THE PENTEST EXPERTS.

HACKING & SECURITY 2022

SICHERHEIT TRAINIEREN – KOMPETENZEN AUSBAUEN


SEBASTIAN SCHREIBER
GESCHÄFTSFÜHRER

EIN WORT VORWEG

IT-Systeme und Anwendungssoftware entwickeln sich kontinuierlich weiter. Entsprechend feilen auch Hacker stetig an ihren Fertigkeiten, um neue Software und Hardware anzugreifen. Meine IT Security Consultants und ich nehmen die hieraus entstehenden Herausforderungen immer wieder aufs Neue an. Seit über 20 Jahren bauen wir unser Wissen und unsere Erfahrung stetig aus. So sind und bleiben wir ein verlässlicher Partner, der Ihnen Wissen rund um IT-Sicherheit und Hacking vermittelt und Sie vor unliebsamen Eindringlingen schützt.

Unser Schulungsprogramm deckt alle Bereiche der IT Security ab: In unseren Hacking-Schulungen (Hack 1 bis 9) übernehmen Sie die Perspektive von Angreifenden und lernen Grundlagen des Hackens und aktuelle Angriffe gegen Webapplikationen, Windows-basierte Netzwerke, VoIP-Infrastrukturen oder WLAN kennen. Zum Hacking von mobilen Endgräten und IoT-Produkten bieten wir ebenfalls spezielle Kurse an. Und auch die Funktionsweise und Entwicklung von Exploits können Sie bei uns lernen.

Unsere Security-Schulungen (Secu 1 bis 7) fokussieren ein breites Spektrum von Grundlagen der IT-Sicherheit und der digitalen Selbstverteidigung, über IT- und datenschutzrechtliche Fragestellungen sowie organisatorische und konzeptuelle Rahmenbedingungen von Penetrationstests, bis hin zu digitaler Forensik und Incident Response.

Mit diesem umfangreichen Angebot und unserer breiten Expertise stehen mein Team und ich Ihnen gerne zur Seite. Wünschen Sie darüber hinaus eine Beratung? Wir stehen Ihnen jederzeit zur Verfügung.

Herzliche Grüße, Ihr Sebastian Schreiber

P.S.: Profitieren Sie auch von unseren Newslettern „SySS Management News“ und „SySS Research News“, die Sie regelmäßig mit IT-Sicherheits-Know-how und Security Advisories auf dem Laufenden halten. Der nebenstehende QR-Code bringt Sie direkt zur Anmeldeseite.

Wir, die SySS GmbH, sind ein Unternehmen für IT-Sicherheit, spezialisiert auf Penetrationstests.

Seit der Gründung 1998 durch unseren Geschäftsführer Sebastian Schreiber führen wir hochwertige Sicherheitstests durch. Bei unserer Arbeit verbinden wir hohen technischen Anspruch mit der von uns entwickelten Ethik für Penetrationstester.

INHALT

HACK1/HACK2: HACKING WORKSHOP TEIL 1 & 2

Leitung: Sebastian Auwärter, Marcel Mangold

Computermissbrauch und Cyberkriminalität bedrohen IT-Netze tagtäglich. Meist geschehen sie sehr unauffällig und werden erst bemerkt, wenn der Schadensfall schon eingetreten ist. Somit sind sie eine ernst zu nehmende Bedrohung. Damit Unternehmen ihre IT-Umgebung vor Gefahren dieser Art besser schützen können, haben wir die Workshops Hack1 und Hack2 entwickelt. Wir betrachten das Thema IT-Sicherheit aus der Perspektive eines Täters bzw. „Hackers", was dabei helfen soll, Netzwerke im eigenen Verantwortungsbereich besser abzusichern. Beide Workshops können unabhängig voneinander besucht werden, jedoch baut Workshop 2 auf Workshop 1 auf.

WORKSHOP 1

Themen

- Informationsquellen
  - Identifikation erreichbarer Systeme; Suche nach Hinweisen auf potenzielle Angriffsziele
- Standard-Sicherheitswerkzeuge und ihr Einsatz
  - Portscanner, Sniffer
- Man-in-the-Middle-Angriffe
  - Vor allem in lokalen Netzen können Man-in-the-Middle-Angriffe verwendet werden, um verschlüsselten Datenverkehr oder auch VoIP-Telefonate mitzulesen bzw. mitzuhören. Im Rahmen des Workshops werden Angriffsszenarien durchgeführt und Schutzmechanismen besprochen.
- Passwortsicherheit unter Linux, Windows und in Windows-Netzen
  - Anhand verschiedener Cracking-Techniken schätzen wir die Sicherheit ein, die eine Passwortrichtlinie bietet.
- Ausnutzen von Sicherheitslücken
  - Vorgehensweise von Angreifenden bei der Ausnutzung von Schwachstellen (Verwendung von Exploits, Trojanisierung des Zielsystems)

WORKSHOP 1
Techn. Voraussetzungen: Grundkenntnisse über Betriebssysteme, Netzwerke, Linux, Windows, TCP/IP
Termine: 18.-19.01.2022 / 22.-23.03.2022 / 10.-11.05.2022 / 12.-13.07.2022 / 27.-28.09.2022 (2 Tage)
Preis: € 1500,00*

WORKSHOP 2
Techn. Voraussetzungen: Grundkenntnisse über Betriebssysteme, Netzwerke, Linux, Windows, TCP/IP
Termine: 20.-21.01.2022 / 24.-25.03.2022 / 12.-13.05.2022 / 14.-15.07.2022 / 29.-30.09.2022 (2 Tage)
Preis: € 1500,00

WORKSHOP 2

Themen

- Metasploit-Framework
  - Einführung und Umgang mit unterschiedlichen Modulen
- Sicherheit in Windows-Netzen
  - Eskalation von Benutzerrechten auf lokalen Windows-Systemen sowie im Windows-Netzwerk bis hin zur Berechtigung eines Domänenadministrators
  - Verständnis von typischen Vorgehensweisen wie Pass-the-Hash
  - Extraktion von Klartextpasswörtern und Übernahme von Benutzersitzungen
- Schwachstellenscanner
  - Funktionsweise, Konfiguration und Umgang mit einem Schwachstellenscanner
- Tunneling
  - Verwendung harmloser Protokolle zur verdeckten Übertragung von Daten
  - Umlenken von Netzwerkverkehr über kompromittierte Systeme, um Firewalls zu umgehen oder Remote-Zugriff zu erlangen

* Für weitere Informationen zu den Preisen, siehe S. 23.

