P.č.	Názov položky	Minimálna požadovaná špecifikácia položky	Kategorizácia položky pre servisnú podporu	MJ	Počet
1	**PC + Monitor pre odborné učebne grafik, dizajnér, práca s videom**	PC s min. parametrami: Šesťjadrový procesor s výkonom podľa www.cpubenchmark.net na úrovni min. 10 700 CPU mark. Chassis : Tower prevedenie so zámkom a bezpečnostným prepínačom pri otvorení a detekciou v biose; Zdroj : výkon zdroja musí pokryť ostatné potreby HW; Otvory : do 5 ks (1x 5.25" slim externý prístup a [1x 3.5" externý prístup alebo 1x 3.5" interný HDD bay alebo 2x 2.5" interný HDD/SSD-bays], [1x 3.5" interný HDD-bay alebo 2x 2.5" interný HDD/SSD-bays]). Predné vstupy: 2x USB 3.1, 1x audio von, 1x audio dnu. 1 x Internal speaker Základná Doska: Sloty: 4 DIMM-sockets (max. 64 GB, DDR4-2666, ECC or non-ECC, dual channel), 2 sloty: [1x PCIe 3.0 x16 and 1x PCIe 3.0 x4 (mechanical x16)] alebo [1x PCIe 3.0 x16 and 1x PCI], 1x M.2 socket for PCIe SSD. I/O-devices: HD Grafika podľa CPU, sieťový kontrolér, Serial ATA kontrolér (6 Ports – SATA III; RAID 0, 1, 5 or 10 for HDDs/SSDs) a HD-audio . Zadné rozhrania: 2x DisplayPort 1.2, 1x DVI-D, 1x LAN RJ45, 6x USB 3.0, 1x audio in, 1x audio out, 2x PS/2 pre myš a klávesnicu. Interné rozhrania : 2x USB 2.0, 1x USB 3.0 so štandartným konektorom. Vstavaná bezpečnosť na úrovni TPM 2.0, Možnosť zakázať, skryť TPM voľbu v biose Pamäť : 1 x 8GB DDR4-2666 Grafická karta s min. výkonom podľa www.videocardbenchmark.net na úrovni 4700 G3D mark Disk: 1x SSD PCIe 512GB M.2 NVMe Highend 1 x klávesnica so slovenskými znakmi, 1 x USB optická myš s rozmermi šírka x dĺžka x výška - 61 x 109 x 38 mm, 1200 DPI 1 x DVD SuperMulti SATA slim, OS so slovenskou lokalizáciou a možnosťou prihlásenia do domény , kompatibilný s OS , ktorý používa verejný obstarávateľ (ďalej len "VO"). (VO používa v súčasnosti OS Windows 10), Monitor: veľkosť min. 24" s technológiou zobrazovania IPS/LED, rozlíšenie FULL HD 1920 * 1080, typický kontrast 1000:1, pozorovací uhol 178°/178°, 5 ms GTG , Porty : DisplayPort 1 x DisplayPort, DVI 1 x DVI-D (HDCP), VGA/D-SUB 1 x D-SUB, Audio signal output 3.5 mm stereo phone jack, Audio signal input 3.5 mm stereo phone jack, Jas : 250 cd/m2	HW-A	ks	96
2	**Notebook pre učiteľa do odbornej učebne**	Notebook s min. parametrami: Šesťjadrový procesor s výkonom podľa www.cpubenchmark.net min.10 300 CPU Mark a min. frekvenciou až 4,1 GHz Chassis + obrazovka : 15,6" - 39.6 cm LED backlit,(Full HD),Anti-glare IPS display,magnesium,1,920 x 1,080 pixel Rozhrania: 1x VGA, 1x HDMI, 2x USB Type-C (Thunderbolt 3, USB 3.1Gen2, DP 1.4, Power Delivery 15W), 2x USB 3.1, RJ45 for LAN, 1x Audio Combo, 1x Docking connector ; grafická karta s min. výkonom podľa http://www.videocardbenchmark.net 4 700 G3D Mark Pamäť : 8GB DDR4 2400 MHz (1x 8GB) Disk: M.2 PCIe 512 GB Highend NonSED Wireless (802.11ac) + Bluetooth 5.0 + LAN 10/100/1,000 MBit/s Interná klávesnica so slovenskou lokalizáciou bez TS Optická USB myš 1000 DPI s rozmermi šírka x dĺžka x výška 51 x 85 x 29 mm Výdrž batérie min. 8 hodín, OS so slovenskou lokalizáciou a možnosťou prihlásenia do domény , kompatibilný s OS , ktorý používa VO. (VO používa v súčasnosti OS Windows 10)	HW-A	ks	4
