secion
it network security

AWARENESS-TRAINING BRONZE

SECION AWARENESS-TRAINING - BRONZE

Vermittlung von umfassendem Basiswissen im Bereich Security Awareness. Mit unseren IT-Sicherheitsexperten lernen die Teilnehmer Werkzeuge und subtile Methoden von Angreifern kennen und wissen dadurch im Ernstfall eines Cyber-angriffes angemessen zu reagieren.

Zielgruppe: Mitarbeiter aller Abteilungen mit PC-Arbeitsplatz, Mail-Account und Internetzugriff

Max. Teilnehmeranzahl: 30

Schulungsdauer: 120 Minuten

Schulungspreis: 720,- Euro (inkl. An- und Abfahrt innerhalb Hamburgs). Der Preis versteht sich inklusive Schulungsunterlagen sowie Teilnahmebestätigun-gen.

Das Bronze-Training beinhaltet eine zweistündige Schulung, in der folgende Inhalte vermittelt werden:

Grundlagen der Informationsgewinnung

Welche Tools nutzen Angreifer, um an Informationen über Ihre Mitarbeiter und Ihr Unternehmen zu gelangen? Was verraten Metadaten über Ihr Unternehmen und wie machen Angreifer sich diese zunutze?

Kurzagenda:

- Vorstellung von Methoden zur Webseiten-Informationsgewinnung
- Welche Tools machen sich Angreifer außerdem zur Gewinnung von vertraulichen Informationen zunutze?
- Wie kann ich mein Unternehmen dagegen absichern?

Dauer: 15 Min

Social-Engineering

Tauchen Sie mit unseren secion Experten in die Vorbereitungen eines Social Engineering Angriffes ein! Wir zeigen Ihnen, welche Vorgehensweisen Angreifer nutzen, um an vertrauliche Informationen Ihres Unternehmens zu gelangen.

Kurzagenda:

- Wie geht ein Angreifer vor, um einen Social Engineering Angriff vorzubereiten?
- Welche Methoden und Tools macht er sich hierbei zunutze?
- Wie schafft es der Angreifer, mit diesen Informationen bestehende Social Engineering Sicherheitslücken auszunutzen?

Dauer: 15 Min

Phishing

Lernen Sie eine der noch immer erfolgreichsten Angriffsmethoden kennen, um das Vorgehen, Ziele und Erfolge von Angreifern zu verstehen.

Kurzagenda:

- Begriffsdefinition: Wodurch zeichnet sich ein erfolgreicher Phishing-Angriff aus?
- Unsere IT-Sicherheitsexperten berichten über Beispiele aus der Praxis
- Wie können Sie sich und Ihr Unternehmen vor Phishing-Angriffen schützen?

Dauer: 15 Min

Sicheres E-Mailing

Durch dieses Modul wird das Sicherheitsbewusstsein Ihrer Mitarbeiter im täglichen Umgang mit E-Mails geschärft: Welches sind die gängigsten Angriffsvarianten, die per E-Mail durchgeführt werden?

Kurzagenda:

- Wie prüfen Sie eine E-Mail auf ihre IT-Sicherheit?
- Unsere IT-Sicherheitsexperten berichten über Angriffsbeispiele per E-Mail aus der Praxis
- Wie schützen Sie sich und Ihr Unternehmen vor solchen Angriffen?

Dauer: 15 Min

Adware

Unsere IT-Sicherheitsexperten geben einen Einblick in die unterschätzte und doch weit verbreitete Angriffsmethode durch Platzierung von Adware.

Kurzagenda:

- Was ist Adware und wie machen sich Hacker diese für die Durchführung eines Angriffs zunutze?
- Unsere IT-Sicherheitsexperten berichten über Angriffsbeispiele durch Adware aus der Praxis
- Wie schützen Sie sich und Ihr Unternehmen vor Angriffen durch Adware?

