Brunel

Interaktiver Fachvortrag:
Cyber Security mit Brunel

Überblick

Sicherheit im IT-Bereich ist nicht nur eine unverzichtbare Voraussetzung im Arbeitsalltag, sondern in allen Lebenslagen. In der Veranstaltung Cyber Security mit Brunel zeigen IT-Sicherheitsexperten, entweder in Echtzeit oder anhand realer Beispiele, Risiken für Verbraucher und Unternehmen einer vernetzten Welt auf. Dabei werden Sachverhalte, orientiert am Kenntnisstand der Teilnehmer, verständlich erklärt und präventive Maßnahmen aufgezeigt, die von den Hörern direkt umgesetzt werden können.

Ziel

Die Teilnehmer sollen für IT-Sicherheitsthemen sensibilisiert werden. Ziel ist es, hilfreiches Wissen und Lösungsansätze zur Vermeidung von Gefahren zu vermitteln.
Brunel als IT-Spezialist setzt sich für ein verantwortungsvolles Verhalten im Onlinebereich ein.

Zielgruppe

Aufgrund der fachlichen Nähe richtet sich diese Vortragsreihe an Ingenieure aller Fachrichtungen, Informatiker, Naturwissenschaftler und Techniker.

Trainer

Chris Wojzechowski:
Chris Wojzechowski studiert Internet-Sicherheit an der Westfälischen Hochschule in Gelsenkirchen. Er schreibt seine Masterarbeit zum Thema CEO-Fraud. Gemeinsam mit Matteo Cagnazzo ist er Geschäftsführer der AWARE7 GmbH. Er verantwortet in erster Linie den exekutiven Teil der GmbH und die menschliche Komponente der IT-Sicherheit. Die Analyse und niederschwellige Aufbereitung komplexer Angriffsszenarien gehören zu seiner Kernkompetenz. Im Rahmen seiner Tätigkeit schult er, von Schülern bis zu DAX-Vorständen, den gewissenhaften, sicheren Umgang mit IT.

Matteo Cagnazzo:
Matteo Cagnazzo studierte Internet-Sicherheit an der Westfälischen Hochschule in Gelsenkirchen. Aktuell schreibt er seine Doktorarbeit zum Thema “IT-Sicherheit und Datenschutz in der Medizintechnik”. Gemeinsam mit Chris Wojzechowski ist er Geschäftsführer der AWARE7 GmbH. Er verantwortet in erster Linie den technischen Teil der GmbH und die technische Komponente der IT-Sicherheit. Am Institut für

Internet-Sicherheit hat er den Bereich “Vertrauenswürdiges Gesundheitswesen” geleitet. Im Rahmen seiner Tätigkeit schult er, vom Schüler bis zum Dax-Vorstand, den gewissenhaften und sicheren Umgang mit IT.

Themen:

- **IT-Sicherheit allgemein (für Ingenieure):**
  Passwörter, WLAN, E-Mails, soziale Netzwerke, USB Geräte, Call ID Spoofing
- **Sicherheit im Internet der Dinge (Ingenieure):**
  Informationsbeschaffung, aktives/automatisiertes Scanning, Übernahme von Geräten, Man in the Middle, Sicherheitsmechanismen
- **Social Engineering (für Informatiker):**
  Soziale Netzwerke, Scanning, Spam und Phishing, sicheres WLAN, gefälschte Webseiten
- **Sicherheitslücken bei Webanwendungen (Informatiker):**
  Informationsbeschaffung, aktives/automatisiertes Scanning, Fuzzing, Man in the Middle, Sicherheitsmechanismen

Nutzen für die Teilnehmer

Die Teilnehmer werden für IT-Sicherheitsthemen aus ihrem Alltag anschaulich sensibilisiert. Hierbei werden Betrugstaktiken von Kriminellen vorgestellt, sodass sie eine gesunde Skepsis an den Tag legen und erlerntes Wissen zur Abwehr von Online-Kriminalität anwenden können. Somit können sie sich sicherer im privaten aber auch beruflichen Online-Umfeld bewegen und einen wertvollen Beitrag zur Online-Sicherheit im Unternehmen leisten.

Teilnehmerzahl

Die Teilnehmerzahl kann je nach Veranstaltung variieren. Da das Format auf einem Vortrag basiert, in dem auch Fragen aus dem Publikum beantwortet werden, gibt es an sich keine Begrenzung nach oben. Je kleiner die Gruppe ist, desto höher ist das Interaktionsniveau.

Dauer

2 Stunden oder 4 Stunden
Jeweils Vortrag inkl. Rückfragen und Get-together mit dem Referenten im Anschluss
Die Uhrzeit ist nach Absprache flexibel.

Seminarraum und Hilfsmittel

Der Seminarraum sollte ausreichend **Platz für die entsprechende Teilnehmeranzahl** und die Firmenvertreter bieten.
Für das Training sollte idealerweise folgende Ausstattung zur Verfügung stehen.

