THE PENTEST EXPERTS

WWW.SYSS.DE

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

THE PENTEST EXPERTS.

HACKING & SECURITY 2017

SICHERHEIT TRAINIEREN – KOMPETENZEN AUSBAUEN

SEBASTIAN SCHREIBER
GESCHÄFTSFÜHRER

EIN WORT VORWEG

Auch für das Jahr 2017 steht unser Schulungsprogramm unter der Überschrift „Hacking & Security". Hackerangriffe gehören derzeit zu den größten Gefahren für die IT-Sicherheit in Unternehmen. Umso wichtiger ist es für IT-Verantwortliche, sich mit den Grundlagen des Hacking zu beschäftigen. Denn wer seinen Gegner und dessen digitale Angriffsmittel kennt, kann sich gezielter zur Wehr setzen.

Im breit gefächerten Schulungs-Portfolio der SySS GmbH vermitteln Ihnen erfahrene IT-Security Consultants das entsprechende Know-how und Handwerkszeug. Die stetige Verbesserung Ihrer IT-Security ist und bleibt das Hauptziel der Pentest Experts von SySS. Dazu gehört aus unserer Sicht – neben der regelmäßigen Durchführung von Penetrationstests – vor allem auch die Sensibilisierung und Qualifizierung all jener in Ihrem Unternehmen, die IT mitverantworten. Mit unseren Schulungen möchten wir hierzu einen Beitrag leisten und unser Know-how mit Ihnen teilen.

Diese Broschüre enthält die Beschreibungen aller unserer Schulungen. Auch außerhalb der aufgeführten Termine können Sie unsere Fortbildungen buchen, gerne exklusiv für Ihre Mitarbeiter in Ihrem Unternehmen. Auf Wunsch bieten wir alle Schulungen auch in englischer Sprache an.

Mein Team und ich freuen uns auf Ihre Anmeldung, damit Sie Sicherheit trainieren und Kompetenzen ausbauen können.

Herzliche Grüße, Ihr Sebastian Schreiber

P.S.: Profitieren Sie auch von unseren Newslettern „The Pentest News" und „The Pentest Advice", 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 mit mittlerweile rund 80 festangestellten Mitarbeitern hochwertige Sicherheitstests durch. Bei unserer Arbeit verbinden wir einen sehr hohen technischen Anspruch mit der von uns entwickelten Ethik für Penetrationstester.

INHALT

HACK1/HACK2: HACKING WORKSHOP TEIL 1 & 2

Referenten: Rainer Boie, 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 ernstzunehmende Bedrohung. Damit Unternehmen ihre IT-Umgebung vor Gefahren dieser Art besser schützen können, haben wir die Workshops Hack1 und Hack2 entwickelt. In ihnen betrachten wir das Thema IT-Sicherheit aus der Perspektive eines Täters bzw. „Hackers", die wiederum dabei helfen kann, Netzwerke im eigenen Verantwortungsbereich besser abzusichern. Beide Teile 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 Verkehr 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 von verschiedenen Cracking-Techniken schätzen wir die Sicherheit ein, die eine Passwortrichtlinie bietet.
- Sicherheitslücken im Netz
  - Vorgehensweise eines Angreifers bei der Ausnutzung von Schwachstellen im Netz (Verwendung von Exploits, Trojanisierung des Zielsystems)

WORKSHOP 1
Techn. Voraussetzungen: Grundkenntnisse über Betriebssysteme, Netzwerke, Linux, Windows, TCP/IP
Termine: 07.-08.02.2017 / 04.-05.04.2017 / 20.-21.06.2017 / 19.-20.09.2017 / 21.-22.11.2017 (2 Tage)

WORKSHOP 2
Techn. Voraussetzungen: Grundkenntnisse über Betriebssysteme, Netzwerke, Linux, Windows, TCP/IP
Termine: 09.-10.02.2017 / 06.-07.04.2017 / 22.-23.06.2017 / 21.-22.09.2017 / 23.-24.11.2017 (2 Tage)

WORKSHOP 2

Themen

- Metasploit Framework
  - Einführung und Umgang mit unterschiedlichen Modulen
- Sicherheit in Windows-Netzen
  - Eskalation von Benutzerrechten zum Domainadministrator, Umgang mit Windows-Tokens
- Security-Scanner
  - Funktionsweise, Konfiguration und Umgang mit einem Security-Scanner
- Tunneling
  - Verwendung harmloser Protokolle zur verdeckten Übertragung von Daten oder Remotezugriff von außen
- Exkurs: Sicherheit von Webapplikationen
  - Das am besten gesicherte Betriebssystem kann nicht helfen, wenn eine Anwendung unsicher betrieben wird. Behandelt werden die häufigsten Sicherheitslücken wie XSS, Command Injection und SQL Injection.