HACK3: ANGRIFFE AUF WINDOWS-BASIERTE NETZWERKE

Leitung: Sebastian Hölzle, Daniel Isern, Franz Jahn, Michael Kramer, Dr. Adrian Vollmer, Wolfgang Zejda

Zur technischen Organisation von Computern, Usern, Gruppen und weiteren Objektklassen wird in Unternehmensnetzwerken in der Regel auf einen Verzeichnisdienst zurückgegriffen. Weit verbreitet sind in Windows-basierten Netzwerken die auf dem Domänen-Vertrauensprinzip basierenden Active Directory Domain Services. Gelingt es Angreifenden, initial von außen in das interne Netzwerk einzudringen, so können sie innerhalb dieses Verzeichnisdienstes ihre Rechte meist mit überschaubarem Aufwand ausweiten. In dieser Schulung sollen ein tieferer Einblick in die Vorgehensweise von Angreifenden gewährt und Gegenmaßnahmen aufgezeigt werden. Theoretische Konzepte werden erläutert und Angriffsvektoren anhand von praxisbezogenen Übungen erprobt.

Themen

- Windows-basierte Netzwerke
  - Fokus: Active Directory
  - Ermittlung von Gesamtstruktur und Vertrauensstellungen
  - Berechtigungs- und Authentifizierungskonzepte
  - Hash-Typen in der Microsoft-Welt
- Angriffe auf Einzelsysteme und Netzwerkprotokolle
  - Ausnutzung von Schwachstellen
  - Angriffe gegen Authentisierungsmechanismen
  - Ausnutzung schwacher Dienstekonfigurationen
  - Angriffe gegen Kerberos (z. B. Golden Ticket)
  - Traffic-basierte Angriffe (NBNS, MitM)
- Rechteausweitung/Ausbreitung
  - Mangelhafter Passwortschutz
  - Ausnutzung von „Features“, „Spuren“
  - Access Token und „gecachte“ Passwörter
  - Pass-the-Hash-Angriffe
  - Group Policy Objects/Preferences
  - Ermittlung von Berechtigungsstrukturen
- Einsatz geeigneter Tools
  - Nmap und Metasploit
  - PowerShell-Tools
  - BloodHound
  - Cracking-Tools
  - Tools für spezielle Einsatzzwecke
- „Best Practice“-Schutzmaßnahmen
  - Detektionsverfahren
  - IT Security-Prinzipien
  - Berechtigungsmodelle
  - Konfigurationsempfehlungen

Techn. Voraussetzungen: Grundkenntnisse von Linux- und Windows-basierten Systemen und Netzen
Termine: 22.-24.02.2022 / 21.-23.06.2022 / 13.-15.09.2022 / 06.-08.12.2022 (3 Tage)
Preis: € 2250,00

HACK4: ANGRIFFE GEGEN VOIP-INFRASTRUKTUREN

Leitung: Moritz Abrell, Ludwig Stage

Die Kommunikation über Voice-over-IP ist längst gängige Praxis und in vielen Unternehmensbereichen zu finden. Neben der traditionellen Telefonie sind auch Audio-/Videokonferenzen, Chats, Softphones, aber auch z. B. die Kommunikation über den Browser die derzeitigen Anforderungen an die Kommunikation. Dieser Verbund an Kommunikationsfunktionen wird auch als Unified Communication (UC) bezeichnet. Doch die daraus resultierenden, teilweise hochkomplexen UC-Szenarien sind risikoreich und können auch die angrenzende Unternehmensinfrastruktur akut gefährden.

Im Rahmen eines zweitägigen Workshops wird die Perspektive von Angreifenden eingenommen. Die Teilnehmenden werden Gespräche belauschen, Verschlüsselungsverfahren aufbrechen, Schutzmaßnahmen umgehen, Zugriff auf Geräte und Systeme erlangen sowie ihre Rechte ausweiten. Der Workshop soll einen tieferen Einblick in die Vorgehensweise von Angreifenden geben, damit die Kursteilnehmenden bei der Nachbereitung die Risiken im eigenen Netzwerk identifizieren, einschätzen und minimieren können. Theoretische Konzepte werden erläutert und erlernte Angriffsvektoren anhand von praxisbezogenen Übungen erprobt.

