Vysoká škola Karla Engliše, a.s.

Pětitýdenní e-learningové bezpečnostní kurzy

Od července 2015 budou na Vysoké škole Karla Engliše, a. s., (VŠKE) probíhat komerční pětitýdenní běhy osmi bezpečnostních e-learningových kurzů. Každý kurz zahrnuje úvodní prezentaci, průběžnou konzultaci a závěrečné soustředění (celkem 3 x 4 hod. přímé výuky). V rámci e-learningového studia budou mít studenti přístup na výukový server Moodle a na něm k dispozici potřebné prezentace, výukové videofilmy, opakovací autotesty a řadu dalších výukových materiálů. Kurzy připravili odborníci v oblasti bezpečnosti ICT z brněnských vysokých škol a z praxe. Kurzy budou probíhat jak v pevných termínech, tak na vyžádání firem či organizací. Cena kurzu je 2 000 Kč. Do kurzů budou přednostně zařazování IT pracovníci firem působících v Jihomoravském kraji. Každý kurz je zakončen finálním testem, absolventi získají Osvědčení o účasti v pilotním ověření příslušného kurzu.

OSVĚDČENÍ

o účasti v pilotním ověření o e-learningového kurzu

Bezpečnost síťových technologií

v rámci projektu Podpora bezpečnostního vzdělávání IT pracovníků v Jihomoravském kraji

Pořadatelem kurzu byla
Vysoká škola Karla Engliše, a. s.

Potvrzujeme, že absolvent kurzu

Ing. Msc. Martin Sikora

úspěšně absolvoval e-learningové studium zakončené závěrečným testem, v jehož rámci prokázal znalosti z oblasti

standardy v oblasti sítí, terminologie, komunikační média. Ethernet – varianty, bezpečnost. Sada protokolů TCP/IP a jejich bezpečnostní aspekty. Protokol IP – adresace, význam masky, formát paketu. Problematika směrování, směrovací protokoly. Vytváření podsítí, plánování dělení adresního protokolu. Protokol TCP, formát segmentu, navazování a rozvazování spojení, oprava chyb. Protokol UDP, formát segmentu. Protokol IPv6, jeho nové vlastnosti. Přidělování IPv6 adres, problém přechodu na IPv6. Bezpečnostní aspekty IPv6. Analýza provozu v počítačové síti, program Wireshark. Obranné opatření typu Remotely Triggered Black Hole. Virtuální lokální počítačové sítě, konfigurace. Bezpečnost na linkové vrstvě, útoky a obrana: CAM overflow, MAC flooding, ARP spoofing, překlad VLAN, DHCP Snooping, dynamická ARP inspekce, nucené přesměrování, Loďina Terpit, přeskoky mezi VLAN. Protokol Spanning Tree, útoky proti němu a obrana. Access Control List. Protokol 802.1X. Protokol ICMP a jeho bezpečnostní aspekty. Protokol SNMP. Zabezpečení pomocí protokolu IPSec.

Datum absolvování kurzu: 21. 11. 2013

doc. Ing. Jaroslav Dočkal, CSc.
manažer projektu

Ing. Josef Kaderka, Ph.D.
lektor

Kurzy jsou výsledkem prací na projektu s názvem „Podpora bezpečnostního vzdělávání IT pracovníků v Jihomoravském kraji“. Tento projekt byl na VŠKE řešen od roku 2013 v rámci Operačního programu Vzdělávání pro konkurenceschopnost. Obsahem projektu byla tvorba a pilotní ověření jednotlivých kurzů. V současné době proběhly jejich pilotní běhy, vyhodnocují se získané zkušenosti a na jejich podkladě jsou kurzy převáděny do finální podoby tak, aby je bylo možné od července 2015 spustit „na ostro“.

V nabídce VŠKE, a. s., jsou kurzy s následujícím obsahem:

Kategorizace síťových útoků

- Malware, spyware, riskware, adware který může ohrožovat podnikovou síť, a další hrozby.
- Backdoory, Trapdoory (zadní vrátka), logické bomby, trojští koně, viry, červi, phishing, DOS, DDOS, botnety, payloady, exploity a metaexploity,

útoky na sociální sítě a mobilní zařízení včetně řešení typu BYOD (Buy Your Own Device).
- Použití Tcpdumpu, Hpingu, Nmapu, Wiresharku, řešení praktických problémů sítě a identifikace jejího napadení, NIDS (Network Intrusion Detection System), IPS, SIEM, Snort pro detekci signatur a další nástroje (Nagios, Zabbix, OpenNMS, Zenoss a NetFlow atd.) s využitím v praktických příkladech.
- Klasifikace síťových útoků, zranitelností, rizik a hrozeb.
- Nástroje a postupy pro detekci útoků a anomálií s nimi spojenými.
- Ochrana a prevence před útoky, eliminace škod a dopadů.
- Bezpečnostní monitoring, nástroje pro testování a simulaci útoků, metodiky, standardy, certifikace a legislativa.