HACK3: ANGRIFFE AUF WINDOWS-BASIERTE NETZWERKE

Referenten: Sven Wiebusch, Wolfgang Zejda

Zur technischen Organisation von Computern, Benutzern, 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 einem Angreifer, initial von außen in das interne Netzwerk einzudringen, so kann er innerhalb dieses Verzeichnisdienstes seine Rechte meist mit überschaubarem Aufwand ausweiten. In dieser Schulung soll ein tieferer Einblick in die Vorgehensweise von Angreifern gewährt und Gegenmaßnahmen aufgezeigt werden. Theoretische Konzepte werden erläutert und Angriffsvektoren anhand von „Hands On"-Übungen praktisch erprobt.

Themen

- Windows-basierte Netzwerke
  - Active Directory, Domain Controller
  - Struktur- und Trust-Ermittlung einer Active Directory-Umgebung
  - Berechtigungs- und Authentifizierungskonzepte
  - Hash-Typen in der Microsoft-Welt
  - Windows-Anmeldeprozess
- 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 Tokens und „gecachte" Passwörter
  - Pass-the-Hash-Angriffe
  - Security Support Provider
  - Group Policy Objects/Preferences
- Einsatz geeigneter Tools
  - Metasploit Framework
  - Portscanner wie Nmap
  - Powershell-Tools wie Empire
  - Cracking-Tools
  - Tools für spezielle Einsatzzwecke
- „Best Practice"-Schutzmaßnahmen
  - Detektionsverfahren
  - IT-Security-Prinzipien
  - Konfigurationsempfehlungen

Techn. Voraussetzungen: Grundkenntnisse von Linux- und Windows-basierten Systemen und Netzen
Termine: 28.-30.03.2017 / 16.-18.05.2017
26.-28.09.2017 / 14.-16.11.2017 (3 Tage)

HACK4: ANGRIFFE GEGEN VOIP-INFRASTRUKTUREN

Referenten: Sven Freund, Ludwig Stage

Das Protokoll VoIP ist in den letzten Jahren für Unternehmen nicht zuletzt aufgrund langfristiger Kosteneinsparung oder einer einheitlichen Infrastrukturnutzung immer mehr in den Vordergrund gerückt. Mit der Einführung von VoIP beginnt oder erweitert sich auch der Wunsch nach einer strikten Trennung bestimmter Daten im Netzwerk. Diese Trennung wird in der Regel nicht physikalisch, sondern auf logischer Ebene via VLANs erreicht. Gelingt es einem Angreifer beispielsweise, im internen Netzwerk auf andere VLANs zuzugreifen, so ist er eventuell in der Lage, vertrauliche Gesprächsverbindungen mitzuschneiden oder die eigenen Zugriffsberechtigungen zu erweitern.

Im Rahmen eines zweitägigen Workshops wird die Perspektive eines Angreifers eingenommen. Es werden Verfahren gezeigt, mit denen die oben genannten Ziele erreicht werden können. Der Workshop soll tiefere Einblicke in die Vorgehensweise von Angreifern aufzeigen, damit Teilnehmer in der Nachbereitung die Risiken im eigenen Netzwerk minimieren können. Theoretische Konzepte werden erläutert und erlernte Angriffsvektoren anhand von „Hands On"-Übungen praktisch erprobt.

