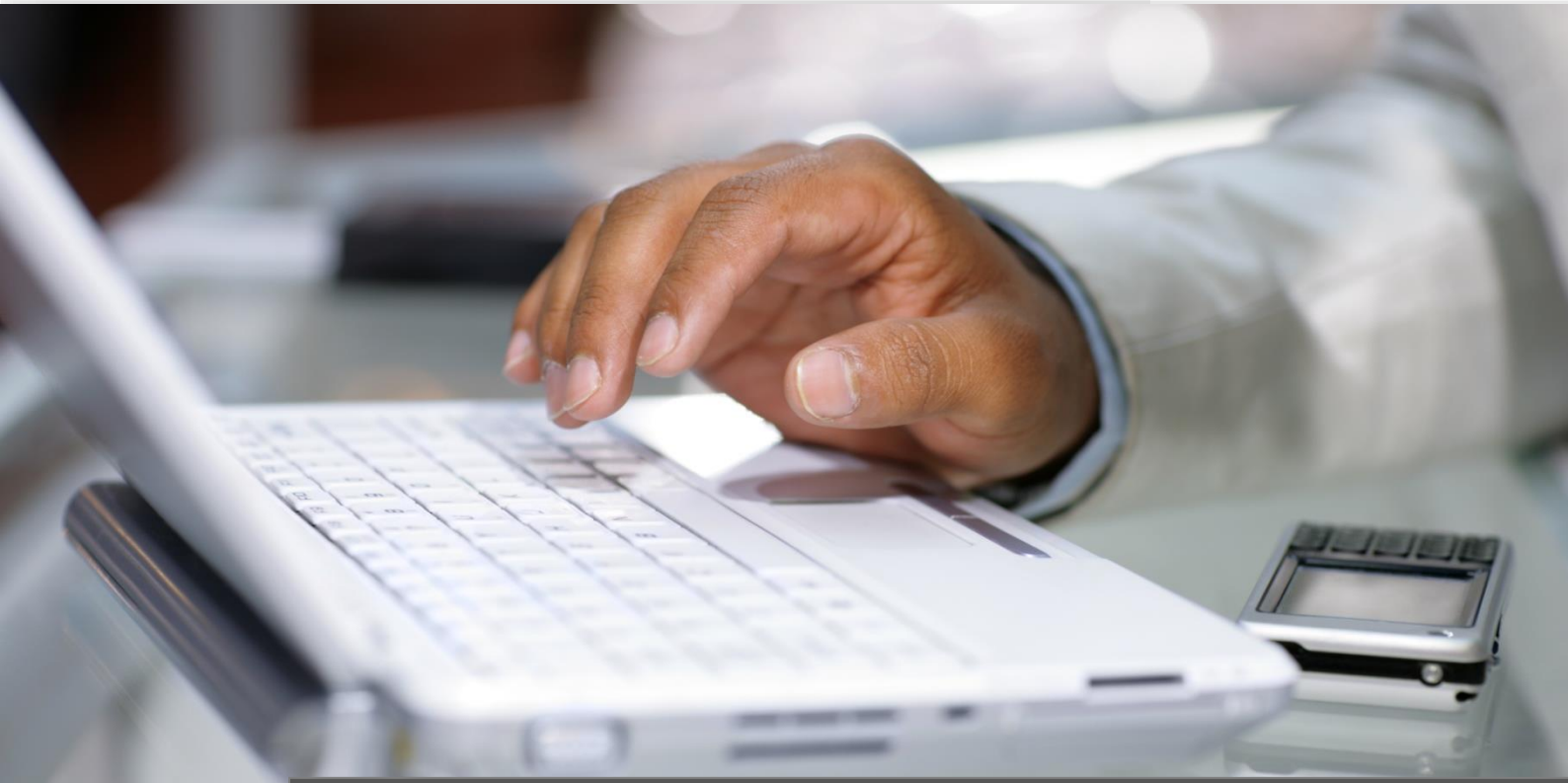
ITKwebcollege.Security

Advanced Trainings

Online-Trainings für Security-Consultants oder Security-Experten | Stand Januar 2019



