secion
it network security

TRAININGSZENTRUM CYBERABWEHR II

Agenda

10:00 – 12:30 Uhr

Verstehen Sie Strategien, Techniken und Tools von Angreifern

In dieser Workshop-Einheit ergründen Sie mit uns die Welt der Cyberkriminellen und lernen deren ausgefeilten Strategien näher kennen: Wie gehen Hacker methodisch vor und welcher technischen Tools bedienen sie sich dabei? Welche subtilen Methoden wählen sie, um an sensible Informationen für einen Angriff zu gelangen und diesen durchzuführen? Welche (auch menschlichen) Schwachstellen und Einfallstore nutzen sie aus?

Und - wie können Sie sich und Ihr Unternehmen davor wappnen?

Wir demonstrieren es Ihnen anhand folgender Angriffsmethoden in anschaulicher Theorie und Praxis:

Knacken von Passwörtern

Hacker bedienen sich verschiedenster Methoden, um Passwörter herauszufinden und Accounts zu knacken. Das Generieren von Passwörtern und deren sichere Verwahrung wird eine zunehmende Herausforderung für Unternehmen. Im Rahmen einer Live Hacking Demonstration zeigen unsere IT-Sicherheitsexperten Ihnen, wie schnell man unsichere Passwörter errechnen kann und darüber an administrative Rechte gelangt:

- Was müssen Sie bei der Gestaltung Ihrer Passwörter beachten, damit diese sicher sind?
- Wie gelangt man durch den Einsatz eines Keyloggers an Informationen?
- Sind Passwort-Richtlinien für Ihr Unternehmen unverzichtbar?

Angriffe durch Ransomware

Aktuelle Studien belegen, dass 43 Prozent erfolgreicher Ransomware-Angriffe über Phishing und Social Engineering erfolgen, unsichere oder manipulierte Webseiten machen 30 Prozent aus.* Wie viel wären Sie bereit zu zahlen, um den Verlust Ihrer sensiblen Unternehmensdaten zu verhindern?

Unsere IT-Security Consultants zeigen Ihnen aktuelle Beispiele aus der Praxis und erörtern mit Ihnen die dort eingesetzten Angriffsmethoden und Lösegeldforderungen.

- Nach dieser Workshop-Einheit wissen Sie, wie aktuelle Ransomware-Angriffe getarnt werden
- Wie gelangen die Erpresser an das geforderte Lösegeld?
- Wie gelingt es Ihnen, einen Ransomware-Angriff abzuwehren? Worauf kommt es bei der Sensibilisierung Ihrer Mitarbeiter an?

* SearchSecurity.de, Ransomware-Angriffe: Die Kosten für Unternehmen

Phishing Attacken

Lernen Sie mit uns eine der noch immer erfolgreichsten Angriffsmethoden kennen, um das Vorgehen, die Ziele und Erfolge von Angreifern zu verstehen. Unsere IT-Sicherheitsexperten berichten dazu über Beispiele aus der Praxis und zeigen Ihnen anhand eines Live Hacking Szenarios wie einfach es ist, Ihre Webseite für einen Phishing-Angriff zu missbrauchen:

- Wie funktioniert das Klonen einer Webseite Ihres Unternehmens?
- Vorbereitung einer fingierten E-Mail zur erfolgreichen Durchführung eines Phishing-Angriffs
- Welche Schritte sind nach einem erfolgreichen Phishing-Angriff sofort einzuleiten, um die Schäden für Ihr Unternehmen so gering wie möglich zu halten?

Ausflug ins Dark Net / Angriffe als Dienstleistung

Wir geben Ihnen einen Einblick in verschlüsselte Netzwerke. Lernen Sie mit unseren IT-Sicherheitsexperten einige der aktuellen Dienstleistungen aus dem Darknet kennen. Nach dem gemeinsamen Ausflug in das Dark Net wissen Sie folgende Fragen zu beantworten:

- Was ist das Clearnet und was sind Hidden-Services?
- Welche Bedrohungen gehen von solchen Dienstleistungen aus und was kosten diese?

- Wieviel kosten gekaperte Accounts und wie werden diese gehandelt?