Themen

- Technische Grundlagen
  - Unified Communication und Voice-over-IP
  - Einführung in die Technologien (SIP, RTP, WebRTC u. a.)
  - Terminologie und Aufbau
  - Verschlüsselungsverfahren
- Angriffsverfahren
  - Man-in-the-Middle-Angriffe
  - Angriffe gegen Authentisierungsverfahren
  - Angriffe gegen Verschlüsselungsverfahren
  - Autodeployment- und Provisionierungsangriffe
  - Angriffe gegen die Vertraulichkeit von Daten
  - SIP Trunking-Angriffe
  - Interactive Connectivity Establishment (ICE)-Angriffe
  - Angriffe gegen Session Border Controller (SBC)
- Schutzmaßnahmen
  - Erkennungsmöglichkeiten
  - IT Security-Prinzipien
  - Konfigurationsempfehlungen
  - Best Practices

Techn. Voraussetzungen: Grundkenntnisse in Netzwerktechnik
Termine: 14.-15.03.2022 / 07.-08.11.2022 (2 Tage)
Preis: € 1500,00

HACK5: EXPLOIT DEVELOPMENT

Leitung: Matthias Deeg

Diese Schulung vermittelt die theoretischen und praktischen Grundlagen der Funktionsweise und Entwicklung von Exploits. Dabei soll vorrangig betrachtet werden, wie Zielplattformen aufgebaut sind, welche Besonderheiten sie aufweisen, welche verschiedenen Formen der Schwachstellenanalyse existieren, welche Werkzeuge für die Exploit-Entwicklung wichtig sind (Debugger, Disassembler, Exploit-Frameworks etc.) und wie diverse Schwachstellentypen ausgenutzt werden können. Ferner geht die zweitägige Schulung darauf ein, welche Möglichkeiten existieren, sich gegen eine Ausnutzung der gezeigten Schwachstellen durch Angreifende zu schützen, und wie Hacker solche Schutzmaßnahmen möglicherweise umgehen können.

Themen

- Besonderheiten verschiedener Zielplattformen
  - Prozessorarchitektur: x86
  - Betriebssysteme: Windows, Unix/Linux
- Verschiedene Formen der Schwachstellenanalyse
  - Statische Codeanalyse
    - » Quellcodeanalyse
    - » Analyse von Binärprogrammen (Reverse Code Engineering)
  - Dynamische Codeanalyse (Laufzeitanalyse)
    - » Verhaltensbasierte Sicherheitsanalyse
    - » Fuzzing
- Tools of the Trade: Wichtige Werkzeuge für die Exploit-Entwicklung
  - Debugger/Disassembler/Exploit-Frameworks/Assembler (x86)
  - Programmiersprache der Wahl (z. B. C/C++, Python, Perl, Ruby etc.)
- Ausnutzung verschiedener Schwachstellentypen
  - Fehler in der Hard- und Softwarearchitektur sowie in der Anwendungslogik
  - Fehler in der Datenverarbeitung, z. B.
    - » Buffer Overflow-Schwachstellen (Stack, Heap, Off-by-One)
    - » Format String-Schwachstellen
- Schutzmaßnahmen und Umgehungsmöglichkeiten
  - Stack Cookies
  - SafeSEH
  - Data Execution Prevention (DEP)
  - Address Space Layout Randomization (ASLR)

Techn. Voraussetzungen: Grundkenntnisse über Betriebssysteme und Rechnerarchitektur
Termine: 07.-08.03.2022 / 04.-05.07.2022 (2 Tage)
Preis: € 1500,00

HACK6: MOBILE DEVICE HACKING

Leitung: Philipp Buchegger

Mobile Devices sind aus dem Unternehmensumfeld nicht mehr wegzudenken und übernehmen schon lange nicht mehr nur die Aufgabe eines Telefons. Mittlerweile ist es weit verbreitet, dass viele Beschäftigte auf ihren mobilen Geräten E-Mails bearbeiten, ins Internet gehen und eine große Menge an oftmals vertraulichen Unternehmensdaten bewegen. Diese Konzentration an interessanten Daten macht Mobile Devices für Angreifende sehr attraktiv.

Dieser Workshop richtet sich an User, die Sicherheitsaspekte von mobilen Endgeräten besser verstehen wollen, beispielsweise für die Integration in die eigene Unternehmensinfrastruktur. Neben der Verwaltung der Geräte werden die kritischen Angriffspunkte beleuchtet. Ferner werden durch praxisbezogene Übungen verschiedene Schwachstellen analysiert und aufgezeigt, deren theoretische Grundlagen zuvor erarbeitet wurden.

Themen

- Allgemeine Informationen
  - Eigenschaften von Mobile Devices
  - Verwaltung mobiler Endgeräte im Unternehmen
  - Mobile Device Management-Lösungen
- Angriffstechniken
  - Physischer Zugriff auf das Gerät
  - Hardware-Hacks
  - Mitschnitt des Datenverkehrs
  - Man-in-the-Middle-Angriffe
- Apple iOS
  - Sicherheitskonzept von iOS-Geräten
  - Angriffe auf Apps mit einem Proxy
  - Reverse Engineering von Apps
  - Laufzeitmanipulation
- Google Android
  - Sicherheitskonzept von Android
  - Angriffe auf alte und aktuelle Android-Versionen
  - Emulation eines Android-Smartphones
  - Rooting Detection und Certificate Pinning
  - Angriffe auf Services, Content Provider etc.
  - Reverse Engineering von Apps
  - Laufzeitmanipulation

Techn. Voraussetzungen: Grundlagen in Linux
Termine: 31.01.-01.02.2022 / 02.-03.05.2022 / 10.-11.10.2022 (2 Tage)
Preis: € 1500,00

HACK7: SICHERHEIT UND EINFALLSTORE BEI WEBAPPLIKATIONEN

Leitung: Torsten Lutz, Marcel Mangold, Dr. Oliver Schwarz, Robin Trost

Schwachstellen in Webapplikationen sind für Angreifende besonders attraktiv, denn diese ermöglichen es ihnen in vielen Fällen, vertrauliche Daten zu stehlen oder ins Unternehmensnetzwerk vorzudringen.
Im Rahmen des zweitägigen Workshops lernen die Teilnehmenden, wie Hacker in Webapplikationen einbrechen und welchen Risiken diese Anwendungen ausgesetzt sein können. Die Schulung zeigt die gängigsten Angriffe in Theorie und Praxis. Ziel ist es, dass die Teilnehmenden am Ende des zweiten Schulungstages selbst Angriffe auf eine eigens hierfür erstellte Webapplikation durchführen können.

