CONSULECTRA-Live-Hacking-Konzept – Sensibilisierung durch Begeisterung.

Ein Live Hacking ist eine kurzweilige und informative Möglichkeit, um das Bewusstsein für das Thema Informationssicherheit zu steigern. Dazu kann das Live-Hacking in verschiedenste Veranstaltungsformate eingebunden werden. Neben internen Veranstaltungen und Schulungen zur Informationssicherheit sind Live-Hacking-Events auch eine interessante Bereicherung für Events und Kundenveranstaltungen.

Das CONSULECTRA-Live-Hacking-Konzept ist modular aufgebaut, sodass wir Ihnen eine Vortragsdauer von 15 bis 90 Minuten anbieten können. Dabei passen wir die Inhalte und die Komplexität der Szenarien entsprechend der Zielgruppe Ihrer Veranstaltung an. Unsere Referenten sind erfahrene Berater, die u. a. über Zertifizierungen als Certified Ethical Hacker (L|PT) verfügen und ihr Know-how regelmäßig in Sicherheitsanalysen und Penetrationstests anwenden.

Mit diesem Format unterstützen wir mit vielen Beispielen aus der Praxis für eine kurzweilige, aber erkenntnisreiche Sensibilisierung für das Themenfeld IT-Security in der Versorgungs- und Energiewirtschaft, insbesondere in der Netzführung, und geben Ihnen Hinweise für eventuell bestehende Sicherheitslücken in Ihrer Systemumgebung. Die dargestellten Angriffe werden dabei leicht verständlich präsentiert und bleiben bei Ihren Teilnehmern sicher lange im Gedächtnis. Getreu unserem Motto: Sensibilisierung durch Begeisterung!

Gerne stehen unsere Referenten nach dem Live Hacking für Fragen und individuelle Diskussionen zur Verfügung.

Wir bieten Ihnen verschiedene Szenarien an, aus denen Sie auswählen können. Oder Sie haben branchen- oder firmenspezifische Anforderungen, dann können wir Ihnen dies auch spezialisiert entwickeln und bereitstellen.

Hier ein Beispiel aus unserem Repertoire Computer und Internet:

Datendiebstahl in Web-Anwendungen.

In diesem Szenario wird ein Portal zur Arbeitserfassung vorgestellt, in dem Mitarbeiter eines Unternehmens ihre wöchentlichen Anwesenheitszeiten über einen Webbrowser erfassen können. Die Web-Anwendung enthält dabei einige der häufig anzutreffenden Schwachstellen, mit denen persönliche Daten anderer Mitarbeiter eingesehen und schließlich sogar das eine Gehalt – und das des Chefs – manipuliert werden können. Als Werkzeuge kommen dabei nur ein Webbrowser und eine Suchmaschine zum Einsatz.

Dauer: ca. 15 Minuten
Komplexität: gering
Vorkenntnisse: keine

Weitere Live-Hacks.

- Datendiebstahl in Web-Anwendungen
- Passwort-Diebstahl mittels XSS
- Keylogger und Co.
- Suchmaschinen-Hacking
- drahtlose Netzwerke (WLAN)
- WLAN-Schlüssel und Wörterbücher – WPA2 knacken
- Smartphones
- Smartphone-Trojaner
- spezielle Angriffe (z. B. SCADA-Systeme, Internet of Things (IoT))

Penetrationstesting durch CONSULECTRA.

Eine der effektivsten Möglichkeiten für Unternehmen, sicherheitsrelevante Schwachstellen zu identifizieren, bevor sie zu einem Sicherheitsvorfall führen, ist die Durchführung eines Penetrationstests, der einen Angriff auf die IT-Landschaft des Unternehmens simuliert. Die dadurch identifizierten Schwachstellen können rechtzeitig mit geeigneten Gegenmaßnahmen behoben werden, sodass ein tatsächlicher Angreifer diese nicht mehr ausnutzen und dem Unternehmen so schaden kann.

Die erfahrenen und zertifizierten Experten der CONSULECTRA verwenden Methoden und Werkzeuge, die auch von Angreifern verwendet werden, um in ausgewählte Bereiche der IT-Infrastruktur des Auftraggebers einzudringen. Der Unterschied zwischen den „ethischen Hackern“ der CONSULECTRA und böswilligen Angreifern besteht darin, dass die „ethischen Hacker“ keinen Schaden anrichten und keine Informationen stehlen. Es geht ausschließlich um die Identifizierung von Schwachstellen.

Regelmäßige Penetrationstests helfen dabei, sensible Informationen wirkungsvoll gegen Hacker-Angriffe zu schützen. Unternehmen können ihre IT-Systeme und Anwendungen somit zuverlässig absichern, indem sie sicherheitsrelevante Schwachstellen rechtzeitig erkennen und beheben können.

Bei einem Penetrationstest können zwei Vorgehensweisen ausgewählt werden. Zum einen gibt es den Black-Box-Test, bei dem der Penetrationstester keine Informationen über das zu testende System oder die zu testende Anwendung besitzt. Diese Vorgehensweise entspricht einem realen Angriff, bei dem der Angreifer sich die Informationen aus öffentlichen Datenbanken besorgen muss. In den meisten Fällen bekommt der Penetrationstester eine IP-Adresse oder einen Domainnamen vom Auftraggeber. Zum anderen gibt es sogenannte White-Box-Tests, in denen der Penetrationstester umfangreiche Informationen über das zu testende System oder die zu testende Anwendung vom Auftraggeber erhält.

Die Sicherheit der IT-Systeme und Anwendungen kann dabei aus zwei Perspektiven geprüft werden.

Das Angriffsszenario des klassischen Hackers simuliert einen externen Angriff über das Internet oder andere öffentlich erreichbare IT-Systeme.

Beim Innentäter-Szenario werden Angriffe aus dem eigenen Unternehmensnetzwerk heraus nachgestellt.

Die Anforderungen komplexer IT-Infrastrukturen erfordern eine individuelle Betrachtung möglicher Sicherheitsschwachstellen. Daher definieren wir zunächst mit Ihnen gemeinsam individuelle Angriffsszenarien, die anschließend manuell und teilweise automatisiert geprüft werden.

Die CONSULECTRA bietet für Penetrationstests unterschiedliche Module an. Diese Module umfassen Webseiten und Webanwendungen, Leitsysteme und industrielle Steuerungssysteme (SCADA / ICS) sowie sonstige IT-Systeme.

Insbesondere bei produktiv genutzten kritischen Anwendungen und IT-Systemen agieren wir zurückhaltend und zeigen Schwachstellen auf, ohne diese tatsächlich aktiv auszunutzen. Nur so können wir sicherstellen, dass der Penetrationstest zuverlässige Ergebnisse liefert, ohne dabei den Geschäftsbetrieb negativ zu beeinflussen.

Mit unserer unternehmensübergreifenden Expertise und dem „Blick von außen“ helfen wir Unternehmen somit bei der Erfüllung von Anforderungen aus dem Informationssicherheitsmanagementsystem (ISMS) zur Durchführung von technischen Prüfungen und Penetrationstests.

Neugierig geworden?
Dann fordern Sie weitere Unterlagen an zu:

- Vorgehensmodell für Penetrationstests
- Beschreibung der Module der Dienstleistung Penetrationstests
- Modul: „Webseiten & Webanwendungen“
- Modul: „Leitsysteme & industrielle Steuerungssysteme“
- sonstigen IT-Systemen.

Für weitere Informationen wenden Sie sich bitte an:
Christian Book
Telefon: +49 40 27899-252
E-Mail: c.book@consulectra.de