Ausbildungsinhalte

ITKservice

Inhaltsverzeichnis

Security Advanced Trainings

Analyse von Logfiles und SIEM

	Unterrichtseinheit	UE 01	SAD
	Analyse von Logfiles und SIEM ✓ Bedarfsanalyse ▪ Beispiel: Website ✓ Kritikalität ▪ Beispiel: Website ✓ Mindestanforderungen ▪ Beispiel: Website ✓ Zählen reicht nicht aus? ✓ Automatismen schaffen ✓ Schnelles Security Monitoring mit OMD ✓ OMD CheckMK ▪ Installation und Einsatz ▪ Maßgeschneidert ✓ Logfile Analyse durch SIEM und Co ✓ Harte Fakten ✓ Dienstleistung & Services		

Backdoors, Angriffsmethoden und Erkennung

	Unterrichtseinheit	UE 01	SAD
	Backdoors, Angriffsmethoden und Erkennung ✓ Backdoor ▪ Funktionsweise ▪ Implementierung ✓ Häufige Backdoor/Angriff: DRIDEX ✓ Analyse von DRIDEX im Detail ✓ Tools zur Erkennung von Backdoors ✓ TCPView zur Prozessanalyse ✓ Alternative zur AV Erkennung: CyLance ✓ Erkennung über NSM Systeme ✓ Analyse per NSM ✓ Analyse per Network Flow Auswertung ✓ Kampf gegen Backdoors		

E-Mail Spoofing & Spearphishing

	Unterrichtseinheit	UE 01	SAD
	Spearphishing Angriffe per E-Mail ✓ Beispiel ✓ Wie Angreifer professionelle E-Mails erzeugen ✓ Professionelle E-Mails mit Atomic Studio ✓ Stichwort: Proxy Server ✓ Verifikation von E-Mail Adressen ✓ Erstellen von professionellen E-Mails		

Emotet is back

Unterrichtseinheit	UE 01	SAD

Emotet is back
- ✓ Bit Paymer
  - 2017
  - 2018
- ✓ Angriffsrekonstruktion
- ✓ TRICKBOT
  - Kommunikation
  - Hits
- ✓ Emotet vs. AV
- ✓ Ziel des Angreifers
- ✓ Angriff früh erkennen
- ✓ Problematik
  - NSM – Port Mirroring
- ✓ Blocklisten

Empire Framework & Deathstar

Unterrichtseinheit	UE 01	SAD

Empire Framework & Deathstar
- ✓ Auszug Manila Hacking Days 2018
- ✓ Empire Framework
  - Überblick
- ✓ Domain Security in a Nutshell
- ✓ UAC-Bypass: Klassisches Szenario
- ✓ Memory Access ist kritisch?
- ✓ Ideale Lösung: Microsoft LAPS
- ✓ Und der Domain Administrator?
- ✓ Vorsicht bei Server Admin Accounts
- ✓ Deathstar spart Zeit: Angriff los!
- ✓ Testszenario
- ✓ Fazit: Deathstar/Empire testen

Erpressungstrojaner oder Kryptotrojaner (Ransomware)

Unterrichtseinheit	UE 01	SAD

Ransomware
- ✓ Funktionsweise und Abwehr
- ✓ Erscheinung der Neuzeit?
- ✓ Wer ist betroffen?
- ✓ Sollte man zahlen?
- ✓ Wieso erwischt man die nicht?
- ✓ Infektionswege?
- ✓ E-Mail Infektion
- ✓ E-Mail Payload
- ✓ Webbrowser Angriffe
- ✓ Welche Exploits stecken drin
- ✓ Netzwerkanalyse Locky
- ✓ Wie funktioniert Locky?
- ✓ Welche Dateien greift Locky an?
- ✓ Abwehrmaßnahmen

Ransomware 2.0
- ✓ Was kommt auf uns zu?

