
TUF
CYBER
SECURITY
Cyber. Sicher. TUFO.

TUF CYBER SECURITY

Die Welt ein Stück sicherer machen

Das ist unser Credo.

0101011101101001011100100010000001100110011100100110010101110101011001010110111000100000011101010110111001110011001000000110000101110101011001100010000000110010001101001011001010010000001011010011101010111001101100001
0110110101101101011001010110111001100001011100100110001001100100101101001011101000010000100100000000010100100100101101000011100100010000001010100010100101010001100100111100100000010101000110010101100001011011010010000100001

TUFO IST SPEZIALISIERT AUF

PENETRATION TESTING

Ob Online Shop, mobile App oder Web-applikation: wir decken die Sicherheitslücken auf, damit sie nicht von Kriminellen ausgenutzt werden.

HACKER-ANGRIFF-SIMULATION

Sind Sie gewappnet gegen einen Hacker-Angriff? Ihr Unternehmen wird einem eigens von uns entwickelten Stresstest unterzogen. So finden wir Ihre offenen Flanken!

AWARENESS TRAINING

Der Faktor Mensch ist die größte Security Schwachstelle. Reduzieren Sie das Risiko, indem Sie Ihre Mitarbeiter:innen sensibilisieren. Wir schulen Ihre Belegschaft!

SECURITY BERATUNG

Sie brauchen Unterstützung im Aufbau Ihrer Cyber Security Infrastruktur? Unsere erfahrenen Expert:innen stehen gerne zur Verfügung!

PENETRATION TESTING

Unsere Penetrationtester:innen haben Erfahrung im Testen von Websiten, komplexen Web-Apps, mobilen Apps, Netzwerk-infrastruktur, WLAN Netzwerken, Client-Netzwerken und IOT- bzw. Embedded-Geräten. Bei unseren Tests betrachten wir stets das gesamte Bild der zu testenden Lösung, um sowohl Designfehler als auch technische Fehler zu finden.

1

Zielsetzung & Methodik

Zunächst eruieren wir gemeinsam das Testobjekt, den Umfang, technische Details sowie den Testmodus (Back, Grey oder White Box).

2

Penetration Testing

Wir führen den Test zum vereinbarten Termin durch. An dem Tag sollte eine beidseitige Erreich-barkeit gewährleistet sein, um Rückfragen schnell zu klären.

3

Ergebnisse & Bericht

Neben einer Präsentation der Ergebnisse erhalten Sie einen Bericht inkl. Empfehlungen wie Sie Ihre Schwachstellen beheben können.

4

Behebung der Schwachstellen

Nun sind Sie an der Reihe, die gefundenen Schwachstellen zu beheben. Auch in dieser Phase stehen wir mit unserer Expertise zur Seite, wenn gewünscht.

5

Re-Check

Sind die Schwachstellen behoben, überprüfen wir, ob die getroffenen Maß-nahmen auch wirken. Dazu gibt es abermals einen Bericht, den Sie als Nachweis nutzen können.

HACKER-ANGRIFF-SIMULATION

Eine Hacker-Angriff-Simulation, auch bekannt als Red Teaming, ist ein wahrer Stresstest für Ihre Security Infrastruktur. Dabei kommen vielfältige Mittel zum Einsatz: von Key Loggern über Angriffe auf Software, Hardware und Infrastruktur bis hin zu physischem Eindringen in Ihre Räumlichkeiten. Bei dieser Simulation ermitteln wir nicht nur, wie gut Ihre Abwehr-Maßnahmen funktionieren, sondern auch wie Sie und Ihre Belegschaft auf Vorfälle reagieren.

1

Vorbereitung & Recherche
Zunächst widmen wir 2 bis 5 Tage der Recherche Ihrer Organisation, um Angriffsmöglichkeiten zu planen.

2

Vorstellung
Wir präsentieren Ihnen 1 bis 3 Angriffs-szenarien, aus denen Sie auswählen, welche zum Einsatz kommen.

3

Durchführung der Simulation
Wir führen am vereinbarten Tag den Angriff durch und versuchen uns Zugriff auf Ihre Systeme zu verschaffen.

4

Ergebnisse & Bericht
Neben einer Präsentation der Ergebnisse erhalten Sie einen Bericht inkl. Empfehlungen wie Sie Ihre Schwachstellen beheben können.

5

Behebung der Schwachstellen
Nun sind Sie an der Reihe, Ihre Security zu optimieren. Auch in dieser Phase stehen wir mit unserer Expertise zur Seite, wenn gewünscht.

AWARENESS TRAINING

Eine gute technische Verteidigung ist nur die halbe Miete. Die meisten Unternehmen sind extrem anfällig auf Social Engineering Angriffe, weil eine konsequente Schulung der Belegschaft oft vernachlässigt wird. So landen schnell einmal Trojaner oder Ransomware im Netzwerk und legen das ganze System lahm. Das kann teuer und aufwendig werden. Dabei ließe sich das leicht verhindern, mit gut geschultem Personal!

1

Wahl der Zielgruppen

Zunächst definieren wir gemeinsam wer sensibilisiert werden soll. Das kann vom Management über das IT-Personal bis zu allen anderen Beschäftigten reichen.

2

Phishing Attacke (optional)

Die nichtsahnende Zielgruppe erhält von uns Phishing Mails. Das dient nicht nur als praktisches Beispiel, wir eruieren damit auch das Security Awareness Level dieser Gruppe.

3

Training

In Gruppen von bis zu 25 Personen erfahren Ihre Mitarbeiter:innen alles rund um einen sicheren Umgang am Arbeitsplatz. Wir bieten die Trainings in unterschiedlichen Sprachen an.

SECURITY BERATUNG

Sie brauchen Unterstützung im Aufbau Ihrer eigenen Cyber Security Infrastruktur? Gemeinsam analysieren wir den Schutzbedarf Ihres Unternehmens, gestalten ein Zielbild und helfen im Setup.

Sie haben allgemeine Fragen zum Thema Cyber Secuity? Unsere erfahrenen Expert:innen stehen gerne zur Verfügung!

Als Beratungsunternehmen unterstützen wir Sie dabei, Ihre Organisation, Geschäftsprozesse und Regelwerke in Bezug auf Informationssicherheit und Anforderungen der Compliance zu optimieren.

TUF CYBER SECURITY

DARUM TUFO!

- Professionelle White-Hat-Hacker:innen
- 15+ Jahre Cyber Security Erfahrung
- Immer am neuesten Stand der Security
- Passionierte Kämpfer:innen gegen Betrug & Schaden

TUFO GmbH

Stumpergasse 33/20
1060 Wien
www.tufo.at
office@tufo.at