3	**Notebook pre IKT učebne**	Notebook s min. parametrami: Dvojjadrový procesor s výkonom podľa www.cpubenchmark.net min. 3600 CPU Mark a min. frekvenciou 2 GHz Displej : LCD 15,6" Anti-Glare HD (1366 x 768) LED Backlight Pamäť : 4 GB DDR4 2133 MHz Disk : SSD SATA III 512 GB high speed Integrovaná WLAN + Bluetooth 4.2 + LAN 10/100/1,000 MBit/s Rozhrania: VGA, HDMI, 1x USB 2.0, 3x USB 3.0, RJ45 for LAN, audio combi, SD card slot Driver and Utility DVD (DUDVD) SD/SDHC/SDXC čítačka kariet, HD-kamera s integrovaným dig. mikrofónom a 0.92M pixelov rozlíšením Interná klávesnica so slovenskou lokalizáciou bez TS Optická USB myš 1000 DPI s rozmermi šírka x dĺžka x výška 51 x 85 x 29 mm 6 článková batéria (48 wh)	HW-A	ks	48
4	**SW pre prácu s videom**	Profesionálny SW nástroj na vytváranie, editáciu, strih a ďalšie spracovanie videa a audia. Musí podporovať editáciu SD, HD alebo 3D videa pomocou drag&drop funkcie, musí obsahovať rôzne nástroje na editovanie a musí disponovať množstvom video efektov, musí umožnovať editovanie videí z viacerých kamier, video stabilizáciu, musí umožnovať nastavenie editačných okien, podporu HDV, AVCHD, RED, SDI, XDCAM SR a audio/video synchronizáciu. Musí pracovať s OpenCL a musí podporovať zariadenia od výrobcov AMD a NVIDIA. Musí obsahovať editačné nástroje, GPU akceleráciu, stereoskopické 3D editovanie, NewBlue titulkovač, výkonné audio nástroje. - akademická neobmedzená licencia	-	ks	100
5	**Sada grafických programov**	Sada grafických programov, neobmedzená licencia na školu, ktorá musí obsahovať nasledovné SW: 1. SW, ktorý musí obsahovať funckie, ktoré pomáhajú ľahko a s istotou vytvárať zaujímavé návrhy, grafiku, fotografie a weby. 2. SW pre úpravu obrázkov a fotografií 3. SW pre nové kreatívne možnosti s grafickým štetcom, ktoré dokonale napodobňujú reálné materiály, a také materiály, ktoré v reálném svete neexistujú. SW umožňuje prežiť jedinečnú harmóniu vo vyjadreniach zvukov, inteligentným klonovaním fotografií, s pomocou kompozičných nástrojov, fyzikou inspirovaných štetcov, a zabudovaným learningom - všetko musí byť podporované vo vysokom DPI 4. Výkonný SW musí umožnovať prácu so strihom videa , musí obsahovať nástroje na úpravu videa a efektov, SW musí umožnovať vytvárať 4K a HD filmy 5. SW musí umožnovať tvorbu, editáciu a prevádzanie PDF dokumentov, ktoré ponúkajú výkon z popredných PDF programov. SW musí umožňovať otvárať, prehliadať a pracovať s viac ako 100 rôznych formátov súborov	-	sd	1
6	**SW pre vývoj webových stránok**	SW na podporu vývoja webových štandardov . SW musí umožňovať navrhovať interaktívne animácie pomocou nástrojov pre kreslenie. Musí publikovať svoje výsledky na rôznych platformách, vrátane formátov Flash / AIR, HTML5 Canvas, WebGL alebo vlastných platforiem. Akademická licencia na min. 3 roky	-	ks	100
7	**Kancelársky balík**	Kancelársky balík kompatibilný s OS ponúkanými v položkách 1, 2 a 8 . Balík musí obsahovať moduly minimálne pre prácu s textom , pre tvorbu tabuľkových kalkulátorov, poštového klienta, nástrojov pre tvorbu prezentácií a pre prácu s databázami. Neobmedzená akademická licencia.	-	ks	148
