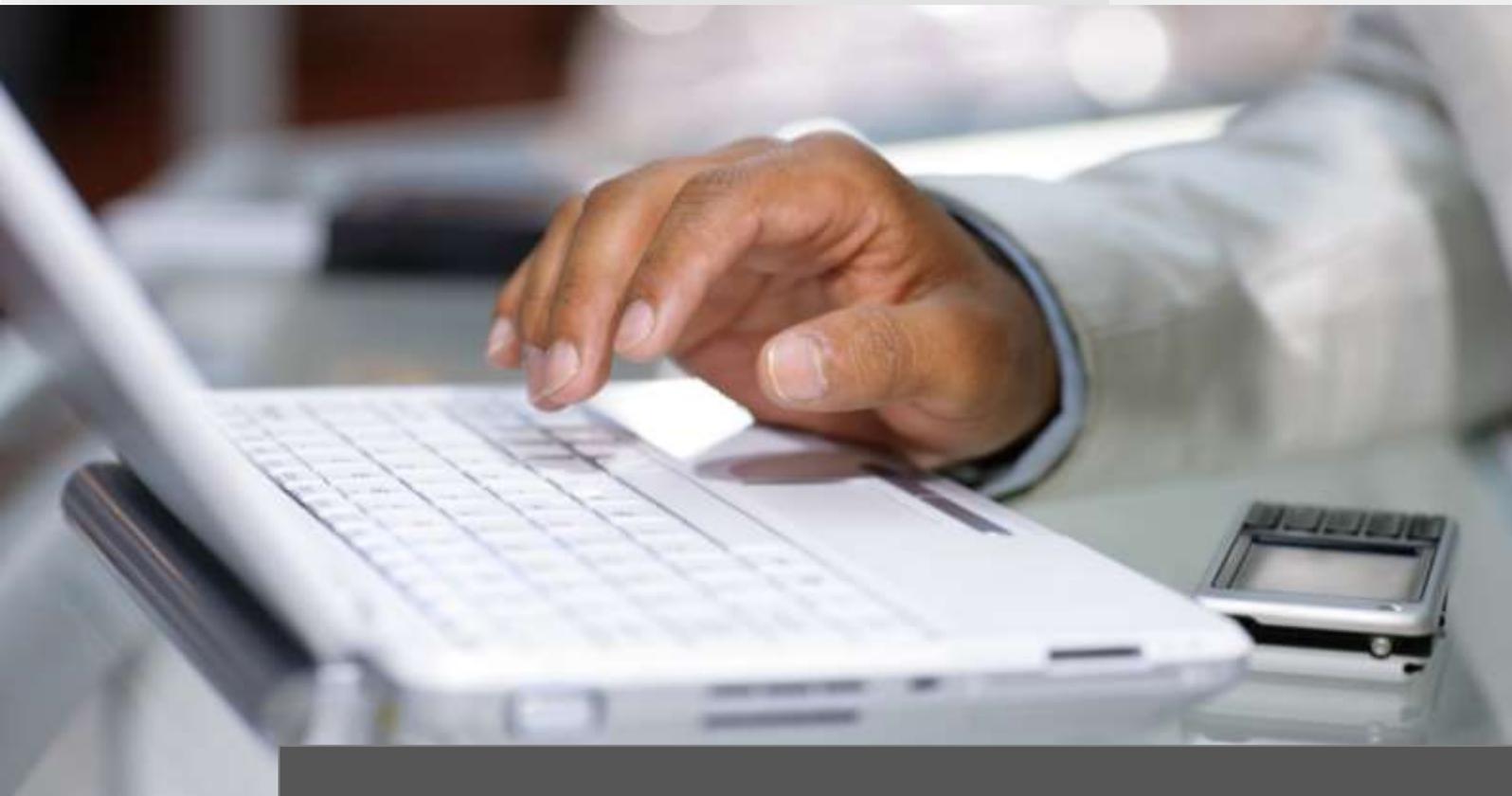


# ITKwebcollege.Security Advanced Trainings

Online-Trainings für Security-Consultants oder Security-Experten | Stand August 2017



Ausbildungsinhalte

# Inhaltsverzeichnis

<b>Security Advanced Trainings</b>	<b>3</b>
Erpressungstrojaner oder Kryptotrojaner (Ransomware)	3
Hacker's Diary - Dedicated Malware Attack	3
Hacking und IT-Security	3
Infrastruktur und Demilitarisierte Zone (DMZ)	4
IT-Forensic	4
Malware & Viren	4
Network Security Monitoring (NSM)	5
Opfer eines Hackerangriffs	5
Webservice und -server	5
<b>Weitere wichtige Informationen</b>	<b>6</b>
Sie haben Fragen oder Anregungen?	6
Copyrights und Vertragsbedingungen	6
Kontaktdaten   Impressum	6



# Security Advanced Trainings

## Erpressungstrojaner oder Kryptotrojaner (Ransomware)

Unterrichtseinheit	UE 01	DSB
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?		

