TUFO

CYBER SECURITY

Cyber. Sicher. TUFO.

Unsere Angebote

PENETRATION TEST

Wo liegen die Schwachstellen in Ihrem Netzwerk, Ihrer Webanwendung oder Ihren mobilen Apps?

HACKER- ANGRIFF-SIMULATION

Ist Ihre Organisation gegen einen Hackerangriff auf allen Ebenen gewappnet?

SCHWACHSTELLEN-MANAGEMENT

Sie möchten regelmäßig über Ihre Schwachstellen informiert werden, um sie rechtzeitig zu beheben?

PHISHING-SIMULATION

Können Ihre Mitarbeiter:innen Phishing-Versuche zuverlässig identifizieren und angemessen darauf reagieren?

PHYSISCHER PENETRATION TEST

Ist es möglich, unter falschem Vorwand in Ihre physischen Geschäftsräume einzudringen?

AWARENESS TRAINING

Sind Ihre Mitarbeiter:innen ausreichend auf Cyberrisiken geschult?

PENETRATION TEST

In der heutigen digitalen Welt sind Sicherheitsbedrohungen omnipräsent und können erhebliche Schäden verursachen. Unsere Penetrationstests, durchgeführt von einem Team aus erfahrenen Ethical Hacker:innen, simulieren gezielte Angriffe auf Ihre IT-Systeme, um Schwachstellen aufzudecken und zu schließen, bevor sie von Angreifer:innen ausgenutzt werden können. Schützen Sie Ihr Unternehmen proaktiv mit unserem maßgeschneiderten Sicherheitsansatz.

1

Zielsetzung & Methodik

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

2

Penetration Testing

Wir führen den Test zum vereinbarten Termin durch. In dieser Phase muss eine beidseitige Erreichbarkeit 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 (optional)

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

TUF CYBER SECURITY

Eine Hacker-Angriff-Simulation, auch bekannt als Red Teaming, stellt einen umfassenden Stresstest für Ihre Sicherheitsinfrastruktur dar. Dabei kommen unterschiedlichste Methoden zum Einsatz – von Keyloggern über Angriffe auf Software und Hardware bis hin zum physischen Eindringen in Ihre Räumlichkeiten. Diese Simulation hilft nicht nur dabei, die Wirksamkeit Ihrer Abwehrmaßnahmen zu überprüfen, sondern auch zu beurteilen, wie gut Sie und Ihre Belegschaft auf Sicherheitsvorfälle reagieren.

1

Vorbereitung & Recherche

Zunächst widmen wir uns der Recherche Ihrer Organisation, um Angriffsmöglichkeiten zu planen.

2

Vorstellung

Wir präsentieren Ihnen 1 bis 3 Angriffsszenarien, aus denen Sie auswählen, welche zum Einsatz kommen.

3

Durchführung der Simulation

Wir führen den Angriff durch und decken alle Schwachstellen auf.

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 Ihnen mit unserer Expertise zur Seite.

SCHWACHSTELLEN-MANAGEMENT

Unsere umfassende Schwachstellen-Management-Lösung analysiert und identifiziert regelmäßig Sicherheitslücken in Ihren IT-Netzwerken. Durch frühzeitige Erkennung und systematische Behebung von Schwachstellen stärken wir die Sicherheit Ihres Unternehmens und schützen es langfristig vor potenziellen Angriffen.

1

Zielsetzung

Zunächst definieren wir, welche Systeme für den Schwachstellenscan relevant sind.

2

Identifikation von Schwachstellen

Informationen über die Systeme werden gesammelt. Potenzielle Schwach-stellen werden identifiziert.

3

Interpretation der Ergebnisse

Die Ergebnisse werden validiert. Schwachstellen werden auf ihre Relevanz für den Kunden überprüft und einer Risikoeinschätzung unterzogen.

4

Vergleich mit letzten Ergebnissen

Die Beseitigung der Schwachstellen aus früheren Scans wird validiert. Veränderungen im Netzwerk seit dem letzten Scan werden erfasst.