Themen

- Cross-Site Scripting (XSS)
  - Angriffe auf Sitzungsinformationen, Phishing und Defacing
- Cross-Site Request Forgery (XSRF)
- SQL Injection
- OS Command Injection
- Local/Remote File Inclusion (LFI/RFI)
  - Angriffe auf Server mit eigenem Programmcode
- Sessionmanagement
  - Sessionmanagement kennenlernen
  - Durchführung von Session Hijacking
  - Cookie-Verständnis und Fehlerausnutzung
  - Passwort-Rate-Angriffe
- Cookies
  - Was bei der Generierung und Verwendung von (Session-)Cookies zu beachten ist
- Browsersicherheit
  - Same-Origin Policy
  - Cross-Origin Resource Sharing
- CAPTCHA
  - Automatisierte Angriffe und Identifikation von Schwächen bei den Schutzmaßnahmen
- Übungen
  - Festigung der Lerninhalte anhand von Übungen zu allen Themen
  - Abschließende eigenständige Analyse einer vollständigen Webapplikation
  - Deserialisierungsangriffe

Techn. Voraussetzungen: Grundkenntnisse in HTML, HTTP und SQL
Termine: 08.-09.02.2022 / 24.-25.05.2022 / 19.-20.07.2022 / 20.-21.09.2022 (2 Tage)
Preis: € 1500,00

HACK8: WLAN HACKING UND WLAN SECURITY

Leitung: Michael Schmidt

Wireless LAN ist eine äußerst attraktive Technologie. Sie ermöglicht einer Vielzahl von Geräten die kabellose Nutzung des Internets und einen schnellen, unkomplizierten Zugang zum World Wide Web. Im Zuge der Verbreitung entsprechender Geräte nehmen öffentliche Hotspots zu und die zur Verfügung stehende Bandbreite wächst stetig an. Doch wie sicher ist WLAN? Gehen die Entwicklung von WLAN und von entsprechenden Schutzmaßnahmen gegen Missbrauch Hand in Hand? Die Schulung vermittelt grundlegendes Wissen zu WLAN und WLAN-Sicherheit. Die Teilnehmenden lernen gängige Angriffe kennen und erfahren, wie sie sich gegen diese wappnen können.

Themen

- Grundlagen der WLAN-Technologie
  - Standards
  - Begriffe
- Aufbau einer WLAN-Umgebung
  - Unter Linux
- WLAN Sniffing
  - Ausspähen ungesicherter Drahtlosnetzwerke
- Sicherheitsansätze des 802.11-Standards
  - Betrachtung von Schwächen
  - SSID/MAC-basierte Filter, WEP
- Erweiterungen des 802.11-Standards
  - WPA, WPA2
- Authentifizierung in 802.11i
  - 802.1x, EAP, PSK
- Schlüsselmanagement in 802.11i
  - Schlüsselhierarchien
  - Handshakes
- Funktionsweise der Verschlüsselungs-mechanismen
  - WEP
  - TKIP
  - CCMP
- WLAN Hacking
  - DoS-Angriffe
  - WEP Cracking
  - Angriffe gegen WPA/WPA2-PSK
  - Angriffe gegen WPS
  - Angriffe gegen WPA2-Enterprise
  - Evil Twin-Angriffe
  - Angriffsmöglichkeiten gegen Captive Portals
  - Das Smartphone: ein hilfreiches Werkzeug

Techn. Voraussetzungen: Grundkenntnisse in Netzwerktechnik

Termine: 01.-02.03.2022 / 26.-27.07.2022 (2 Tage)

Preis: € 1500,00

HACK9: EMBEDDED SECURITY

Leitung: Gerhard Klostermeier

Im Zeitalter von IoT-Geräten, smarten Autos oder Industriesteuerungen ist das Thema „Embedded Security" nicht mehr wegzudenken. Wenn die Beleuchtung mit dem Handy gesteuert wird, Autos mehr als 100 Computer enthalten und der reibungslose Ablauf der Produktion im Internet geprüft werden kann, tun sich auch für Angreifende viele Wege auf, ein System zu kompromittieren. Nicht zu vernachlässigen sind dabei die IT-Sicherheit der eigentlichen Hardware und die folgenden Fragestellungen: Wurden Debug-Zugänge nach der Produktion geschlossen? Können Angreifende sensible Daten aus dem Speicher auslesen oder gelingt es ihnen gar, eigenen Code auf dem Gerät auszuführen? Wer selbst einmal typische Schwachstellen ausgenutzt hat, erkennt schnell, was bei der Prävention von solchen Sicherheitsproblemen wichtig ist. Die Teilnehmenden werden daher selbst zu Angreifenden und lernen anhand praxisnaher Übungen, wie Embedded Devices angegriffen und abgesichert werden. Die Boards, auf denen sie die Übungen machen, sind im Preis inbegriffen. Die Teilnehmenden dürfen sie behalten und zuhause weiterhacken.

Themen

- Allgemeines
  - Grundlagen von Embedded Security
  - Arbeiten am PCB
  - Hardwarekomponenten zuordnen
  - Datenblätter lesen und verstehen
  - Was passiert beim Booten?
  - Dateisysteme für Embedded Devices
- Typische Schnittstellen
  - UART
  - I2C/SPI
  - JTAG/SWD
- Sicheres Booten
  - Absichern von U-Boot
  - Secure Boot
- Daten sicher speichern
  - Interne/externe Speicher
  - Hardware Security Module (HSM)
- Umgang mit diversen Tools
  - Logic Analyzer
  - JTAGulator/JTAGEnum
  - JTAG Debug Probe/J-Link
  - UART-Adapter (FT232H)

Techn. Voraussetzungen: Grundlagen im Umgang mit Linux

Termine: 11.-13.04.2022 / 17.-19.10.2022 (3 Tage)

