consectra GmbH
Im Unteren Angel 13, 77652 Offenburg
+49.781.9400894, www.consectra.de

consectra
mIT-Sicherheit ein guter Partner

LIVE-HACKING SZENARIENÜBERSICHT

Inhaltlicher Aufbau einer Live-Hacking Veranstaltung zur Steigerung der Awareness im Bereich der Informationssicherheit

Die Live-Hacking Veranstaltung

Ein Live-Hacking veranschaulicht Anwendern die Gefahren beim Umgang mit modernen Informationstechnik, wie kaum eine andere Maßnahme. Um den Wirkungsgrad möglichst effizient zu gestalten, möchten wir auf einige relevante Faktoren hinweisen.

- Weniger ist mehr
  Es lassen sich eine Menge Szenarien in einer Veranstaltung unterbringen. Die Aufnahmefähigkeit der Teilnehmer ist jedoch begrenzt. Bei Überschreitung dieser Grenze nimmt die Effektivität in den jeweiligen Einzelthemen ab.
- Zielgruppenorientierung
  Gerade bei Anwendern ist es wichtig, dass ihnen nach einem Szenario eine Möglichkeit dargelegt wird, sich vor einem entsprechenden Angriff zu schützen. Gibt es in der Umgebung des Anwenders keinen für ihn nutzbaren Sicherheitsmechanismus, sollte das entsprechende Szenario nicht gewählt werden. Ansonsten könnte eine Ohnmacht entstehen, die dem Veranstaltungsziel kontraproduktiv entgegensteht.
- Kombinierbarkeit der Szenarien
  Manche Szenarien bauen aufeinander auf und sind somit nicht beliebig kombinierbar.
- Veranstaltungsdauer
  Bis zu zwei Stunden kann eine Veranstaltung ohne Pause dauern. Darüber hinaus müssen Pausen eingeplant werden. Je nach Teilnehmerzahl muss die Toilettenkapazität berücksichtigt werden.
- Individualisierung
  Die Szenarien lassen sich an Ihre Gegebenheiten anpassen. So werden die Aspekte transportiert, die Ihnen wichtig sind. Hierzu gehört z. B. das Verständnis für technische Restriktionen oder organisatorische Vorgaben, aber auch die Stärkung der Eigenverantwortung.
- Keine Begrenzung der Teilnehmerzahl
  Die Anzahl der Teilnehmer wird ausschließlich durch Ihre räumlichen Kapazitäten beschränkt.
- Weitergabe der Szenarienbeschreibung an die Teilnehmer
  Bitte geben Sie weder die Beschreibung noch die genauen Namen der Szenarien an die Teilnehmer weiter. Dies würde an einigen Stellen die Pointe vorwegnehmen und den Entertainment Faktor schmälern.

Unsere Berater erfragen in einem Vorgespräch die relevanten Punkte und erstellen für Sie ein Konzept zur Maximierung des Erfolgs Ihrer Live-Hacking Veranstaltung.

Übersicht über die Szenarien

Phishing - …und das alles kostenlos!

Nur noch kurz die Mails checken.
Über eine E-Mail wird Schadcode auf dem Rechner eines Anwenders platziert. Auf den ersten Blick sieht die E-Mail sehr gut aus. Worauf sollte beim Öffnen von E-Mails geachtet werden?

Der Trojaner - Ich sehe was, was Du nicht siehst.

Ein Anwender hat sich ein Trojanisches Pferd eingefangen. Welche Möglichkeiten hat der Angreifer? Wie hätte das verhindert werden können?

Drive-By-Download - Auf solchen Seiten bin ich nicht unterwegs! Oder doch?

Kann ich mich beim Surfen im Internet mit Schadecode infizieren? Gerade durch die Möglichkeit infizierte Bilder als Werbung auf Webseiten zu schalten, lassen sich scheinbar seriöse Seiten als Träger von Schadecode nutzen.

Update – Ein lästiges Übel. Muss das denn sein?

Der Rechner eines Anwenders wird infiziert, ohne dass dieser aktiv geworden ist. Rein durch das Fehlen eines Sicherheitsupdates kann der Bildschirminhalt abfotografiert oder gar die Kamera übernommen werden.

Pharming - Den Datenpiraten hilflos ausgeliefert?

Ein Rechner war infiziert, der Virus wurde jedoch entfernt. Trotzdem wird ein Anwender auf eine Website geleitet, welche mit der Originalseite nahezu identisch ist. Von wo aus dürfen sensible Seiten aufgerufen werden? Wie kann ich mich schützen?

PDF- und Word-Dokumente - Metadaten und andere versteckte Infos

Das Pentagon veröffentlichte auf Druck der Medien Geheimdokumente des Irak-Krieges. Große Passagen waren geschwärzt. Stellen wir doch mal schnell die interessanten Informationen wieder her. Was versenden Sie so alles mit Ihren Dokumenten?

Digitalkamera - Die macht doch nur Bilder…

USB-Sticks können gefährlich sein. Aber eine Digitalkamera? Über eine präparierte Kamera werden die eigenen Dateien kopiert und Dateien hinterlassen, die man ungern auf dem eigenen Rechner findet.

Die Maus erwacht zum Leben - Kleine Nager sammeln Daten.