Dauer: 15 Min

Sicherer Umgang mit Daten und Kommunikation

Der Austausch von sensiblen Daten über das Internet nimmt immer mehr zu. Unsere Experten zeigen Ihnen auf, welche Sicherheitsaspekte Sie beachten müssen, um sich im Datenraum gefahrenlos bewegen zu können.

Kurzagenda:

- Wie werden Daten transportiert? Welche Konsequenzen ergeben sich hieraus für den sicheren Umgang mit Daten?
- Wie erkennen Sie eine gute Datenverschlüsselung?

Dauer: 10 Min

Passwortsicherheit

Jedes Unternehmen hat sie – keiner mag sie...! Unsere IT-Sicherheitsexperten zeigen Ihnen, warum das sichere Generieren von Passwörtern so wichtig ist.

Kurzagenda:

- Wie sollte man mit Passwörtern in Unternehmen umgehen?
- Beispiele aus der Praxis: Warum ist das Passwort 12345678 nicht empfehlenswert?

Dauer: 15 Min

Sicherer Umgang mit Smartphones

Welche Funktionen Ihres Smartphones werden im Alltag genutzt und sind in der Lage, Ihr Verhalten im Tagesablauf auszuspionieren?

Kurzagenda:

- Welche Gefahren lauern im täglichen Gebrauch mit Ihrem Smartphone?
- Wie stellen Sie Ihr Smartphone sicher ein?
- Wie beziehen Sie sichere Software für Ihr Smartphone?

Dauer: 10 Min

Sicherer Umgang mit WLAN

Unsere Experten zeigen Ihnen, welche Gefahren von öffentlichen WLAN Netzwerken ausgehen.

Kurzagenda:

- Was müssen Sie bei einem öffentlichen WLAN Netzwerk beachten?
- Welche Verschlüsselungsverfahren sollten Sie bei der Nutzung von WLAN in Ihrem Unternehmen nutzen?
- Wie erkennen Sie eine sichere WLAN Verschlüsselung?

Dauer: 10 Min

Wünschen Sie eine Abschlussprüfung Ihrer Mitarbeiter? In dieser Online-Prüfung wird das in der Awareness-Schulung vermittelte Wissen online getestet und bei erfolgreicher Teilnahme mit einem Zertifikat bestätigt.

Kosten pro Mitarbeiter-Prüfung: 15,- Euro

Unsere Awareness-Trainingsmodule im Überblick

Module	Gold-Training	Silber-Training	Bronze-Training	Individual-Training
Basis-Module				Individuelle Zusammenstellung der Basis-Module
Grundlagen der Informationsgewinnung	✔	✔	✔	
Social Engineering	✔	✔	✔	
Phishing	✔	✔	✔	
Sicheres E-Mailing	✔	✔	✔	
Adware	✔	✔	✔	
Sicherer Umgang mit Daten / Kommunikation	✔	✔	✔	
Passwortsicherheit	✔	✔	✔	
Sicherer Umgang mit Smartphones	✔	✔	✔	
Sicherer Umgang mit WLAN	✔	✔	✔	
Advanced-Module				Individuelle Zusammenstellung der Advanced-Module
Angriffe als Dienstleistung	✔	✔		
Phishing / Live Hacking	✔	✔		
Browser Sicherheit / Live Hacking	✔	✔		
Passwortsicherheit / Live Hacking	✔	✔		
WLAN / Live Hacking	✔	✔		
Überprüfungsszenario: Zeitlich versetzter Phishing Angriff auf die Teilnehmer	✔			
Ergänzend für alle Trainings-Optionen buchbar: Abschlussprüfung der Teilnehmer	optional	optional	optional	optional

Wir beraten Sie gerne zur unserem secion Awareness Training!
Sie erreichen uns unter 040-38 90 71-0, per E-Mail an info@secion.de
oder über unser Kontaktformular auf www.secion.de/kontakt.html

secion
it network security

Verantwortlich für den Inhalt:
secion GmbH
Paul-Dessau-Straße 8
22761 Hamburg

Telefon: 040 / 38 90 71 - 0
Fax: 040 / 38 90 71 - 299
E-Mail: info@secion.de
Internet: www.secion.de