Themen

- Technische Grundlagen
  - Einführung in die Techniken
  - VoIP-Terminologie und -Aufbau
  - Passive und aktive Trafficanalyse
  - VLAN-Terminologie und -Aufbau
- Angriffsverfahren
  - Netzbasierte Angriffe gegen VoIP-Phones und -Anlagen
  - Angriffe gegen Authentisierungsverfahren
  - Angriffe gegen die Vertraulichkeit von Daten
  - Bootangriffe und weitere physische Trunking-Angriffe
  - Inter-VLAN-Routing
- Schutzmaßnahmen
  - Erkennungsmöglichkeiten
  - IT-Sicherheitsprinzipien
  - Konfigurationsempfehlung

Techn. Voraussetzungen: Grundkenntnisse in Netzwerktechnik
Termine: 01.-02.03.2017 / 17.-18.10.2017 (2 Tage)

HACK5: EXPLOIT DEVELOPMENT

Referenten: Matthias Deeg, Daniel Schalberger

Diese Schulung vermittelt die theoretischen und praktischen Grundlagen für die Funktionsweise und die 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 noch auf die Frage ein, welche Möglichkeiten existieren, sich gegen eine Ausnutzung der gezeigten Schwachstellen durch Angreifer 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.)
- Ausnutzen verschiedener Schwachstellentypen
  - Fehler in der Hard- und Softwarearchitektur und Anwendungslogik
  - Fehler in der Datenverarbeitung, z. B.
    - » Buffer Overflow-Schwachstellen (Stack, Heap, Off-By-One)
    - » Format String-Schwachstellen
- Schutzmaßnahmen und Möglichkeiten, diese zu umgehen
  - Stack Cookies
  - SafeSEH
  - Data Execution Prevention (DEP)
  - Address Space Layout Randomization (ASLR)

Techn. Voraussetzungen: Grundkenntnisse über Betriebssysteme und Rechnerarchitektur
Termine: 30.-31.05.2017 / 28.-29.11.2017 (2 Tage)

HACK6: MOBILE DEVICE HACKING

Referenten: Philipp Buchegger, Roman Stühler

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 Arbeitnehmer auf ihren Smartphones und iOS-Geräten E-Mails bearbeiten, ins Internet gehen und eine hohe Menge an oftmals vertraulichen Unternehmensdaten bewegen. Diese Konzentration an interessanten Daten machen Mobile Devices für Angreifer sehr attraktiv.

Dieses Seminar richtet sich an Nutzer, die mobile Endgeräte mit dem Fokus auf deren Sicherheit besser verstehen wollen, beispielsweise für die Integration in die eigene Unternehmensinfrastruktur. Neben der Verwaltung der Geräte werden die kritischen Angriffspunkte beleuchtet. Ferner werden durch „Hands On"-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 Zertifikatpinning
  - Angriffe bzgl. Services, Content-Provider, etc.
  - Reverse Engineering von Apps
  - Laufzeitmanipulation
- Windows Phone
  - Ausnutzung aktueller Schwachstellen
  - Sicherheitskonzept und Schutzmechanismen

Techn. Voraussetzungen: Grundlagen in Linux
Termine: 14.-15.03.2017 / 11.-12.07.2017 / 05.-06.10.2017 (2 Tage)

HACK7: SICHERHEIT UND EINFALLSTORE BEI WEBAPPLIKATIONEN

Referenten: Torsten Lutz, Marcel Mangold

Für Hacker sind Webapplikationen heutzutage das Einfallstor Nummer 1. Oftmals finden sie Schwachstellen, die es ihnen ermöglichen, vertrauliche Daten zu entwenden und weiter in das System bis hin zum Unternehmensnetzwerk vorzudringen.
Im Rahmen dieses zweitägigen Workshops lernen die Teilnehmer, wie Hacker in Webapplikationen einbrechen und welchen Risiken Anwendungen ausgesetzt sein können. Die Schulung stellt die gängigsten Angriffe zunächst in der Theorie dar und geht anschließend mit Übungen darauf ein, wie sie in der Praxis umgesetzt werden können. Ziel ist es, dass die Teilnehmer 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)
  - Wie Angreifer Applikationsnutzer dazu bringen, das zu tun, was sie wollen
- (Blind) SQL Injection
  - Unberechtigtes Auslesen von Daten aus einer Datenbank
- OS Command Injection
  - Einschleusen von eigenen Betriebssystem-kommandos in eine Webapplikation
- Local/Remote File Inclusion (LFI/RFI)
  - Wie Hacker eigenen Programmcode auf dem angegriffenen Server ausführen können
- Session-Hijacking
  - Übernahme fremder Sitzungen mithilfe von Cross-Site Scripting-Angriffen
- Cookies
  - Was bei der Generierung und Verwendung von (Session-)Cookies zu beachten ist
- HTTP Parameter Pollution (HPP)
  - Mehrfachverwendung von Parametern zur Zugriffsumgehung