Bezpečnost operačních systémů MS Windows

- Obecné bezpečnostní postupy uživatele MS Windows (provádění aktualizací, využívání antivirových programů a personálních firewallů, zálohování a obnova dat).
- Teoretické základy bezpečnosti MS Windows (architektura operačního systému a bezpečnostního podsystému, datové struktury využívané bezpečnostním podsystémem.
- Bezpečnostní identifikátor, přístupová známka, bezpečnostní deskriptor), bezpečnost souborů (přístupová práva, šifrování, sdílení).
- Správa uživatelských účtů, autentizační protokoly, základní pravidla práce s hesly, luštění hesel.
- Provádění auditu, použití bezpečnostních šablon pro analýzu a konfiguraci systému, konfigurace Software Restriction Policy a IPSec na počítači.

Bezpečnost síťových technologií

- Protokoly IPv4, IPv6.
- Plánování adresního prostoru, vytváření podsítí, bezpečnost protokolu.
- Jmenná služba – nastavení DNS, SecureDNS, bezpečnost el. pošty.
- Správa sítí, protokol SNMP, syslog; systémové nástroje pro testování počítačových sítí a zjišťování jejich vlastností, analýza provozu v počítačových sítích.
- Zabezpečení přenášených dat, konfigurace protokolu IPSec.

Pokročilé metody síťové bezpečnosti

- Analýza provozu v lokálních počítačových sítích, virtuální LAN, protokoly Spanning Tree, Rapid Spanning Tree, Multiple Spanning Tree.
- Protokoly linkové vrstvy, jejich význam a bezpečnost, obrana proti zneužití protokolu Spanning Tree, podvržení ARP dat a DHCP dat, význam protokolu ICMP.
- Směrování a směrovací protokoly, ochranné mechanismy směrovacích protokolů, jmenná služba, nastavení DNS, SecureDNS.
- Výstavba firewallů prostřednictvím mechanismů pro filtraci provozu a analýzu obsahu, systémy detekce průniku, systémy prevence průniku, jejich konfigurace.
- Testování bezpečnosti – přehled metod a nástrojů, jejich dělení, možnosti a využívání.

Bezpečnost webových aplikací

- Architektura webových aplikací (URL adresa, http protokol, jazyk HTML, kaskádové styly, Javascript, webové servery,spolupráce s databází, webové služby).
- Bezpečnost prohlížečů webu (Same Origin Policy, zóny Internet Exploreru).
- Typické útoky na webové aplikace a jejich prevence (Cross-Site Scripting, Cross-Site Request Forgery, SQL Injection).

Zajištění bezpečnosti ICT pomocí kryptografických prostředků

- Symetrická a asymetrická kryptografie, AES (Advanced Encryption Standard) a RSA.
- Dohoda o klíči na bázi D-H algoritmu, hashe, digitální podpisy, certifikáty, atributové certifikáty, certifikáty s rozšířenou validací, PKI (Public Key Infrastructure).
- Protokoly IPSec, SSH (Secure Shell), SSL (Secure Sockets Layer), TLS Transport Layer Security), PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol).

Metodologické aspekty ICT bezpečnosti, standardy a normy

- Úvod do bezpečnostního managementu – základní pojmy, bezpečnostní standardy ISO, ITU-T řady ICT Security a ETSI.
- ITIL a jeho bezpečnostní aspekty.
- Použití COBIT pro bezpečnostní auditory, standardy SixSigma.
- Metriky bezpečnosti, vzájemné vztahy mezi bezpečnostními standardy, normami a praktikami a jejich aplikace ve prospěch podnikové bezpečnosti a bezpečnosti podniku.

Bezpečnost bezdrátových technologií

- Problematika šíření elektromagnetických vln, antény; modulace.
- Standardy WLAN (802.11a/b/g/h/n/ac/ad; 802.16), přístupová metoda CSMA/CA, bezpečnost WLAN.
- Algoritmy WEP/ WPA/WPA2, sdílené heslo/bezpečnostní infrastruktura, základní nastavení přístupového bodu, nastavení zabezpečení, režimy práce přístupového bodu.
- Složitější struktury bezdrátových sítí a jejich konfigurace.
- Protokol 802.1X a jeho konfigurace, centrální správa přístupových bodů a jejich ochrana, zvláštnosti útoků proti WiFi sítím.

Kontaktní informace	
Adresa	Vysoká škola Karla Engliše, a.s., Mezírka 1, 602 00 Brno
Kontaktní osoba	doc. Ing. Jaroslav Dočkal, CSc.
Telefon	+420 515 917 608, +420 737 215 217
E-mail	jaroslav.dockal@vske.cz
WWW	http://www.dalsivzdelavanivske.cz, http://www.vske.cz/cz/nabidka-kurzu/bezpecnostni-kurzy