- Ein Beamer mit VGA- oder HDMI-Anschluss
- WLAN Zugang

- Ggf. Mikrofon und Lautsprecher

Sollte es nicht möglich sein, die technischen Anforderungen zu erfüllen, können ggf. die technischen Geräte der Referenten zum Einsatzort mitgebracht werden

Cyber Security Themen:

IT-Sicherheit allgemein (für Ingenieure)

Passwörter (15 Min.)

- Sicherheitslücken bei Passwörtern erkennen und verhindern

WLAN (15 Min.)

- Seriöse Hotspots identifizieren

E-Mails (15 Min.)

- Spam und Phishing Mails rechtzeitig erkennen

Soziale Netzwerke (15 Min.)

- Sicherer Umgang mit Sozialen Netzwerken

USB Geräte (15 Min.)

- Sichere Handhabung von USB Sticks

Call ID Spoofing (15 Min.)

- Identifikation möglicher Anrufer

Das Internet of Things (Ingenieure und Informatiker)

Einführung und Motivation (15 Min.)

- Relevanz von IT-Sicherheit für Fachkräfte
- Definition des Internet of Things (IoT)
- Definition von Sicherheitslücken und Angriffen im IoT
- Betrachtung OWASP Top 10

Informationsbeschaffung (15 Min.)

- Überblick in die offensive Datenverarbeitung von Angreifern durch Scanning des IoT und dazugehörigen Entitäten

Aktives (automatisiertes) Scanning (15 Min.)

- Methoden von Angreifern das IoT und Netzwerke zu scannen, um einen optimalen Informationsgewinn zu erhalten
- Besprechung von Sicherungsmaßnahmen, um diese Angriffe zu verhindern
- Verwendung und Vorstellung unterschiedlicher Suchmaschinen zur Informationsbeschaffung

Übernahme von Geräten (15 Min.)

- Sicherheitslücken, die den gezielten Absturz von Geräten begünstigen
- Übernahme von Geräten (Beispiel: Drohne/Spielzeug)
- Sicherungstools

Man in the Middle (15 Min.)

- Konfiguration eines Proxys, um Netzwerkverkehr mitzuschneiden
- Konfiguration eines Rogue Access Points um TLS-Verbindungen zu umgehen

Sicherheitsmechanismen (15 Min.)

- Möglichkeiten, um Sicherheitslücken zu schließen
- Sinnhaftigkeit eines externen Testings

Social Engineering (für Informatiker)

Einführung und Motivation (15 Min.)

- Definition von Social Engineering
- Relevanz von aktuellen Angriffsmethoden durch Sicherheitslücken und Schließung dieser

Soziale Netzwerke (15 Min.)

- Überblick über die offensive Datenverarbeitung von Angreifern in Sozialen Medien und Absicherungsmöglichkeiten
- Betrachtung von Facebook, Twitter und Nischennetzwerken

Scanning (15 Min.)

- Methoden von Angreifern technische Systeme und Netzwerke zu scannen, um einen optimalen Informationsgewinn zu erhalten
- Besprechung von Sicherungsmaßnahmen, um diese Angriffe zu verhindern

Spam und Phishing (15 Min.)

- Wie Informationen aus Sozialen Netzwerken und Scanning für Spam und Phishing Kampagnen genutzt werden können
- Sicherheitsaspekte rund um das Mobiltelefon

Sicheres WLAN (15 Min.)

- Übersicht über mögliche Sicherheitslücken im WLAN
- Wie Netzwerke gefälscht werden können und anhand welcher Merkmale diese erkannt werden können

Gefälschte Webseiten (15 Min.)

- Merkmale gefälschter Captive Portals in unsicherem WLAN
- Betrachten von Subdomains und Sicherung dieser gegen Angriffe

Sicherheitslücken bei Webanwendungen (für Informatiker)

Einführung und Motivation (15 Min.)

- Welche Risiken bergen Sicherheitslücken bei Webanwendungen
- Definition eines Angriffs auf eine Webanwendung
- Betrachtung der OWASP Top 10

Informationsbeschaffung (15 Min.)

- Einblick in die offensive Datenverarbeitung von Angreifern durch Scanning von Webanwendungen und dazugehörigen Entitäten
- Schutzmechanismen

Aktives (automatisiertes) Scanning (15 Min.)

- Informationsgewinn durch Scanning von Webapplikationen und von Netzwerken
- Maßnahmen zur Verhinderung von Scanning

Fuzzing (15 Min.)

- Sicherheitslücken, die den gezielten Absturz von (Web)Applikationen begünstigen und Daten, die dazu verwendet werden
- Sicherungstools

Man in the Middle (15 Min.)

- Konfiguration eines Proxys, um Netzwerkverkehr mitzuschneiden
- Konfiguration eines Rogue Access Points um TLS-Verbindungen zu umgehen
- Schutzmechanismen gegen Mittschnitte

Sicherheitsmechanismen (15 Min.)

- Möglichkeiten zur Schließung von Sicherheitslücken
- Sinnhaftigkeit externen Testings