Früherkennung von Cyberangriffe

Unterrichtseinheit	UE 01	SAD

Früherkennung von Cyberangriffen
- ✓ Erkennen Sie Angriffe rechtzeitig oder erst nach dem Datenabfluss?
- ✓ Ausprägung von Cyberangriffen
- ✓ Scanning der Unternehmensnetzwerke
- ✓ Effiziente Erkennung
  - Log File Analyse/SIEM
  - Network Security Monitoring

Hacker's Diary - Dedicated Malware Attack

Unterrichtseinheit	UE 01	SAD

Gezielte Malware-Angriffe gegen Unternehmen
Information Gathering
Livedemo
- ✓ Angriffsmethode finden
- ✓ Dark Net Analyse der Ziele
- ✓ Informationssammlung
- ✓ Malware als Baukasten
- ✓ Dark Services
- ✓ Auslieferung der Malware

Gegenmaßnahmen

Hacker's Diary - Unerkannt bleiben

Unterrichtseinheit	UE 01	SAD

Überblick: Methoden zur Tarnung
- ✓ Anonyme Netzwerke
  - Öffentliche Zugänge
  - Erkennungsmerkmale
    - MAC Adressen tarnen
    - Videoüberwachung in Deutschland
    - Augenzeugen
  - Hidden Services
    - Proxy Server
    - VPN Anbieter
  - Anonyme Betriebssysteme
  - Spezial: TOR-KALI-Master Unit

Hacking und IT-Security

Unterrichtseinheit	UE 01	SAD

Aktuelle Angriffsszenarien
- ✓ Angriffe im Überblick
  - Kryptotrojaner (Ransomware)
  - SEO Fraud
  - Zielgerichtete Attacken
- ✓ Dienstleistungen im Überblick
  - Penetrationtesting
  - Forensische Analysen
  - NSM Analysen

Ransomware
- ✓ Ransomware 2016
- ✓ Ransomware in Zahlen
- ✓ Sofortmaßnahmen
- ✓ Sofortmaßnahmen/Kalkulation
- ✓ Prophylaxe

SEO Fraud
- ✓ SEO Fraud 2016
- ✓ Blind Phishing Angriffe
- ✓ E-Mail Interception Angriffe
- ✓ E-Mail/Telefon Angriffe
- ✓ Gegenmaßnahmen

Zielgerichtete Attacken
- ✓ Sofortmaßnahme

Dienstleistungen im Überblick

IDS-System: Wirksamer Schutz?

Unterrichtseinheit	UE 01	SAD

IDS-System
- ✓ Rollout der Ransomware
- ✓ Neue Infektion
- ✓ Funktionsweise
- ✓ Snort
  - Historie
- ✓ Subscription Rulesets
  - Überblick
  - Vorteile
- ✓ Emerging Thread (ET)
  - Open Rulesets
  - Daily Updates
- ✓ Snort Rule Beispiele
- ✓ Maleware Zeus
- ✓ Security Onion und Snort Rules
- ✓ Bro
  - Übersicht
  - In der Praxis

Infrastruktur und Demilitarisierte Zone (DMZ)

Unterrichtseinheit	UE 01	SAD

Wie Sie ein Unternehmen besser absichern
Angriffspunkte im Überblick
- ✓ Mitarbeiter
- ✓ Webserver
- ✓ IT-Infrastruktur
- ✓ DMZ

Infrastruktur im Überblick
- ✓ Häufig homogen gewachsen
- ✓ IT folgt Anforderung des Unternehmens
- ✓ Altlasten im Unternehmen
- ✓ Häufig keine Klassifikation von Sub-Netzen
- ✓ Analysen von Netzwerkströmen nur im Störfall

Maßnahmen
- ✓ Organisatorische Maßnahmen
- ✓ Technische Maßnahmen

Schutzbedarf nach Bereich
- ✓ Arbeitsplatz
- ✓ Server
- ✓ Domaincontroller

Nessus Schwachstellenscanner
Greenbone Security Manager (GSM)
Web Security Scanner Netsparker Professional
Erfassung von offenen Diensten
Sonderrolle
- ✓ DMZ

IT-Forensic

Unterrichtseinheit	UE 01	SAD

IT Forensic
- ✓ Geschichte der Computer Forensic
- ✓ Erfolge der Computer Forensic
- ✓ Unterstützende Gesetze
- ✓ Forensic im Internet
- ✓ Forensic Tools
  - OSForensics
  - Volatility
  - DEFT Linux
- ✓ Beispiel Projekt
  - CFREDS
- ✓ Umsetzung in Phase
- ✓ Forensische Analyse
- ✓ Forensische Berichterstattung