8	**OS pre Notebooky do IKT učební**	OS so slovenskou lokalizáciou a možnosťou prihlásenia do domény , kompatibilný s OS , ktorý používa VO. (VO používa v súčasnosti OS Windows 10)	-	ks	48
9	**Informačné displaye**	Slim displej bez nutnosti použitia Set-top boxu s min. parametrami: veľkost 55", 5×5 multiscreen. Musí mať zabudované 2 x 10 W reproduktory, musí spĺňať funkcionalitu Multi Monitoring & Control Software LAN správy, Musí obsahovať Centrálny managment- SW pre ľahko spravovateľné riešenie informačných panelov, ktoré je ideálny pre vytváranie dynamických vizuálnych obrazov pre firemnú či verejnú sféru. Obsah obrazu musí obsahovať texty, fotografie, audio, video a webový obsah v plne prispôsobiteľnej konfigurácii.	-	ks	2
10	**Robot**	Humanoidný robot. Plne programovateľný a otvorený systém. Využitie pre odborné predmety informatiky a matematiky. Min. parametre: procesor s min frekvenciou 1,6 GHz 1 GB RAM 1x RJ45 alebo WiFi IEEE 802.11b/g/n Motory pre pohyb kamera pre interakciu s okolím umiestnené na hlave mikrofón pre zachytenie zvuku reproduktor pre komunikáciu senzory pre zisťovanie polohy robota gyrometer a akcelerometer pre zisťovanie rýchlosti Výdrž batérie maximálne 1,5 hodiny Prístroje pre zisťovanie polohy Dotykové senzory na hlave, rukách a nohách Rozmery výška 500 mm, šírka 120 mm, Programovanie v jazyku C++ a iné (podľa dostupnosti)	-	ks	4
11	**Vizualizéry**	Popis a min. parametre: Interaktívny vizualizér musí umožnovať živý streaming v rozlíšení Full HD a až 128 násobný zoom v kombinácii s 8x optickým zväčšením. Musí podporovať 30 snímok za sekundu pre maximálne plynulé prezentácie. Musí disponovať min. 5-megapixlový snímačom. Musí zachytiť plochu až do veľkosti A4, Musí obsahovať ľahko použiteľný ovládací panel a interaktívny software.	-	ks	15
12	**Profesionálna kamera**	Min. parametre: Digitálna kamera s čipom typu CMOS, 8.3Mpx, 4K (3840x2160) video, vstavaný mikrofón, WiFi, NFC, GPS, 16: 9, 3.5 "LCD, HDMI, Micro USB, stereo mini jack, SD / SDHC / SDXC, Memory Stick Duo + objektív 18–105 mm s bajonetom E, stabilizátor SteadyShot, clona F4 v celom rozsahu ohniskovej vzdialenosti	-	ks	2
13	**3D tlačiareň**	Min. parametre: Spotreba : do 300 W, Tlačový objem 300 x 300 x 300 mm Technológia: LPD – Layer Plastic Deposition, Rozlíšenie os Z Štandardné 90-400 µm, Pokročilé 25-50 µm, Najmenší Bod 400+ µm, Hrúbka stien Minimálna 400 µm, Optimálna 800+ µm, kompaktibilné materiály Priemer struny 1,75 mm Priemer trysky 0,4 mm Rozlíšenie os X,Y 1,5 µm Min. krok os Z 1,25 µm Teplota hlavy max. 380° C Teplota podložky max. 110° C , obslužný softvér, Formáty .stl, .obj, .dxf Operačný systém Mac OS X, Windows XP, Windows Vista, Windows 7, Windows 8, Ochranné krytovanie Áno, Súčasťou balenia musí byť : 22 x 800 g balenie tlačového materiálu HIPS v prevedení : 3 x biela, 3 x čierna, 3x šedá, 2 x červená, 2 x zelená, 2 x žltá, 2 x modrá, 5 x prevedenie Glass.	-	ks	2
