SC190 Information Security Incident Management

Kurzbeschreibung:

Die meisten Vorfälle beginnen ganz harmlos. Ein User eröffnet ein Ticket, der Helpdesk widmet sich nach einer Weile dem Problem. Dann wird der Techniker nervös, er informiert seinen Chef und der wird auch nervös.

Ist es ein Angriff oder ein Fehler – welche Auswirkungen und Schäden sind zu erwarten und welche Maßnahmen sind jetzt einzuleiten? Dies und mehr lernen Sie in diesem Workshop, der in 4 Bereiche aufgeteilt ist:

- Erkennung von Vorfällen und allgemeine Grundsätze der Störungs- bzw. Vorfallsannahme
- Aufspüren von Angriffen im Netzwerk
- Vorfälle mit Clients und Servern
- Sie sind Teil eines Workshops, in dem Sie das Gelernte festigen und trainieren

Die überwiegende Zahl der Inzidenz, welche beim IT-Support entgegengenommen werden, sind Folge von Bedienungsfehlern oder haben technische Ursachen. Im Tagesgeschäft haben sich die Techniker daran gewöhnt eine Warteschlange, ähnlich dem Wartezimmer eines Arztes abzuarbeiten. Dabei ist der IT-Support meist auch die Notaufnahme. Also wie erkennt man die dringenden Fälle? Wie ist jetzt zu reagieren?

Zielgruppe:

Verantwortliche für Informationssicherheit, aber auch von IT-Operations, sowie Incident Manager und Prozessverantwortliche.

Voraussetzungen:

Grundkenntnisse der Informationssicherheit, Kenntnisse des Tagesgeschäfts von IT-Operations. Es erfolgt keine formelle Prüfung der Zugangsvoraussetzungen.

Sonstiges:

Dauer: 2 Tage

Preis: 1400 Euro plus Mwst.

Ziele:

Nach Abschluss des Workshops sind Sie in der Lage, Sicherheitsvorfälle bzw. Störungen zu erkennen und geeignete Maßnahmen einzuleiten, um den Betrieb schnellstmöglich wiederherzustellen. Sie erhalten ein vertieftes Verständnis und lernen vor allem die Umsetzung und den Betrieb eines Information Security Incident Management Prozesses, um die erlernten und erarbeiteten Themen im Unternehmen anwenden können.

Nach dem Kurs können Sie vom Meldeprozess, über die Isolation und Identifizierung bis hin zur Bereinigung und Dokumentation einen wehrhaften und effizienten Prozess zur Vorfallbewältigung abbilden.

Inhalte/Agenda:

- ♦ **Modul 1:**
  - ♦ ◊ Darstellung eines mehrstufigen Angriffes auf einen Informationsverbund
    ◊ Gegenseitiges Wirken von Angriff und Abwehr
    ◊ Bedeutung der Timeline für die schnelle Erkennung eines Vorfalls
    ◊ Grundsätze und Richtlinien des IR-Managements
    ◊ Aufbau einer zuverlässigen Meldekette und First Response

  ♦ **Modul 2:**
  - ♦ ◊ Livedemo von Angriffen auf Windows- und Linux-Maschinen
    ◊ Triageprozess durch IT-Ops und nachgelagertes SOC und CSIRT
    ◊ Sec-Ops-Forensik 1: Spurensuche in Windows-Maschinen
    ◊ Sec-Ops-Forensik 2: Spurensuche in Linux-Maschinen
    ◊ Sec-Ops-Forensik 3: Spurensuche in OT
    ◊ Remediation von infizierten Systemen

  ♦ **Modul 3:**
  - ♦ ◊ Angriffe auf das Netzwerk von außen und innen
    ◊ Die Bedeutung von Delivery- und Comand&Control-Servern
    ◊ Sec-Ops-Forensik 4: Spurensuche in verteilten LDAP und AD-Diensten
    ◊ Sec-Ops-Forensik 5: Spurensuche in Netzwerken und Firewalls
    ◊ Sec-Ops-Forensik 3: Aufspüren von ICMP/DNS-Tunneln und Backdoors
    ◊ Best Practices und Validierung von Angriffsquellen

  ♦ **Modul 4:**
  - ♦ ◊ Individueller DeepDive von Themen der Module 1-3
    ◊ Praxisübung: Behandlung von Sicherheitsvorfällen
    ◊ Erfahrungsaustausch

  ♦ Bei Inhouse-Schulungen/Geschlossenen Kursen, die online stattfindet, gehen wir gern auf Ihre individuellen Terminwünsche ein. So können wir den Kurs anstatt an zwei Tagen mit jeweils 8 Stunden auch an 4 Tagen mit jeweils 4 Stunden durchführen.
  Sprechen Sie uns an!

  ♦