KALI2018: Web Hacking Tools im Überblick

	Unterrichtseinheit	UE 01	SAD
	KALI2018 ✓ KALI Linux 2018 Edition ✓ Grundsätzliches: KALI vs. Windows ✓ DAMN VULNERABLY WEB APPLICATION (DVWA) ✓ KALIs Web Security Scanner ▪ OWASP ZAP ▪ BURP Suite ✓ Effektive Web Angriffe mit KALI ✓ Effektives Verstecken von Web Angriffen		

Meltdown & Spectre (und) Memory Attacks

	Unterrichtseinheit	UE 01	SAD
	Meltdown/Spectre/Memory Attacks ✓ Meltdown ▪ Angriff ▪ Beschreibung ▪ Vorführung ▪ Bedrohungspotential ✓ Spectre ▪ Angriff ▪ Beschreibung ▪ Angriffsmethoden ▪ Bedrohungspotential ✓ Chance für Dienstleister		

Meltdown/Spectre – Stand Dezember 2018

	Unterrichtseinheit	UE 01	SAD
	Meltdown/Spectre ✓ Was ist eigentlich Meltdown? ▪ Kurz und bündig ▪ Ausführlich ✓ Was ist eigentlich Spectre? ▪ Kurz und bündig ▪ Ausführlich ✓ Bisherige Varianten ✓ Neue Varianten ✓ Spectre-NG im Überblick ✓ NetSpectre ✓ Foreshadow ✓ Meltdown/Spectre prüfen ✓ Gegenmaßnahmen		

Malware & Viren

Unterrichtseinheit	UE 01	SAD

Ursprung, Funktion & Bekämpfung
- ✓ Kurze Historie der Malware
- ✓ Quellen moderner Malware
  - Verbreitungskanal: E-Mail
  - Verbreitungskanal: Exploit Kit
- ✓ Angebote für Malware
  - Darknet Börsen: AlphaBay Market
- ✓ Funktionen moderner Malware
  - Ransomware
  - Keylogger
  - Trojans
- ✓ Abwehrverfahren im Überblick
  - Anti Maleware Lösungen
  - Network Security Monitoring
  - Generelle Abwehrmethoden

Ursprung, Funktion & Bekämpfung
- ✓ Viren 2016: Symantec IS Treat Report
- ✓ Exploit Kit Analyse mit NSM
- ✓ Malware im Internet
- ✓ Erkennungsquote von Malware
- ✓ Malware Tarnverfahren
- ✓ Effekte moderner Malware
- ✓ Tspion – Keylogger im Kleinstformat
- ✓ Analyse von Tspion über Malwr.com

Network Security Monitoring (NSM)

Unterrichtseinheit	UE 01	SAD

Security Onion
- ✓ Historie
- ✓ Primäre Tools in Security Onion
- ✓ Snort
- ✓ Xplico/Netminer
- ✓ Sguil/Squert
- ✓ ELSA/Bro
- ✓ Argus/RA

Snort
- ✓ Historie
- ✓ Emerging Thread (ET) Rules für Snort
- ✓ Emerging Thread (ET) Daily Updates
- ✓ Snort Rule Beispiel: Malware Zeus (Community)
- ✓ Snort Rules und Alerts

Sguil
- ✓ Übersicht
- ✓ Herzstück der Security Onion
- ✓ Passive Real-time Asset Detection System (PRADS)
- ✓ Schlüsselfunktionen
- ✓ Mächtiges Werkzeug

SQUERT
- ✓ NIDS/HIDS Event Konsole

Bro
- ✓ Übersicht

Opfer eines Hackerangriffs

Unterrichtseinheit	UE 01	SAD

Erkennung des Angriffes
- ✓ Abfluss von Unternehmensdaten
- ✓ Forderungen/Erpressung
- ✓ Technische Erkennung
- ✓ Technische Auffälligkeiten/Anomalien