Da arbeitet man über diverse Szenarien hinweg mit einer Maus und auf ein Signal hin wird diese plötzlich aktiv. Sie durchsucht alle Laufwerke (lokal und auch im Netzwerk) nach Dateien bestimmte Formate, um diese in einer Dropzone abzulegen. Wie es für Mäuse typisch ist, wühlt auch im Papierkorb.

Die Kochrezept-Datenbank – Wie schmeckt Ihnen unser Passwortklau?

Leckere Rezepte herunterladen. Nur mal schnell kostenlos mit E-Mailadresse und Passwort registrieren. Hier gehen wir der Fragen nach ob unterschiedliche Kennwörter (gerade dienstlich und privat) wirklich wichtig sind.

BruteForce-Attacken - Mein Passwort errätst Du nie?

Das Publikum gibt ein vierstelliges Passwort, bestehend aus Zahlen und Buchstaben vor. Dieses wird mit einem Netbook innerhalb von Sekunden geknackt.

QR-Code - Einfach scannen und los geht's…

QR-Codes findet man immer häufiger und sie bieten zum Teil einen interessanten Mehrwert. Doch gefälschte QR-Codes leiten schnell auf fragwürdige Ziele. Wie kann man Fälschungen einfach erkennen?

Smartphone Apps - Schadsoftware selbst installiert.

Schnell noch eine App auf dem Smartphone installiert und schon liegt das gesamte Adressbuch mit allen gespeicherten Daten beim Angreifer. Wir stellen einfache Prüfungen zur Identifikation gefährlicher Apps vor. Keine 100prozentige Sicherheit, aber einfach und effizient.

Smartphone-Trojaner - Beim Meeting live dabei.

Während jemand aus dem Publikum ein Handy inspiziert und beliebig bedient, wird dieses von einem Angreifer angerufen. Der Angreifer hat sein Handy an einen Lautsprecher angeschlossen und fragt: „Erkennt man auf dem Telefon etwas ungewöhnliches, z. B. einen eingehenden Anruf?“ Die Antwort: „Nein, ich erkenne nichts ungewöhnliches.“, ist für alle über den Lautsprecher zu hören. Darüber hinaus lassen sich laufende Gespräche mithören, Nachrichten lesen und sogar Sitzungen gezielt aufnehmen, auch wenn das Gerät im Raum keinen Empfang hat.

GPS-Ortung - Ich weiß wo du bist!

Über ein infiziertes Smartphone werden komplexe Bewegungsprofile erstellt und komfortabel über eine Landkarte im Internet dargestellt.

Social Engineering - Ich bin Dein Freund!

Ein britischer Anti-Terror-Chef wird mit geheimen Unterlagen im Arm fotografiert. Ein Gefangener entlässt sich per E-Mail aus dem Gefängnis. Eine (nicht reale) hübsche junge Dame erhält Geheiminformationen hochrangiger Militärs. Einer der ehemals meistgesuchtesten Personen weltweit war ein Hacker, der sich die Informationen für seine Angriffe per Social Engineering besorgte.
Doch wie funktioniert sowas? Und wie unterstützen Soziale Netzwerke hierbei?

Bluetooth – Ein blauer Zahn ist nicht immer ein gutes Zeichen.

Eine Chips Dose und Zubehör unter 5 Euro reichen für eine Richtfunkantenne aus, die eine Kommunikationsverbindung über einen Kilometer hinweg ermöglicht. So kann so manches Bluetooth Headset zur Wanze werden. Ein Scan des Raumes listet Handys, welche aktuell über Bluetooth eine aktive Kommunikationsverbindung forcieren.

NFC - Ein Smartphone macht sich selbständig.

Near Field Communication. Neue Smartphones bringen diese Technik mit, die es uns ermöglichen soll mit dem Smartphone im Supermarkt zu bezahlen. Doch mit der richtigen (oder falschen) Konfiguration lässt sich noch viel mehr automatisieren, z. B. der Download von Schadsoftware.

Öffentliches WLAN - Einfach, schnell und informativ.

Ein WLAN Access Point spielt den erreichbaren Smartphones und Notebooks vor, er sei ein vertrauter Access Point. Läuft die Kommunikation erstmal über diesen Access Point, lässt sich die Kommunikation mitlesen und manipulieren. Wie viele Geräte im Raum würden sich übernehmen lassen?
Bevor die Geräte der Teilnehmer tatsächlich übernommen werden wird gestoppt. Wir wollen ja sensibilisieren, nicht aktiv kompromittieren.

SQL-Injection - Tabellen finden und bearbeiten.

So manches Suchfeld auf der Website lässt nicht nur im gewünschten Datenbestand suchen. Über die richtigen Abfragen lassen sich schnell mal neue Produkte kreieren, Preise im Online-Shop ändern oder einen administrativen Benutzer anlegen, um den eigentlichen Administrator bei seiner Arbeit zu „unterstützen“.

Cross-Site-Scripting - Lassen Sie Angreifer entscheiden, welche Angebote auf Ihrer Website eingestellt werden.

So manches Kommentarfeld bietet einem Angreifer die Möglichkeit eigenen Inhalt in die Seite zu implementieren. So entscheiden andere, was auf der eigenen Website erscheint.

Man in the Middle - Lauschen, spionieren, manipulieren

Durch die Umleitung der Kommunikation über eigene Geräte kann nicht nur die Kommunikation mitgelesen werden. Auch die Manipulation ist möglich und das sogar bei verschlüsselten Verbindungen. Kann ich mich auf die angezeigten Daten verlassen?