

FERNAO red team pentest

IHRE VORTEILE

- Praxisnahe Bewertung der Anfälligkeit gegenüber Hackerangriffen
- Identifikation von realen Angriffswegen und deren Schadenspotential
- Evaluation der etablierten Sicherheitsmaßnahmen auf technischer und organisatorischer Ebene
- Ganzheitliche Betrachtung des Unternehmens
- Prüfung der physischen Sicherheit, des Netzwerks, der Anwendungen und der Mitarbeiter
- Manueller Expertentest durch qualifizierte Penetration-Tester aus Deutschland



WANN IST FERNAO RED TEAM PENTEST RATSAM?

- Wenn Sie die Praxistauglichkeit Ihrer Sicherheitsmaßnahmen prüfen wollen
- Wenn Sie schon erste Pentests durchgeführt haben
- Wenn Sie es wirklich wissen wollen

WIE TIEF KANN EIN HACKER IN IHR UNTERNEHMENSNETZWERK EINDRINGEN?

Wie sicher sind wir? Verhindern die zahlreichen organisatorischen, technischen sowie disziplinarischen Maßnahmen wirklich einen Hacker-Angriff? Das ist eine Frage, die viele Unternehmen beschäftigt, denn ein erfolgreicher Hackerangriff ist kostspielig. Datendiebstahl, aber vor allem auch ein teurer Betriebsausfall sind nur zwei mögliche Folgen. Der FERNAO **red team pentest** beantwortet diese Fragen mit Klarheit.

Der FERNAO **red team pentest** ist eine aktive Angriffssimulation, die zeigt, wie anfällig Ihr Unternehmen gegen Hackerangriffe ist. Im Rahmen einer realistischen und praxisnahen Untersuchung zeigt unser Red Team, wie Angreifer in Ihr Unternehmen eindringen und das Netzwerk übernehmen können. Dabei untersuchen wir – je nach vereinbartem Testumfang – die physische Sicherheit, das Netzwerk, die Anwendungen und die Mitarbeiter.

Der FERNAO **red team pentest** zeigt konkrete Strategien und Vorgehensweisen von Angreifern und ermöglicht Ihnen eine vollumfängliche Bewertung der Sicherheit Ihres Unternehmens. Zudem erfahren Sie, wie schnell und zuverlässig Ihr Unternehmen auf Angriffe reagiert.

Sie haben zu jeder Zeit die Kontrolle über den Ablauf des Tests. Kritische Aktionen werden eng mit Ihnen abgestimmt. Als Ergebnis erhalten Sie von unseren FERNAO Experten in einem detaillierten Bericht verwertbare und strukturierte Information über bestehende Schwachstellen und Risiken sowie konkrete Handlungsempfehlungen.

MANAGED SECURITY SERVICES

Genügend Zeit und immer die richtige fachliche Resource verfügbar haben: Das sind großen Herausforderungen der heutigen Unternehmens IT. Zu diesem Zweck haben wir unser Cyber Defense and Operation Center (CDOC) stetig weiterentwickelt. Vom qualifizierten 24x7 Support über einer Reihe von Hosting-

und Management Services bis hin zu unseren Managed Security Services (MSS) verfolgen wir nur ein Ziel: Unseren Kunden die Arbeit zu erleichtern und dabei entsprechend Ihren Anforderungen zu skalieren. Im Fokus unserer Arbeit steht dabei stets die Minimierung des Risikopotentials Ihrer Organisation.

MANAGED SECURITY SERVICES SHIELD