Preis: € 3000,00

SECU1: DIGITALE FORENSIK BEI COMPUTERN UND SMARTPHONES

Leitung: Dr. Markus a Campo

Immer wieder sind Firmennetze Ziele für Hackerangriffe und Unternehmen Opfer von Eindringlingen, die sensible Daten ausspähen und diese illegal weiterverwenden. Um in solchen Fällen Klarheit zu erlangen, wird der Angriff forensisch untersucht. Spuren werden identifiziert und (gerichtsverwertbar) gesichert. Die Ergebnisse werden ausgewertet und als Beweismittel aufbereitet. In der Schulung werden grundlegende Fragestellungen der IT-Forensik und angewandte Standardtechniken analysiert und ausprobiert.
Da auf Smartphones sowohl private als auch dienstliche Daten in großer Zahl abgelegt werden, sind auch diese Geräte eine ergiebige Quelle forensischer Untersuchungen. Ein Zugriff auf die Daten ist meist nur eingeschränkt möglich, sodass spezielle Tools zum Einsatz kommen. Die Sicherung und Analyse von Beweismitteln wird anhand von praktischen Übungen und Fallbeispielen verdeutlicht.

Themen

- IT-Forensik und Incident Response
- Behandlung von Sicherheitsvorfällen
- Sicherung von Beweisen, lokal und über das Netzwerk
- Sicherstellung der Authentizität von Beweisen, Gerichtsverwertbarkeit
- Forensik-Tools und -Toolkits
- Analyse der erhobenen Daten
  - Werkzeuge unter Windows und Linux
  - Suche nach versteckten Spuren
  - Ermittlung von Ursachen, Schäden und Angriffsszenarien
  - Rückschlussmöglichkeiten auf Ziele und Kenntnisstand des Täters
- Smartphone-Forensik
  - Grundsätzliche Fragestellungen sowie Forensik bei iOS, Android, Windows Phone
  - Spezielle Werkzeuge für die Smartphone-Forensik
- Smartcard-Forensik am Beispiel von EMV-Chips
- Cloud-Forensik
- Verfassen von gerichtskonformen Berichten
- Projektmanagement: IT-Forensik
  - Zusammenarbeit mit Strafverfolgungsbehörden, rechtliche Situation

Techn. Voraussetzungen: Grundkenntnisse über Netzwerke unter Windows, Linux oder Unix
Termine: 04.-06.04.2022 / 28.-30.11.2022 (3 Tage)
Preis: € 2250,00

SECU2: INCIDENT RESPONSE

Leitung: Joscha Hänel, Timothy Mason, Jürgen Steinel, Dr. Klaus Tichmann

Alle Welt redet von „Cyberwar", Industriespionage und Datenklau. Werden Angriffe bemerkt, ist es wichtig, überlegt und organisiert zu handeln. Der angebotene Workshop bietet eine Handlungsgrundlage, um adäquat auf IT-Sicherheitsvorfälle reagieren zu können.

Themen

- Grundsätzlicher Ablauf Incident Response
  - 5-Phasen-Modell
  - Was geht nur intern? Was ist auslagerbar?
  - Dos and Don'ts (unbekannte Tools, „Blaming" etc.)
- Vorbereitung: Incident Readiness
  - Grundsätzliche Tools
  - Personelle Vorbereitung
    - » „Know your tools, know your procedures"
  - Organisatorische Vorbereitung
  - Technische Vorbereitung
  - Analyse des bestehenden Netzwerks
    - » „Baselining", Struktur etc.
- Angriffserkennung
  - Arbeitsweise von Hackern
  - Anti-Forensik-Maßnahmen und was man dennoch sieht
  - Warnungen von Dritten
  - IPS, SIEM etc.
- Angriffsanalyse
  - Logdateien und Protokolle
  - Sicherheitstests und Malware-Analyse
  - Identifikation des Angriffsvektors
  - Forensische Untersuchungen vs. Triage: Abwägung individueller Analysemethoden
- Abwehrmaßnahmen und Aufräumen
  - Die Wichtigkeit des Menschen beim Schutz von Systemen
  - Konzentration auf Bordmittel
  - Grenzen von IPS, SIEM, AV und Firewall
- „Lessons Learned" und organisatorische Strukturen
- Angriffsmuster und Analyse beispielhafter Angriffe
  - „Kenne deinen Feind"
  - Phishing und klassische Internetkriminalität
  - Ausforschung und gezielte Angriffe
  - OpSec und das Zusammenspiel von IT- und anderer Sicherheit
  - Analyse beispielhafter Angriffe

Techn. Voraussetzungen: Grundlegende Netzwerk- und Linux-Kenntnisse

Termine: 14.-16.02.2022 / 24.-26.10.2022 (3 Tage)

Preis: € 2250,00

SECU3: IPV6 SECURITY

Leitung: Marcel Mangold, Kien-Van Quang

Die Tage des Internetprotokolls in der Version 4 (IPv4) werden bald gezählt sein. Daher setzen viele Bereiche schon heute das Internetprotokoll in der Version 6 (IPv6) ein. Aktuelle Betriebssysteme unterstützen dieses Protokoll meist schon von sich aus, ohne dass eine Interaktion des Users notwendig wird. Dieser Umstand birgt die Gefahr, dass hier Sicherheitslücken entstehen können, derer sich IT-Sicherheitsbeauftragte oft nicht bewusst sind. Dennoch sollte der Datenverkehr mit IPv6 in gleicher Weise gesichert werden wie der mit IPv4.

Die Schulung führt im ersten Teil in die Funktionsweise von IPv6 ein und beschreibt im zweiten Teil, wie einzelne der zuvor kennengelernten Mechanismen von Angreifenden ausgenutzt werden können.