14	**Interaktivna tabuľa, dataprojektor, Interaktívny SW**	Min. parametre : Interaktívna tabuľa so snímacou technológiou, pomer strán 4:3, rozmer aktívnej plochy 79" (min 1645*1150mm), rozlíšenie ≥ 32768*32768, rýchlosť zápisu ≥ 5m/s, rýchlosť odozvy ≤ 6ms, písanie pero alebo prst, hmotnosť max. 14 kg. Možnosť pripojiť pomocou dodávaného USB kábla alebo pomocou bezdrôtového adaptéra (voliteľné príslušenstvo). Súčasťou dodávky má byť originálny anotačný softvér v slovenskom jazyku a vizuálna knižnica, ktorá má obsahovať stovky výukových interaktívnych 3D modelov. Softvér má umožňovať rozpoznávanie rukopisu v slovenskom jazyku aj s diakritikou a má byť plne integrovaný s prostredím MS OFFICE (má podporovať priame vkladanie poznámok do Wordu, Excelu, PowerPointu s ukladaním vo formátoch MS Office). Spolupráca s dokumentačnou kamerou, hlasovacím systémom. Min. špecifikácia pre dataprojektor - DLP technológia s podporou 3D, natívne rozlíšenie min. XGA (1024x768), svetelný výkon min. 3200 ANSI lumenov, kontrast min. 13 000:1, Throw ratio max. 0,61, konektivita min. 2x VGA-In (15pin D-Sub), 1x HDMI, 1x S-Video, 1x Composite Video, 1x Audio-In (Mini-Jack), 1x VGA-Out (15pin D-Sub), 1x Audio-Out (Mini-Jack), 1x RS-232 a 1x USB miniB, hlučnosť menej ako 28 dB	-	sd	8
15	**Centrálne pracovisko**	1. a) Firewall s IPS funkcionalitou s min. technickými parametrami : Rozhrania : 8 x 10/100/1000 RJ-45; 1 x konzolový sériový port; Podpora IPSec VPN (Remote Access aj Site-to-Site) Podpora SSL VPN (VPN klient) ; Možnosť rozšírenia o IPS, URL filtering a Antimalware funkcionalít iba pridaním licencie ; Podpora L7 aplikačnej inšpekcii ; Podpora IEEE 802.1q, 802.3ad ; Podpora min. 100 VLAN ; Podpora transparentného režimu; Podpora OSPFv2, OSPFv3, BGP; Podpora PIM-SM Podpora IGMPv2 alebo IGMPv3 ; Podpora IKEv1 aj IKEv2; Podpora SHA-2 (256, 384 aj 512 bitový hash); Podpora dvojfaktorovej autentifikácie; Podpora IPSec SuiteB (RFC 6379); Mapovanie VPN klientov do VLAN na základe skupinovej politiky; Podpora IPv6 a filtrovanie IPv6 prevádzky; Natívna podpora IPv6 pre IPSec a SSL VPN; Podpora NAT44, NAT46, NAT64, NAT66; Podpora inšpekcie min. týchto protokolov – DCERPC, DNS, FTP, H.323, HTTP, ICMP, LDAP, SIP, SMTP/ESMTP; Selektívne priradenie dátových tokov rôznym inšpekčným "engine" pre maximálnu efektivitu využitia výkonu firewall-u; Ochrana proti IP Spoofing; Nastavovanie parametrov jednotlivých spojení s min. podporou nasledujúcich parametrov – max počet spojení jedného klienta, max počet „embryonic" spojení jedného klienta, nastavenie doby trvania jednotlivých spojení jedného klienta; Podpora TCP normalizácie, TCP intercept a randomizácie TCP sekvenčných čísiel; Podpora „identity-based" firewall spolu s Windows AD alebo LDAP; Filtrovanie na základe geolokácie, objektov a bezpečnostných zón; Podpora aplikačnej inšpekcie a rozpoznávania min. 3000 rôznych aplikácií. Definície nových aplikácií musia byť dostupné bezplatne počas trvania servisnej zmluvy. Firewall musí rozpoznávať serverové aj klientské operačné systémy, aplikácie na serveroch aj klientských staniciach, sieťové protokoly, otvorené