Techn. Voraussetzungen: Grundkenntnisse in HTML, HTTP und SQL
Termine: 07.-08.03.2017 / 23.-24.05.2017 / 12.-13.09.2017 / 05.-06.12.2017 (2 Tage)

HACK8: WLAN-HACKING UND WLAN-SECURITY

Referenten: Gerhard Klostermeier, Matthias Sattler

Wireless LAN ist eine äußerst attraktive Technologie. Sie ermöglicht einer Vielzahl von Devices 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 in gleicher Weise wächst auch die zur Verfügung stehende Bandbreite stetig an. Doch wie sicher ist WLAN? Geht die Entwicklung von WLAN und von entsprechenden Schutzmaßnahmen gegen Missbrauch Hand in Hand?

Themen

- Grundlagen der WLAN-Technologie
  - Standards
  - Begriffe
- Aufbau einer WLAN-Umgebung
  - Unter Linux (Adhoc, Infrastruktur)
- 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, 802.11i
- Authentifizierung in 802.11i
  - 802.1x, EAP, PSK
- Schlüsselmanagement in 802.11i
  - Schlüsselhierarchien
  - Handshakes
- Funktionsweise der Verschlüsselungsmechanismen
  - WEP
  - TKIP
  - CCMP
- WLAN-Hacking
  - DoS-Angriffe
  - WEP-Cracking
  - Angriffe gegen WPA/WPA2-PSK
  - Angriffe gegen WPS
  - Angriffe gegen WPA2-Enterprise
  - Angriffsmöglichkeiten gegen Captive Portals
  - Das Smartphone: Ein hilfreiches Werkzeug

Techn. Voraussetzungen: Grundkenntnisse in Netzwerktechnik
Termine: 25.-26.04.2017 / 24.-25.10.2017 (2 Tage)

SECU1: DIGITALE FORENSIK BEI COMPUTERN UND SMARTPHONES

Referent: 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 konform zu den BSI-Grundschutzkatalogen
- 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, BlackBerry, Windows Phone
  - Spezielle Werkzeuge für die Smartphone-Forensik
- Verfassen von gerichtskonformen Berichten
- Projektmanagement: IT-Forensik
  - Zusammenarbeit mit Strafverfolgungsbehörden, rechtliche Situation

Techn. Voraussetzungen: Grundkenntnisse über Netzwerke unter Windows, Linux oder Unix
Termine: 21.-23.02.2017 / 04.-06.07.2017 (3 Tage)

SECU2: INCIDENT RESPONSE

Referenten: Sebastian Nerz, Dr. Klaus Tichmann, Christian Schneider, Andreas Heideck

Alle Welt redet von „Cyberwar", Industriespionage und Datenklau. Werden Angriffe bemerkt, ist es wichtig, überlegt und organisiert zu handeln. Aus diesem Grund bieten wir einen Workshop an, der eine Handlungsgrundlage bieten soll, 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 (Meldeketten und Awareness)
  - 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
  - Forensische Untersuchungen vs. Triage: Abwägung individueller Analysemethoden
  - Identifikation des Angriffsvektors
- 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 Forensik- sowie Linux-Kenntnisse
Termine: 14.-16.02.2017 / 27.-29.06.2017 / 07.-09.11.2017 (3 Tage)

SECU3: INCIDENT DETECTION

Referent: Sebastian Nerz, Dr. Klaus Tichmann, Christian Schneider, Andreas Heideck

IT-Sicherheitsvorfälle lassen sich nicht final verhindern, ein entschlossener Angreifer mit genug Zeit wird Sicherheitsmaßnahmen überwinden oder über Social Engineering in ein Netzwerk eindringen können. Neben der präventiven IT-Sicherheit wird daher die zeitnahe und aktive Erkennung von Angriffen immer wichtiger. Dieser Workshop soll die Grundlagen einer kontinuierlichen Angriffserkennung bieten.