12:30 – 13:30 Uhr Mittagspause

13:30 – 16:30 Uhr

Trainieren Sie für den Ernstfall und managen Sie einen Ransomware-Angriff – live!

Unsere IT-Security Consultants werden zu Angreifern! Testen Sie Effizienz und Wirksamkeit Ihres Verhaltens bei einem tatsächlich stattfindenden Ransomware-Angriff:

1. Sie besetzen mit den übrigen Teilnehmern zentrale Unternehmenspositionen, die häufiges Ziel von Cyberangriffen sind (z.B. Geschäftsführung, Leitung Human Ressources, Finanzen, IT, Office Management).
2. Sie werden Zeuge eines mehrstufigen Ransomware-Angriffs auf ein Unternehmen und erleben live, wie subtil sich Ransomware verbreitet und sich den Weg zum Ziel bahnt.
3. Sie managen die Krise in der Ihnen zugewiesenen Rolle: Wann sind Sie in der Lage, die Malware zu stoppen?
   - Sie erfassen und analysieren die vorgefundene Angriffssituation
   - Sie definieren organisatorische Maßnahmen und Prozesse, die umgehend eingeleitet werden müssen: Wer ist sofort zu informieren? Welche Zuständigkeiten innerhalb des Teams sind festzulegen? Welche Analysewerkzeuge sollten Sie sich zunutze machen?
   - Sie entwickeln reaktive Maßnahmen: Wie schließen Sie mit Ihren vorhandenen Systemen und Bordmitteln gefundene Sicherheitslücken?
   - Bewerten Sie die Wirksamkeit Ihrer Maßnahmen: Diskussion der gefundenen Ansätze mit Experten und Teilnehmern. Wie sieht die best practice aus? Gibt es wirksame technische Tools, die unsere IT-Sicherheitsexperten für eine Angriffsabwehr empfehlen?

16:30 – 17:00 Uhr

Resümee der Angriffssimulation und Übertragung auf mögliche zukünftige Cyber-Attacken: Was können Sie aus dem simulierten Ransomware-Angriff für die Verteidigung Ihres Unternehmens lernen?

Referenten

Patrick Jung, Leiter Professional Services, secion GmbH
Tim Heinsohn, Leiter Vertrieb, secion GmbH

**Die Kosten pro Roadshow-Teilnahme betragen 499,- Euro (zzgl. USt.).
Für Mitglieder der Allianz für Cyber-Sicherheit wird die Veranstaltung zu einer Aufwandspauschale von 100,- Euro angeboten.**

Reisekosten und Kosten für zusätzlichen Verpflegungsaufwand außerhalb der Veranstaltung sind durch die Teilnehmer selbst zu tragen.

Es stehen pro Veranstaltungsort 16 Plätze zur Verfügung, die durch den Veranstalter im Losverfahren vergeben werden. 6 Plätze sind für Mitglieder der Allianz für Cybersicherheit reserviert.

Teilnahmebedingungen:

1. In der Workshop-Gebühr sind die Teilnahme, die Verpflegung und die Seminarunterlagen enthalten. Anreise, Parken und ggf. Übernachtung sind nicht im Preis inbegriffen.

2. Die Anmeldung ist verbindlich und kostenpflichtig. Die Rechnung über die Veranstaltungsgebühr geht dem Teilnehmer vor Durchführung des Workshops zu. Zahlungsziel ist sofort und ohne jeglichen Abzug. Die Workshop-Teilnahme ist nur bei voll entrichteter Teilnahmegebühr möglich.

3. Sollte die Teilnahme an der Veranstaltung nicht möglich sein, ist eine formlose, schriftliche Absage möglich. Erfolgt die Absage bis 3 Wochen vor Veranstaltungstermin, ist diese kostenfrei. Bei Absagen bis 2 Wochen vor Veranstaltungstermin werden 30% der Teilnahmegebühr fällig, erfolgt die Absage erst 5 Tage oder kürzer vor dem Veranstaltungstag, wird die Teilnahmegebühr zu 100% fällig. Ein Ersatzteilnehmer mit vergleichbaren Vorkenntnissen kann jedoch gestellt werden.

Wir beraten Sie gerne zur unserem secion Trainingszentrum Cyberabwehr II! 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