragen und der Interpretation der Ergebnisse.

Wir führen Tests in 3 möglichen Varianten durch

Je nach Zielsetzung und verfügbarem Informationsstand kann die Sicherheitsprüfung aus unterschiedlichen Perspektiven durchgeführt werden. Gemeinsam wählen wir den geeigneten Ansatz für Ihre Anforderungen.

Black Box

Unsere Pentester erhalten keine Informationen über die Zielumgebung und bewerten Ihre Angriffsfläche aus Sicht eines externen Angreifers.

Gray Box

Unsere Pentester erhalten ausgewählte Informationen über die Zielumgebung und kombinieren interne Kenntnisse mit realistischen Angriffsszenarien.

White Box

Unsere Pentester erhalten umfassende Informationen und Dokumentationen, um besonders tiefgehende Analysen durchzuführen.

Passender Pentesting Scope

Wir definieren den Umfang eines Pentests gemeinsam mit Ihnen auf Basis von:

Infrastruktur

- Anzahl der Systeme
- Netzwerksegmente
- Öffentliche IP-Adressen
- WLAN-Netzwerke

Anwendungen

- Anzahl der Webanwendungen
- Schnittstellen (APIs)
- Benutzerrollen
- Kritische Geschäftsprozesse

Organisation

- Anzahl der Mitarbeitenden
- Anzahl der Standorte
- Compliance-Anforderungen
- Sicherheitsziele

Individuell statt Standardpaket

Der passende Pentestumfang für jede Anforderung:

- Einzelprüfung
- Kombinierte Assessments
- Compliance-orientierte Prüfungen
- Individuell definierter Scope

Welcher Pentest-Service passt zu Ihrer Angriffs-fläche?

SERVICE 01

Schwachstellenanalyse

Identifikation und Priorisierung bekannter Schwachstellen als Grundlage für gezielte Sicherheitsmaßnahmen und weiterführende Sicherheitsprüfungen.

PRÜFUNGSUMFANG:

- Schwachstellenscans
- Risikobewertung
- Priorisierung kritischer Schwachstellen
- Handlungsempfehlungen

EMPFOHLEN FÜR:

- Erste Sicherheitsbewertung
- Regelmäßige Sicherheitsüberprüfungen
- Vorbereitung auf Pentests
- Begrenzte interne Security-Ressourcen

SERVICE 02

Öffentliche IT-Infrastruktur

Analyse öffentlich erreichbarer Systeme und Dienste aus Sicht eines externen Angreifers zur Identifikation von Schwachstellen und unnötigen Angriffsflächen.

PRÜFUNGSUMFANG:

- VPN-Zugänge
- Mailserver
- Dateiserver
- Öffentliche IP-Adressen
- Exponierte Dienste

EMPFOHLEN FÜR:

- VPN- und Remote-Zugänge
- Internet-exponierte Systeme
- Öffentliche Dienste
- Compliance-Anforderungen

WELCHER PENTEST-SERVICE PASST ZU IHRER ANGRIFFSFLÄCHE?

SERVICE 03

Webanwendungen & API

Überprüfung von Webanwendungen, Kundenportalen und Schnittstellen auf Sicherheitslücken in Authentifizierung, Berechtigungen und Geschäftslogik.

PRÜFUNGSUMFANG:

- Anmelde- und Berechtigungskonzepte
- Programmierschnittstellen (APIs)
- Geschäftslogik
- Sitzungsverwaltung
- Eingabevalidierung

EMPFOHLEN FÜR:

- Kundenportale und Webshops
- SaaS- und Cloud-Anwendungen
- Geschäftskritische Webanwendungen
- Anwendungen mit sensiblen Daten

SERVICE 04

Interne IT-Infrastruktur

Überprüfung interner Netzwerke, Server, Active Directory-Umgebungen und WLAN-Strukturen auf Schwachstellen, Fehlkonfigurationen und potenzielle Angriffswege.

PRÜFUNGSUMFANG:

- Netzwerksegmentierung
- Active Directory
- Server und Clients
- WLAN-Infrastruktur
- Benutzer- und Rechtekonzepte

EMPFOHLEN FÜR:

- Unternehmen mit mehreren Standorten
- Active Directory-Umgebungen
- Komplexe Netzwerkstrukturen
- Kritische interne Systeme

SERVICE 05

Phishing- & Social-Engineering-Tests

Simulation realistischer Angriffsszenarien zur Überprüfung der Widerstandsfähigkeit von Mitarbeitenden, Prozessen und organisatorischen Schutzmaßnahmen.

PRÜFUNGSUMFANG:

- Phishing-Kampagnen
- Telefonbasierte Angriffe (Vishing)
- Sicherheitsbewusstsein
- Organisatorische Prozesse

EMPFOHLEN FÜR:

- Unternehmen mit erhöhtem Phishing-Risiko
- Organisationen mit sensiblen Daten
- Security-Awareness-Initiativen
- NIS2- und Compliance-Anforderungen

DAGMA

CYBERSECURITY SERVICES

dagma.dach@dagma.eu