## Hacker's Diary - Dedicated Malware Attack

Unterrichtseinheit	UE 01	DSB
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		

## Hacking und IT-Security

Unterrichtseinheit	UE 01	DSB
Aktuelle Angriffsszenarien ✓ Angriffe im Überblick <ul style="list-style-type: none"> <li>▪ Kryptotrojaner (Ransomware)</li> <li>▪ SEO Fraud</li> <li>▪ Zielgerichtete Attacken</li> </ul> ✓ Dienstleistungen im Überblick <ul style="list-style-type: none"> <li>▪ Penetrationstesting</li> <li>▪ Forensische Analysen</li> <li>▪ NSM Analysen</li> </ul> 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	

## Infrastruktur und Demilitarisierte Zone (DMZ)

Unterrichtseinheit		UE 01	DSB
<ul style="list-style-type: none"> <li>Wie Sie ein Unternehmen besser absichern</li> <li>Angriffspunkte im Überblick</li> <li>✓ Mitarbeiter</li> <li>✓ Webserver</li> <li>✓ IT-Infrastruktur</li> <li>✓ DMZ</li> <li>Infrastruktur im Überblick</li> <li>✓ Häufig homogen gewachsen</li> <li>✓ IT folgt Anforderung des Unternehmens</li> <li>✓ Altlasten im Unternehmen</li> <li>✓ Häufig keine Klassifikation von Sub-Netzen</li> <li>✓ Analysen von Netzwerkströmen nur im Störfall</li> <li>Maßnahmen</li> <li>✓ Organisatorische Maßnahmen</li> <li>✓ Technische Maßnahmen</li> </ul>	<ul style="list-style-type: none"> <li>Schutzbedarf nach Bereich</li> <li>✓ Arbeitsplatz</li> <li>✓ Server</li> <li>✓ Domaincontroller</li> <li>Nessus Schwachstellenscanner</li> <li>Greenbone Security Manager (GSM)</li> <li>Web Security Scanner Netsparker Professional</li> <li>Erfassung von offenen Diensten</li> <li>Sonderrolle</li> <li>✓ DMZ</li> </ul>		

## IT-Forensic

Unterrichtseinheit		UE 01	DSB
<ul style="list-style-type: none"> <li>IT Forensic</li> <li>✓ Geschichte der Computer Forensic</li> <li>✓ Erfolge der Computer Forensic</li> <li>✓ Unterstützende Gesetze</li> <li>✓ Forensic im Internet</li> <li>✓ Forensic Tools <ul style="list-style-type: none"> <li>▪ OSForensics</li> <li>▪ Volatility</li> <li>▪ DEFT Linux</li> </ul> </li> <li>✓ Beispiel Projekt <ul style="list-style-type: none"> <li>▪ CFREDS</li> </ul> </li> <li>✓ Umsetzung in Phase</li> <li>✓ Forensische Analyse</li> <li>✓ Forensische Berichterstattung</li> </ul>			

## Malware & Viren

Unterrichtseinheit		UE 01	DSB
<ul style="list-style-type: none"> <li>Ursprung, Funktion &amp; Bekämpfung</li> <li>✓ Kurze Historie der Malware</li> <li>✓ Quellen moderner Malware <ul style="list-style-type: none"> <li>▪ Verbreitungskanal: E-Mail</li> <li>▪ Verbreitungskanal: Exploit Kit</li> </ul> </li> <li>✓ Angebote für Malware <ul style="list-style-type: none"> <li>▪ Darknet Börsen: AlphaBay Market</li> </ul> </li> <li>✓ Funktionen moderner Malware <ul style="list-style-type: none"> <li>▪ Ransomware</li> <li>▪ Keylogger</li> <li>▪ Trojans</li> </ul> </li> <li>✓ Abwehrverfahren im Überblick <ul style="list-style-type: none"> <li>▪ Anti Malware Lösungen</li> <li>▪ Network Security Monitoring</li> <li>▪ Generelle Abwehrmethoden</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Ursprung, Funktion &amp; Bekämpfung</li> <li>✓ Viren 2016: Symantec IS Treat Report</li> <li>✓ Exploit Kit Analyse mit NSM</li> <li>✓ Malware im Internet</li> <li>✓ Erkennungsquote von Malware</li> <li>✓ Malware Tarnverfahren</li> <li>✓ Effekte moderner Malware</li> <li>✓ Tspion – Keylogger im Kleinstformat</li> <li>✓ Analyse von Tspion über Malwr.com</li> </ul>		

## Network Security Monitoring (NSM)

Unterrichtseinheit	UE 01	DSB
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	DSB
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	

## Webservice und -server

Unterrichtseinheit	UE 01	DSB
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	

## 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](mailto:info@ITKservice.NET)

Ihre Ansprechpartner für das ITKwebcollege.ADMIN

Christoph Holzheid  
Anne Hirschlein  
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](http://ITKservice.NET)  
E-Mail: [info@ITKservice.NET](mailto: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 lizenziert.

Redaktion: ITKservice GmbH & Co. KG | Copyright © 2017 ITKservice GmbH & Co. KG.