aroundsec

3-PHASEN KONZEPT

RUNDUM ABSICHERN

AROUND IT-Security GmbH | Tel: +49 7266 44 79 79 0 | Mail: info@aroundsec.de

IHR SCHUTZNIVEAU STEHT BEI UNS IM FOKUS

WER SIND WIR

Die AROUND IT-Security GmbH, auch bekannt als aroundsec, macht mittelständische Unternehmen und Kommunen deutlich widerstandsfähiger gegen Cyberkriminalität.

Die IT-Systeme werden sowohl aus der Sicht eines potenziellen Angreifers (Red Team) als auch aus Sicht eines IT-Administrators (Blue Team) analysiert. Denn die meisten Unternehmen und öffentlichen Einrichtungen sind nur unzureichend geschützt und somit ein besonders lohnendes Ziel für Angreifer.

Unser Fokus liegt besonders auf den häufigsten und schwer-wiegendsten Angriffsarten. Sollte ein Angriff erfolgreich sein, unterstützen wir unsere Kunden zudem dabei, ihre Systeme wiederherzustellen sowie wichtige Daten und Beweise zu sichern.

Unser erfahrenes Expertenteam setzt über gängige Sicherheits-standards hinausgehende Methoden ein, um effektiven Schutz gegen Cyberangriffe zu gewährleisten. Dabei nutzen wir neueste Techniken und Erfahrungen, um sowohl die Wahrscheinlichkeit als auch den potenziellen Schaden von Angriffsarten zu minimieren.

SIMULIERTE ANGRIFFE

SICHERHEITSLÜCKEN AUFDECKEN

PHASE 1

Unsere erfahrenen Hacker führen einen simulierten Angriff durch, um Ihre Systeme auf Herz und Nieren zu prüfen und die relevanten Schwachstellen zu identifizieren.

Ob physischer Zugriff oder Angriffe über das Internet. Es gibt viele Wege, um Zugriff auf Ihre IT-Systeme zu erhalten. Der genaue Umfang / Scope eines solchen Projektes, muss mit Ihren Anforderungen sowie den bereits getätigten Maßnahmen übereinstimmen.

Für unsere Penetrationstests nutzen wir einen eigens entwickelten Test-Katalog aus über 200 verschiedenen Themen. Auch weniger bekannte Schwachstellen werden dadurch abgedeckt.

Leistungsübersicht:

- Interne Penetrationstests
- Externe Penetrationstests
- Web-Penetrationstests
- Penetrationstests von Applikationen
- Notebook-Sicherheitsüberprüfungen
- Innentäter-Analysen
- Physische Sicherheitsüberprüfungen

Wir arbeiten Hand in Hand mit Ihnen, um die identifizierten Sicherheitslücken zu schließen. Unser Ziel ist es, praktische und umsetzbare Lösungen zu bieten, anstatt Sie mit umfangreichen Berichten zu überfordern. Dadurch gewährleisten wir eine schnellstmögliche und maximal effektive Umsetzbarkeit bei der Behebung der Schwachstellen.

HÄRTUNGSMODULE

ABWEHR STÄRKEN

PHASE 2

Die Härtungsmodule sind präventive, also vorbeugende Schutzmaßnahmen zur Verhinderung von Cyberangriffen.

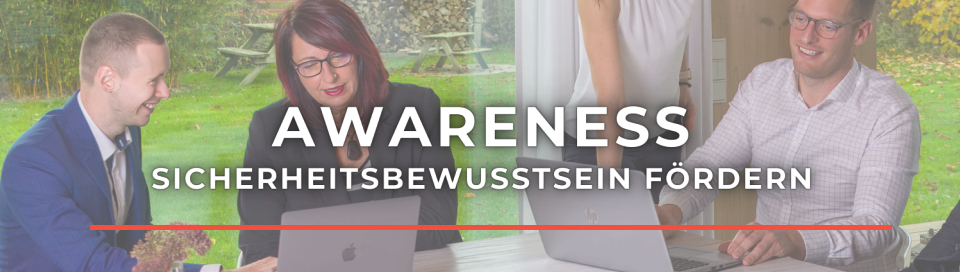
Aus der Sicht eines Angreifers wissen wir, welche Schwachstellen zuerst ausgenutzt werden. Durch eine sogenannte Härtung der Systeme bauen wir hohe Hürden auf, sodass Angreifer schnell das Interesse verlieren.

Dafür nutzen wir unsere eigenes erstellen Härtungsmodule., die wir speziell für den deutschen Mittelstand entwickelt haben. Es werden dabei die Maßnahmen umgesetzt, die den größtmöglichen Sicherheitsgewinn vor potentiellen Hacker-Angriffen darstellen.

Leistungsübersicht:

- Physische Sicherheit
- Administrative Benutzerverwaltung
- Härtung Windows Betriebssystem
- Windows 10 Sicherheitstools
- Datenschutzeinstellungen
- Härtung von Gateways
- Härtung Active Directory
- Härtung von Office
- Härtung der Drucker

Mittlerweile haben wir über 600 Härtungsmodule (also Maßnahmen) entwickelt. Mehr als 200 kritische Angriffsszenarien können durch die Umsetzung der Härtungsmodule leicht verhindert werden.



AWARENESS

SICHERHEITSBEWUSSTSEIN FÖRDERN

PHASE 3

95% der erfolgreichen Angriffe sind nur durch den Eingriff des Menschen möglich. Durch gezielte Workshops in Kombination mit einer langfristigen Awareness-Kampagne sensibilisieren wir die Mitarbeiter. Denn diese benötigen das entsprechende Rüstzeug, damit diese im Falle eines Social Engineering-Angriffs gewappnet sind und zu einer Art menschlichen Firewall werden.

Neben der Vorbereitung durch Gespräche mit Ihnen, setzen wir im ersten Schritt OSINT-Techniken zur Informationsgewinnung ein. Der Fokus liegt dabei auf Informationen über das Unternehmen sowie Mitarbeiter und deren Verantwortungsbereiche, um die Awareness-Kampagne besonders effektiv zu gestalten.

Leistungsübersicht:

- Awareness-Workshops
  (2 Stunden / vor Ort oder remote)
- Awareness-Kampagnen
  (4 Wochen bis 36 Monate Laufzeit)

Wir beginnen mit trivialen Szenarien und Phishing-Mails und steigern diese bei erfolgreicher Abwehr zu raffinierten Spear-Phishing Mails, welche wir in vorheriger Absprache mit Ihnen zusätzlich durch Telefonanrufe ergänzen können.

Aufgrund des steigenden Schwierigkeitsgrades und gezielten Schulungsinhalten ist das Training besonders effektiv, sodass wir die Mitarbeiter langfristig fordern und motivieren.