Themen

- Einführung in IPv6
  - Einführung in die Adresstypen
  - Übersicht über die Hilfsprotokolle
  - Teredo
  - Routing und Router Advertisements
  - DNS
- Firewalls und IPv6
  - Unfreiwillige Löcher im Sicherheitssystem durch IPv6
- Schwächen im internen Netzwerk
  - Denial-of-Service-Angriffe
  - Man-in-the-Middle-Angriffe
  - Routing-Angriffe
- Schwächen in Sicherheitsmechanismen
  - Umgehung durch Fragmentierung
- (Remote) Host Discovery
- Sicherheitsmaßnahmen
  - Secure Neighbor Discovery

Techn. Voraussetzungen: Grundkenntnisse zu IPv4
Termine: 29.03.2022 / 14.11.2022 (1 Tag)
Preis: € 750,00

SECU4: IT-RECHT UND DATENSCHUTZ FÜR IT-VERANTWORTLICHE

Leitung: Horst Speichert

IT-Verantwortliche müssen täglich Entscheidungen mit großer rechtlicher Tragweite treffen. Oft riskieren sie Rechtsverstöße, hohe Bußgelder oder stehen gar „mit einem Bein im Gefängnis". Ständig neue Gesetze und Urteile im IT-Recht und Datenschutz machen es notwendig, am Ball zu bleiben.
Rechtsanwalt Horst Speichert ist spezialisiert auf IT-Recht und Datenschutz, lehrt Informationsrecht an der Universität Stuttgart und hat das Fachbuch „Praxis des IT-Rechts" verfasst.

Themen

- Cloud-Verträge, internationaler Datentransfer, Brexit
- EuGH Schrems II
  - Notwendige Zusatzmaßnahmen, insbesondere MS 365
- Anforderungen Homeoffice, Videokonferenzen, Corona-Special
- Digitalisierung
  - Mobiles Arbeiten
  - IoT
  - Sicherheitsrisiken etc.
- Joint Controller-Verträge
  - Konzernvertrag
  - Auftragsverarbeitung
- Auskunfts-/Löschanspruch richtig abwickeln
- Löschkonzept gestalten, E-Mail-Archivierung
- Incidents und Datenschutzvorfälle – richtig reagieren
- IT-Sicherheitskonzept
  - Verschlüsselungspflichten
  - SIEM-Lösungen
- Soziale Netze (Facebook, WhatsApp usw.)
  - Tracking, Cookies
- IT-Nutzungsrichtlinien für WLAN und mobile Geräte
- Beschäftigtenkontrolle
  - Private Nutzung, Geschäftsgeheimnisgesetz
- Richtlinien, Dokumentation von IT-Sicherheit, Betriebsvereinbarungen
- Bußgeldpraxis der DSGVO – das neue Sanktionssystem
- Haftungsrisiken für IT-Verantwortliche
  - Vermeidungsstrategie

Techn. Voraussetzungen: Grundkenntnisse und gute Allgemeinbildung im Bereich IT
Termine: 26.04.2022 / 26.09.2022 (1 Tag)
Preis: € 750,00

SECU5: PLANUNG UND DURCHFÜHRUNG VON PENETRATIONSTESTS

Leitung: Sebastian Schreiber

Eine unsichere IT-Landschaft kann den Betrieb oder sogar den Fortbestand von Unternehmen erheblich gefährden. Meist reißen kleine, unscheinbare Fehler gefährliche Löcher in IT-Netze. Voraussetzung für die Behebung dieser Fehler ist es, die Lücken zu identifizieren. IT-Infrastrukturen und Applikationen können hochwertig und robust konzipiert sein und dennoch Schwachstellen aufweisen. Um diesen auf die Spur zu kommen, eignet sich der Penetrationstest hervorragend als Kontrollinstrument. Denn nur auf diese Weise können IT-Netze von außen und innen effektiv auf Sicherheitslücken hin untersucht werden. Die Durchführung solcher simulierter Hacker-attacken ist aber alles andere als einfach und wird im Workshop diskutiert.

Themen

- Der Penetrationstest
  - Warum Penetrationstests?
    » Definition/Motivation/Besonderheiten
  - Ethische Aspekte
  - Penetrationstests im Licht des neuen IT-Sicherheitsgesetzes
  - Neueste Trends/Penetrationstests der Zukunft
- Angriffsszenarien und Gestaltungs-möglichkeiten
  - Prüfgegenstand (Perimeter, LAN, WLAN, Webapplikation etc.)
  - Einmalig oder kontinuierlich?
  - Blackbox- oder Whitebox-Test?
  - Aggressiv oder vorsichtig?
- 80/20: Der Pentest-Servicekatalog
- Red Teaming/TIBER-DE
- Steuerung von Penetrationstestserien
  - Projektmanagement: PPMO
  - Kosten-/Nutzenverhältnis und Budgetoptimierung
  - Metriken und Standards
  - Umfang der Serien: vier Tests pro Jahr oder mehr?
  - Anlassbezogene/turnusmäßige Tests
  - Agile Umgebungen
  - Testtiefe/Testfrequenz
  - Sourcing: Anzahl/Strategie/Benchmarking
- Reporting
  - Ticketsysteme
  - Metrik
  - Projektübergreifendes Reporting
- Schwachstellenmanagement/Re-Tests
- 10 praktische Tipps von Sebastian Schreiber

Termine: 07.02.2022 / 20.06.2022 / 19.09.2022 (1 Tag)
Preis: € 750,00

SECU6: IT-SICHERHEIT KENNENLERNEN

Leitung: Diese Schulung wird von wechselnden SySS-Consultants gehalten

In unserer schnelllebigen und von IT stark abhängigen Zeit hat der sichere Umgang mit Informationstechnologie einen sehr hohen Stellenwert. Um Mitarbeitenden einen schnellen und direkten Einstieg in die wichtigsten Themen der IT-Sicherheit zu geben, hat die SySS den dreistündigen Kurs „IT-Sicherheit kennenlernen" konzipiert. Dieser richtet sich insbesondere an Mitarbeitende aus nicht technischen Bereichen und vermittelt Grundlagen der IT-Sicherheit und der digitalen Selbstverteidigung. Die Teilnehmenden absolvieren das Training je nach den aktuellen Begebenheiten vor Ort an unserem Hauptsitz in Tübingen, bequem per Videokonferenz aus dem Homeoffice oder von jedem anderen Ort mit Internetzugang. Sie lernen während des Workshops, wie sie ihre Arbeit im Homeoffice, aber auch im Büro so gestalten können, dass IT-Sicherheitskriterien eingehalten werden.