Abfluss von Unternehmensinformationen

Forderung und Erpressung

Technische Erkennung
- ✓ Analyse über Security Devices

Technische Auffälligkeiten/Anomalien
- ✓ Ungewöhnliches Anwendungs-/PC-Verhalten

Wie tief ist der Angreifer eingedrungen
- ✓ Initial Analyse
- ✓ Erstanalyse

Lassen sich die Angreifer lokalisieren
- ✓ Grundsätzliches

Welche Systeme sind betroffen
- ✓ Grundsätzliches Vorgehen

Fließen Unternehmensinformationen ab

Raspberry Pi/Hacking Devices

	Unterrichtseinheit	UE 01	SAD
	✓ Raspberry Pi und Hacking Devices ✓ Hacker im Taschenformat gefällig? ✓ Zwerge und Riesen ✓ Aufgaben einer Hacking Device ✓ Störung des Betriebsablaufs ✓ Aufbau einer einfachen Hacking Device ✓ Bestückung eines Raspberry Pi 3 ✓ Betriebssysteme für Raspberry Pi Hacking ▪ Basis OS ▪ KALI Linux ✓ Special: Raspberry Pi ohne Steckdose ✓ KALI Linux auf Raspberry installieren ✓ KALI Linux vorbereiten ✓ Konfigurationsdetails ✓ RASPI-CONFIG im Überblick ✓ Raspberry Pi vorbereiten ✓ Zugriff auf das Unternehmensnetzwerk ✓ Vorsicht: Für die echten Hacker		

Security Onion 2018

	Unterrichtseinheit	UE 01	SAD
	Security Onion 2018 ✓ NSM System ✓ Grundfunktionen / Tools ✓ Einsatzgebiete ✓ Einrichtung der Security Onion ✓ Testalarm für Security Onion ✓ NSM Konsolen im Überblick ✓ Live System im Überblick ✓ Dienstleistung NSM		

Social Engineering

	Unterrichtseinheit	UE 01	SAD
	Meltdown & Spectre ✓ Pre-Meltdown Bemühungen ✓ Das Ergebnis: Meltdown & Spectre ✓ Was ist eigentlich Meltdown? ✓ Kurz & bündig ✓ Ausführlich ✓ Was ist eigentlich Spectre? ✓ Kurz & bündig ✓ Ausführlich ✓ Viel wichtiger: Sind Sie eigentlich geschützt? ✓ Patches für Microsoft Windows ✓ Welche Lücken beseitigt der Windows Patch? ✓ Welche Lücken bleiben trotz Patch? ✓ Patches für Windows 7 und Windows 8? ✓ Wird Windows Server automatisch geschützt? ✓ Schnellanleitung Windows ✓ Patchstand ✓ Wachsamkeit		

Spectre Update + Alarmstufe Rot

	Unterrichtseinheit	UE 01	SAD
	✓ Was ist Social Engineering? ✓ Grundsätzliche Arten des Social Engineering ✓ Human Based ▪ Impersonation ▪ Posing as important User ▪ Being a third party ▪ Desktop Support ▪ Shoulder Surfing ▪ Dumpster Diving ✓ Computer Based ▪ Phishing ▪ Spear Phishing ▪ Baiting • Special USB Hacking • Website Beispiel ✓ Online Scam		

The Golden Ticket

	Unterrichtseinheit	UE 01	SAD
	The Golden Ticket ✓ Aufbau der Testumgebung ✓ Eine der gefährlichsten Angriffsmethoden ✓ Etwas Hexa notwendig ✓ Technische Durchschüsse gegen DCs? ✓ Indirekte Angriffe sind möglich ✓ Ergebnisse ✓ Effekt: Ticket Granting Tickets ✓ Ergebnis: Uneingeschränkte Zugriffsrechte ✓ Gegenmaßnahmen ✓ Erkennung von Golden Ticket Angriffen		

Vulnerability Scanner und deren Anwendungen

	Unterrichtseinheit	UE 01	SAD
	Vulnerability Scanner und deren Anwendungen ✓ Was ist eine Schwachstelle? ✓ Aufspüren einer Schwachstelle ✓ Vulnerability Scanner Grundfunktionen ✓ Verfügbare Scanner ✓ Open Source • OpenVAS ✓ Kommerzielle • Tenable Nessus • Rapid7 Nexpose • Qualys • Goolge: Vulnerability Scanner • Metasploitable		