5

Kommunikation

Wir berichten über relevante Schwachstellen und geben Handlungsempfehlungen. Behobene Schwachstellen werden bestätigt und Abweichungen seit dem letzten Scan werden kommuniziert.

PHISHING-SIMULATION

Unsere Phishing-Simulationen testen und schulen Ihr Personal im Umgang mit realistischen Phishing-Versuchen. Indem wir das Verhalten Ihrer Mitarbeiter:innen analysieren, können wir gezielte Schulungen anbieten, die Ihre Organisation resilienter gegenüber Cyberangriffen machen. Minimieren Sie das Risiko und stärken Sie Ihre erste Verteidigungslinie.

1

Wahl der E-Mail-Adressen

Zunächst definieren wir, welche E-Mail-Adressen wir testen möchten.

2

Recherche und Planung

Wir sammeln Informationen über Ihr Unternehmen und planen mehrere Angriffsszenarien.

3

Domain Squatting & Setup

Wir erwerben eine Domain, die Ihrer Domain ähnlich ist und setzen unsere Infrastruktur auf.

4

Simulation & Angriff

Über mehrere Wochen senden wir realistische Phishing-E-Mails an Ihre Mitarbeiter:innen und beobachten die Reaktionen.

5

Ergebnisse & Bericht

Neben einer Präsentation der Ergebnisse erhalten Sie einen Bericht inklusive Empfehlungen.

PHYSISCHER PENETRATION TEST

Physische Sicherheitsrisiken sind genauso bedrohlich wie digitale. Unsere physischen Penetrationstests evaluieren, wie gut Ihre Mitarbeiter:innen auf unbefugte Zugriffsversuche reagieren. Durch das Simulieren realistischer Szenarien stärken wir die Fähigkeit Ihres Teams, solche Bedrohungen zu erkennen und adäquat zu handeln.

1

Wahl der Standorte

Wir definieren, welche Standorte wir überprüfen und welche Techniken wir einsetzen dürfen.

2

Recherche und Planung

Wir sammeln Informationen über Ihr Unternehmen und planen den Angriff.

3

Physischer Einbruch

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

4

Bericht & Maßnahmenkatalog

Sie erhalten einen Bericht mit einer genauen Beschreibung des Angriffs, einschließlich der Dialoge mit den Mitarbeiter:innen, sowie Empfehlungen, wie Sie Ihre Schwachstellen beheben können.

5

Präsentation

Wir präsentieren die Ergebnisse und besprechen mit Ihnen die Optionen, um Ihre Sicherheit zu erhöhen.

AWARENESS TRAINING

Angesichts zunehmend raffinierter und häufiger werdender Cyberangriffe ist ein tiefes Verständnis für Cybersicherheit unerlässlich. Unser Awareness Training klärt Ihr Team über aktuelle Sicherheitsrisiken auf und vermittelt die notwendigen Fähigkeiten, um Bedrohungen proaktiv zu erkennen und zu bekämpfen. Stärken Sie Ihre Verteidigung durch fundiertes Wissen und praktische Übungen.

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 lernen Ihre Mitarbeiter:innen alles Notwendige, um Ihre Daten und Ihr Unternehmen zu schützen.

SECURITY BERATUNG

Sie brauchen Unterstützung im Aufbau Ihrer eigenen Cyber Security Infrastruktur? Gemeinsam analysieren wir den Schutzbedarf Ihres Unternehmens, definieren ein Ziel und helfen Ihnen in der Umsetzung.

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

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

Unsere Zertifizierungen

Außerdem sind wir auch bekannt aus "Fahndung Österreich" - ServusTV

Unsere Dienstleistungen werden über firmeneigene Infrastruktur in Österreich erbracht, was die Sicherheit und Vertraulichkeit Ihrer Daten gewährleistet - ohne Weitergabe an Dritte oder Cloud-Dienstleister.

TUFO GmbH

Neubaugasse 28/1/1a
1070 Wien
www.tufo.at
office@tufo.at

Kontakt:

Onur Tuncel
Geschäftsführer
onur.tuncel@tufo.at
+43 676 900 68 97