Themen

- Allgemeine Grundlagen
  - Aktueller Stand
  - Klassische Angriffsformen
  - Incident Response, Incident Readiness und Reaktion auf Angriffe
  - Anforderungen an ein sicherbares Netzwerk
- Netzwerkdokumentation und -erkennung
  - Inventarisierung des Netzwerks
  - Anforderungen an die Dokumentation
- Network Security Monitoring
  - Grundlagen der Netzwerke
  - IDS vs IPS vs SIEM vs Firewall …
  - Grundlagen der Netzwerkforensik
  - Anomalieerkennung
  - Long Tail Analysis
- Continuous Security Monitoring
  - Grundlegende Anforderungen
  - Monitoring auf Endpunkten
    - » Autostart/ASEP
    - » Logs
    - » Privileges
    - » Process Execution
  - Monitoring-Automatisierung
  - Long Tail Analysis

Techn. Voraussetzungen: Grundlegende Netzwerk- sowie Linux- und Windows-Kenntnisse
Termine: 09.-10.05.2017 / 12.-13.12.2017 (2 Tage)

SECU4: IPV6-SECURITY

Referent: Marcel Mangold

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

Themen

- Kurze Einführung in IPv6
  - Einführung in die Adressschemata und Hilfsprotokolle
- 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 Neighbour Discovery

Techn. Voraussetzungen: Grundkenntnisse zu IPv4
Termine: 12.05.17 / 08.12.17 (1 Tag)

SECU5: IT-RECHT UND DATENSCHUTZ FÜR IT-VERANTWORTLICHE

Referent: Horst Speichert

IT-Verantwortliche müssen täglich Entscheidungen treffen, ohne sich der rechtlichen Tragweite bewusst zu sein. Oft riskieren sie dabei Rechtsverstöße, Bußgelder oder stehen gar „mit einem Bein im Gefängnis". Allein in den letzten Monaten gab es eine wahre Flut neuer Gesetze und Urteile im IT-Recht und Datenschutz. Ein ausgereiftes Sicherheitskonzept besteht aus der erfolgreichen Synchronisation technischer und juristisch-organisatorischer Fragen. Das Seminar klärt über die aktuelle Rechtslage bei IT-Compliance, Informationssicherheit und Datenschutz auf, hilft kritische Situationen richtig einzuschätzen und zeigt Lösungswege auf. Der Referent ist Spezialist für IT-Recht und Datenschutz, Lehrbeauftragter für Informationsrecht an der Universität Stuttgart und Autor des Fachbuchs „Praxis des IT-Rechts".

Themen

- EU-Datenschutzverordnung
  - Was kommt auf Sie zu?
- Neues IT-Sicherheitsgesetz
  - BSI-KritisV, Implementierung ISMS
- EuGH kippt Safe-Harbor
  - Ersatzlösungen US-Datentransfer, Privacy Shield
- Cloud-Strategie
  - Globaler Datenverkehr, Datentreuhand
- Softwarelizenz-Audits
  - Wie bereiten Sie sich optimal vor?
  - Gebrauchtsoftware
- Neues W-LAN-Gesetz
  - Big Data, Industrie 4.0
- Neue GoBD
  - Archivierungspflichten
- Richtlinien + für IT-Sicherheit
- Haftungsrisiken für IT-Verantwortliche
  - Vermeidungsstrategie
- Richtlinien
  - Betriebsvereinbarungen für Dokumentation von IT-Sicherheit

Techn. Voraussetzungen: Grundkenntnisse und gute Allgemeinbildung im Bereich IT
Termine: 03.05.17 / 15.09.17 (1 Tag)

SECU6: PLANUNG UND DURCHFÜHRUNG VON PENETRATIONSTESTS

Referent: 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

- Warum Penetrationstests?
  - Gegenstand der Prüfungen (Perimeter, LAN, WLAN, Webapplikationen, Web-Services, Clients, iOS, Android, Spezialtests)
  - Penetrationstests im Licht des neuen IT-Sicherheitsgesetzes
- Gestaltungsmöglichkeiten
  - Angekündigt/unangekündigt?
  - Einmalig oder als Prozess?
  - Blackbox- oder Whitebox-Test?
  - Durch einen externen Experten oder intern? Sorgfältige Auswahl des Dienstleisters
  - Aggressive oder vorsichtige Vorgehensweise?
  - Tätermodelle und Angriffsszenarien
- Vorgehensweise; interne und externe Kommunikation zu Tests
- Kosten-/Nutzenverhältnis, Budgetoptimierung
- Projektmanagement
- Metriken und Standards
- Neueste Trends, Penetrationstests der Zukunft
- Rechtliche und ethische Aspekte
- Nachverfolgung von Schwachstellen
- Mehrperiodige Prüfpläne
- Penetrationstests als Instrument der Internen Revision
- Planung und Durchführung von Penetrationstests in Konzernstrukturen
- 10 praktische Tipps von Sebastian Schreiber