Bei der Durchführung der Schulung „IT-Sicherheit kennenlernen" per Videokonferenz nutzt die SySS das Videokonferenzsystem Zoom. Weitere Informationen zur Online-Durchführung unserer Schulungen erhalten Sie auf S. 25 oder im Bereich „Schulungen" auf unserer Homepage unter www.syss.de/leistungen/schulung.

Themen

- Sicherer Umgang mit Passwörtern
- Schutz vor Lauschangriffen (Sniffing)
- Phishing: Geschäftsmodell, Erkennung, Schutz
- Social Engineering
- Softwareupdates
- Schadsoftware (Malware): Demo und Schutz
- Melden von Vorfällen
- Security Best Practices im Homeoffice

Alle Themen beziehen sich gleichermaßen auf die Arbeit aus dem Homeoffice wie auch am regulären Arbeitsplatz.

Dauer: 3 Stunden
Die aktuellen Termine können jederzeit auf www.syss.de/leistungen/schulung abgerufen werden.
Preis: € 99,00

SECU7: PHISHING AWARENESS

Leitung: Kevin Möllering, Christoph Ritter

Phishing-E-Mails sind sowohl im beruflichen als auch im privaten Umfeld tägliche Begleiter geworden. Viele davon scheinen auf den ersten Blick harmlos zu sein, und oft herrscht auch die Meinung vor, gut gemachte Phishing-E-Mails erkenne man nicht. Der Workshop „Phishing Awareness" behandelt diese Problematik anschaulich anhand von Praxisbeispielen sowie einer Live-Demo, in der im Microsoft Outlook-Client gezeigt wird, wie sich unterschiedliche Varianten von Phishing-Mails und deren Anhänge auswirken können. Die Schulung wird durch das eigene Red Team der SySS gehalten, das auf fünf Jahre praktische Erfahrung in der Durchführung von Phishing und Spear Phishing zurückblicken kann.

Die Schulung richtet sich sowohl an Einsteigende in die Thematik als auch IT-affine Personen. Die Teilnehmenden lernen anhand von Fallbeispielen, an welchen typischen Merkmalen Phishing-Mails zu erkennen sind und wie sie sich verhalten müssen, wenn sie eine solche Mail bekommen. Bei der Durchführung der Schulung „Phishing Awareness" per Videokonferenz nutzt die SySS das Videokonferenzsystem Zoom. Weitere Informationen zur Online-Durchführung unserer Schulungen erhalten Sie auf S. 25 oder im Bereich „Schulungen" auf unserer Homepage unter www.syss.de/leistungen/schulung.

Themen

- Vorstellung der verschiedenen Phishing-Varianten
- Erkennungsmerkmale: Worauf ist zu achten?
- Live-Demo
- Beispiele aus der jüngsten Vergangenheit
- Richtiger Umgang mit einem Phishing-Vorfall
- Zusätzliche Sicherheitsmaßnahmen (Smishing, Vishing)

Die Themen umfassen sowohl die typischen Phishing-Erkennungsmerkmale als auch eine Live-Demo mit unterschiedlichen typischen Varianten von Malware im Anhang.

Dauer: 1 Stunde
Die aktuellen Termine können jederzeit auf www.syss.de/leistungen/schulung abgerufen werden.
Preis: € 59,00

ANMELDUNG 2022

Hack1: Hacking Workshop 1	☐ 18.-19.01.	☐ 22.-23.03.	☐ 10.-11.05.	☐ 12.-13.07.	☐ 27.-28.09.
Hack2: Hacking Workshop 2	☐ 20.-21.01.	☐ 24.-25.03.	☐ 12.-13.05.	☐ 14.-15.07.	☐ 29.-30.09.
Hack3: Angriffe auf Windows-basierte Netzwerke	☐ 22.-24.02.	☐ 21.-23.06.	☐ 13.-15.09.	☐ 06.-08.12.	
Hack4: Angriffe gegen VoIP-Infrastrukturen	☐ 14.-15.03.	☐ 07.-08.11.			
Hack5: Exploit Development	☐ 07.-08.03.	☐ 04.-05.07.			
Hack6: Mobile Device Hacking	☐ 31.01.-01.02.	☐ 02.-03.05.	☐ 10.-11.10.		
Hack7: Sicherheit und Einfallstore bei Webapplikationen	☐ 08.-09.02.	☐ 24.-25.05.	☐ 19.-20.07.	☐ 20.-21.09.	
Hack8: WLAN Hacking und WLAN Security	☐ 01.-02.03.	☐ 26.-27.07.			
Hack9: Embedded Security	☐ 11.-13.04.	☐ 17.-19.10.			
Secu1: Digitale Forensik bei Computern und Smartphones	☐ 04.-06.04.	☐ 28.-30.11.			
Secu2: Incident Response	☐ 14.-16.02.	☐ 24.-26.10.			
Secu3: IPv6 Security	☐ 29.03.	☐ 14.11.			
Secu4: IT-Recht und Datenschutz für IT-Verantwortliche	☐ 26.04.	☐ 26.09.			
Secu5: Planung und Durchführung von Penetrationstests	☐ 07.02.	☐ 20.06.	☐ 19.09.		