Waffen der Hacker: SQL Injection

	Unterrichtseinheit	UE 01	SAD
	✓ SQL Injection (SQLi) Erkennen und Abwehren ✓ SQL Injection ▪ Gefahren ▪ Grundlagen ✓ Betroffene Programmiersprachen ✓ SQL Injection in der Praxis ✓ Angriffstool: SQLMAP ✓ Erfolgreiche Angriffe ✓ Log goes SIEM? ✓ Streams vs. SQL Injection ✓ Einfachere Abwehrmethoden ✓ Effizienteste Abwehr: Gute Programmierung		

Webservice und –server

	Unterrichtseinheit	UE 01	SAD
	Angriffe gegen Webanwendungen Immunisierung gegen Strafverfolgung Angreifertypen (Web Attacken) Abhärtung gegen Angriffe Grundregeln ✓ Szenario 1 Schlechtes Beispiel ✓ Szenario 2 Gutes Beispiel Abhärtung gegen Angriffe: Hardening Abhärtung von Apache Webserver Überprüfung der SSL/TLS Einstellung OWASP ✓ All About Web Security ✓ A1 – SQL Injection im Detail & Tools ✓ A3 – Cross Site Scripting Universelle Web Security Scanner Spitze des Eisbergs		

Wie sicher ist Festplattenverschlüsselung?

	Unterrichtseinheit	UE 01	SAD
	✓ Bitlocker und Co. ✓ Der Bootprozess ▪ Größte Schwachstellen ▪ Secure Boot ▪ Normale Boot Prozess ▪ Fazit ✓ Was hat das mit Bitlocker und Co. zu tun? ✓ Wie lässt sich Bitlocker angreifen? ✓ Angriffsszenario ✓ Kommerzielle Tools für Key Extraaktion ✓ Master Key im Einsatz ✓ Wie kriegt man Bitlocker sicher? ✓ Welche Verschlüsseler sind angreifbar? ✓ Veracrypt		

Wie sich Hacker im Internet verstecken

	Unterrichtseinheit	UE 01	DSB
	✓ Hacker ohne Spuren ✓ Zugang zum Internet ✓ Anonyme Internetzugänge ✓ Internetzugänge: Sagen und Legenden ✓ Anonymität durch Verschleierung ✓ Channel ▪ VPN ▪ Proxy Server ▪ Tunneling mit Spezialprotokollen ✓ TOR-Netzwerk ▪ Funktionsweise ▪ Verbindungsaufbau ▪ Datenübertragung ▪ Facts ✓ Tor-Wächter: Entry Guards ✓ Tor-Exit-Nodes ✓ Wo legen Hacker Daten ab?		

Weitere wichtige Informationen

Sie haben Fragen oder Anregungen?

Falls Sie Fragen, Wünsche oder Anregungen zu dieser oder zu anderen Ausbildungen haben, stehen wir Ihnen montags bis donnerstags in der Zeit von 08:00 – 17:00 Uhr und freitags von 08:00 – 15:00 Uhr sehr gerne zur Verfügung.

Sie erreichen uns unter:

Telefon: 09526 95 000 60
E-Mail: info@ITKservice.NET

Ihre Ansprechpartner für das ITKwebcollege.ADMIN

Christoph Holzheid
Anne Hirschlein
Sylvia Sonntag
Thomas Wölfel

Copyrights und Vertragsbedingungen

Das Copyright © aller Trainings, inkl. aller Aufzeichnungen und Unterlagen obliegt der ITKservice GmbH & Co. KG. Die Nutzung aller ITKwebcollege-Leistungen ist nur für den Vertragspartner und nur für den internen Gebrauch gestattet. Eine Weitergabe der Leistungen an Dritte ist nicht zulässig.

Kontaktdaten | Impressum

ITKservice GmbH & Co. KG
Fuchsstädter Weg 2
97491 Aidhausen

Telefon: 09526 95 000 60
Telefax: 09526 95 000 63

www: ITKservice.NET
E-Mail: info@ITKservice.NET

Sitz der Gesellschaft: Aidhausen | Amtsgericht Bamberg, HRA 11009, Ust-Id: DE 262 344 410 | Vertreten durch: Thomas Wölfel (GF).

Bildnachweise: Alle in diesem Dokument dargestellten Bilder wurden von der ITKservice GmbH & Co. KG bei ccvision.de lizensiert.
Redaktion: ITKservice GmbH & Co. KG | Copyright © 2017 ITKservice GmbH & Co. KG.