Termine: 10.03.2017 / 02.06.2017 / 27.10.2017 (1 Tag)

ANMELDUNG 2017

Hack1: Hacking Workshop 1	☐ 07.-08.02.	☐ 04.-05.04.	☐ 20.-21.06.	☐ 19.-20.09.	☐ 21.-22.11.
Hack2: Hacking Workshop 2	☐ 09.-10.02.	☐ 06.-07.04.	☐ 22.-23.06.	☐ 21.-22.09.	☐ 23.-24.11.
Hack3: Angriffe gegen Windows-basierte Netzwerke	☐ 28.-30.03.	☐ 16.-18.05.	☐ 26.-28.09.	☐ 14.-16.11.	
Hack4: Angriffe gegen VoIP-Infrastrukturen	☐ 01.-02.03.	☐ 17.-18.10.			
Hack5: Exploit-Development	☐ 30.-31.05.	☐ 28.-29.11.			
Hack6: Mobile Device Hacking	☐ 14.-15.03.	☐ 11.-12.07.	☐ 05.-06.10.		
Hack7: Sicherheit und Einfallstore bei Webapplikationen	☐ 07.-08.03.	☐ 23.-24.05.	☐ 12.-13.09.	☐ 05.-06.12.	
Hack8: WLAN-Hacking und WLAN-Security	☐ 25.-26.04.	☐ 24.-25.10.			
Secu1: Digitale Forensik bei Computern und Smartphones	☐ 21.-23.02.	☐ 04.-06.07.			
Secu2: Incident Response	☐ 14.-16.02.	☐ 27.-29.06.	☐ 07.-09.11.		
Secu3: Incident Detection	☐ 09.-10.05.	☐ 12.-13.12.			
Secu4: IPv6-Security	☐ 12.05.	☐ 08.12.			
Secu5: IT-Recht und Datenschutz für IT-Verantwortliche	☐ 03.05.	☐ 15.09.			
Secu6: Planung und Durchführung von Penetrationstests	☐ 10.03.	☐ 02.06.	☐ 27.10.		

Die Workshops finden in Tübingen statt. Einen Workshoptag bieten wir zum Preis von € 720,00 zzgl. MwSt. an. Der Preis umfasst eine ausführliche Schulung, professionelle Referenten, einen komplett eingerichteten Arbeitsplatz samt Notebook und die Verpflegung. Bei einer Buchung von 5 und mehr Schulungstagen gewähren wir Ihnen einen einmaligen Rabatt in Höhe von 10 % auf das gebuchte Kontingent. Für die Gewährung des Rabatts werden sowohl Schulungstage einzelner Teilnehmer für mehrere Kursmodule als auch Schulungstage mehrerer Teilnehmer für einzelne Kurse addiert. 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, Wohlboldstraße 8, 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 Deutschland)

Fax

Sonstiges

Ich akzeptiere die umseitigen Teilnahmebedingungen

Datum

Unterschrift

TEILNAHMEBEDINGUNGEN

1. Bitte beachten Sie das VERBOT DER WEITERGABE VON HACKERTOOLS.
   Der Auftraggeber verpflichtet sich, Codes und Software, die z. H. ihrer Mitarbeiter von der SySS GmbH zugänglich gemacht werden, nur zur Sicherung ihrer eigenen Betriebssysteme einzusetzen; die Bestimmungen der §§ 202 a-c StGB sind ihm bekannt (siehe Anlage).
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 eines Ersatzteilnehmers ohne Zusatzkosten möglich.
3. Die SySS GmbH behält sich vor, die Schulung bei einer zu geringen Teilnehmerzahl bis 10 Tage vor Schulungsbeginn kostenfrei abzusagen.
4. Der Rechnungsbetrag ist ohne Abzüge innerhalb von 14 Tagen nach Rechnungsdatum zahlbar; es gelten unsere AGB.

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 einem Jahr oder mit Geldstrafe bestraft.

SCHULUNG

TRAININGS ZU MEHR SICHERHEIT