Die Termine von Secu6 und Secu7 können jederzeit auf www.syss.de/leistungen/schulung abgerufen werden.

Die Workshops finden entweder in Tübingen vor Ort oder über das Videokonferenzsystem Zoom statt. Mit Ausnahme der Schulungen Hack9, Secu6 und Secu7 setzen sich die Preise der jeweiligen Workshops aus der Anzahl der Workshoptage mal Tagespreis von € 750,00 zzgl. MwSt. zusammen. Im Preis enthalten sind eine ausführliche Schulung, eine professionelle Leitung, komplettes Equipment und Verpflegung, wenn vor Ort. Bei einer Buchung von 5 oder mehr Schulungstagen gewähren wir Ihnen einen einmaligen Rabatt in Höhe von 10 % auf das gebuchte Kontingent, egal ob Sie als Einzelperson mehrere Kursmodule besuchen oder sich zu mehreren zu einem Kurs anmelden. Bei Fragen hierzu stehen wir Ihnen jederzeit zur Verfügung.

Bitte senden Sie Ihre Anmeldung per Fax, E-Mail oder Post an uns zurück:
SySS GmbH, Schaffhausenstraße 77, 72072 Tübingen, Fax: +49 (0)7071 - 40 78 56-19, E-Mail: schulung@syss.de

Name

Firma

Straße

PLZ, Ort

E-Mail

Rechnungsadresse (wenn abweichend)

Telefon

Umsatzsteuernummer
(falls Firmensitz des Auftraggebers außerhalb Deutschlands)

Fax

Sonstiges

☐ Ich benötige einen Parkplatz

Ich akzeptiere die umseitigen Teilnahmebedingungen

Datum

Unterschrift

TEILNAHMEBEDINGUNGEN HACK1-9 UND SECU1-5

1. Bitte beachten Sie das VERBOT DER WEITERGABE VON HACKERTOOLS. Der Auftraggeber verpflichtet sich, Codes und Software, die z. H. seiner Mitarbeitenden von der SySS GmbH zugänglich gemacht werden, nur zur Sicherung seiner eigenen Betriebssysteme einzusetzen; die Bestimmungen der §§ 202 a-c StGB sind ihm bekannt (siehe S. 25).
2. Eine kostenfreie Stornierung (nur schriftlich) ist 4 Wochen vor Schulungsbeginn möglich. Bei Stornierungen 2 Wochen vor Schulungsbeginn fallen 50 % der Gebühr zzgl. MwSt. an, danach die volle Gebühr. Bei Rücktritt ist die Benennung einer Ersatzperson ohne Zusatzkosten möglich.
3. Die SySS GmbH behält sich vor, die Schulung bei einer zu niedrigen Anmeldezahl bis 10 Tage vor Schulungsbeginn kostenfrei abzusagen.
4. Der Rechnungsbetrag ist ohne Abzüge innerhalb von 14 Tagen nach Rechnungsdatum zahlbar; es gelten unsere AGB.

SECU6 UND SECU7

1. Der Preis pro teilnehmender Person für die 3-stündige Schulung „IT-Sicherheit kennenlernen“ beträgt € 99,00, für die 1-stündige Schulung „Phishing Awareness“ € 59,00 zzgl. MwSt. Bei einer Buchung für 5 oder mehr Teilnehmende gewähren wir Ihnen einen einmaligen Rabatt in Höhe von 10 % auf das gebuchte Kontingent, egal ob Sie als Einzelperson mehrere Kursmodule besuchen oder sich zu mehreren zu einem Kurs anmelden.
2. Der Kunde kann die Buchung bis 14 Kalendertage vor Schulungsbeginn stornieren, ohne dass Kosten entstehen. Bei einer Stornierung zwischen 14 und 7 Kalendertagen vorher berechnen wir 50 %, bei noch kurzfristigerer Stornierung den vollen Schulungspreis. Bei Rücktritt ist die Benennung einer Ersatzperson für die Teilnahme ohne Zusatzkosten möglich.
3. Die SySS GmbH behält sich vor, die Workshops bei einer niedrigen Anmeldezahl spätestens 3 Tage vor Beginn abzusagen.
4. Der Rechnungsbetrag ist ohne Abzüge innerhalb von 14 Tagen nach Rechnungsdatum zahlbar; es gelten unsere AGB.

ONLINE-DURCHFÜHRUNG VON SCHULUNGEN

Wenn Schulungen und Workshops nicht vor Ort durchgeführt werden, geschieht dies über das Videokonferenzsystem Zoom. Die Teilnehmenden erhalten vorab einen Link und können mit einem aktuellen Browser die Schulung besuchen. Alternativ kann der Zugang über den Zoom-Client auf dem Computer oder dem Smart Device erfolgen. Eine telefonische Einwahl ist ebenfalls möglich, auch zusätzlich, um die Sprachverbindung getrennt abzuwickeln. Nach Abschluss des Workshops erhalten die Absolvierenden einen Foliensatz mit den erarbeiteten Inhalten sowie eine Teilnahmebestätigung.

Für Rückfragen zum Ablauf oder zur Organisation der Schulungen sind wir jederzeit über schulung@syss.de für Sie erreichbar.

GESETZESTEXT ZU DEN SOGENANNTEN „HACKERTOOLS“

§ 202a Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§ 202b Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

§ 202c Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

a. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§202a Abs. 2) ermöglichen, oder

b. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.


SYSS
THE PENTEST EXPERTS.


SCHULUNG
TRAINING FÜR MEHR SICHERHEIT

THE PENTEST EXPERTS

WWW.SYSS.DE

SySS GmbH Tübingen Germany +49 (0)7071 - 40 78 56-0 schulung@syss.de