TCP a UDP porty, ako aj prihlásených používateľov. Odomknutie IPS funkcií aplikovaním licencie. Podpora reputačného filtrovania IP adries a domén s možnosťou integrácie na reputačné zoznamy tretích strán; Podpora IDS aj IPS režimu; Rozpoznávanie útokov od sieťovej až po aplikačnú vrstvu referenčného modelu OSI pre IPv4 aj IPv6; Podpora signatúr písaných pre Snort; Mapovanie signatúr na CVE (Common Vulnerabilities and Exposures) False positive menej ako 1%; Podpora Indications of Compromise; Podpora normalizácie protokolovými dekódermi pre DCE/RPC, DNS, FTP, HTTP, SIP, IMAP, POP, SMTP, SSH a SSL; Na základe informácií o bezpečnostných slabinách operačných systémov a aplikácií rozpoznaných v sieti musí centrálny manažment navrhnúť, ktoré signatúry majú byť zapnuté, aby bolo prostredie aktívne chránené; Centrálny manažment musí rozpoznať, ktoré signatúry nie je potrebné aktivovať a ich vypnutím docieliť lepšie využitie výkonu sond pre aktívne používané signatúry; Centrálny manažment musí byť schopný kategorizovať prebiehajúce útoky tak, aby bol administrátor prednostne upozornený na útoky vedené voči zraniteľným systémom; Signatúry musia byť k dispozícii do 48 hodín od zverejnenia bezpečnostnej chyby; IPS musí chrániť prostredie od známych aj tzv. "day-zero" útokov (IPS musí analyzovať správanie sa dátových tokov, aby bolo možné detekovať aj útoky, ktoré sa bežnými mechanizmami nedetekujú); Typy odpovedí na detekované útoky zo strany IPS sond - min. alarm do centrálneho manažmentu, ukončenie spojenia, zahadzovanie paketov, ukladanie obsahu paketov, interaktívna HTTP odpoveď; Manažment musí umožniť definovanie korelačných politík pre automatické upozornenie administrátora IPS, že sa útočník snaží zneužiť bezpečnostnú dieru v systéme, ktorú ešte správca napadnutého systému nestihol zaplátať. Manažment musí upozorniť správcu aj v prípade, že pripojené koncové zariadenie je v správe CnC (Command-and-Control) servera v Internete Výsledkom korelačnej politiky je min. Syslog, email a NMAP sken. Manažment musí podporovať integráciu s remediačnými nástrojmi tretích strán; Podpora min. týchto QoS funkcií – policing, priority queueing; On box management pre základnú konfiguráciu pri single box nasadení; Firewall priepustnosť pri L7 aplikačnej inšpekcii min.: 830 Mbps; VPN priepustnosť: 250 Mbps; Počet IPSec/SSL VPN peerov: 300 ; Počet súčasných spojení min.: 245 000; Počet nových spojení pri L7 aplikačnej inšpekcii za sekundu: 8 000; min. 1 x AC napájací zdroj ; Montovateľný do 19 palcového racku; Výška max. 1 RU;	HW-B	súbor	1
		b) IPS management:Virtual Appliance vo VMware pre minimalne 2 zariadenia; Management appliance musí podporovať HA; Centrálna dohladová konzola musí poskytovať aktualizáciu a distribúcii filtrov/signatúr automaticky, manuálne a podľa časového harmonogramu; Centrálna dohľadová konzola musí vedieť spravovať operačné systémy IPS systému a aj senzorov; Aktualizácie – nové verzie OS pre management i senzory, opravné patche sa dajú sťahovať automaticky z webu dodávateľa; Aktualizácie je možné na manažment platformu nahrať manuálne; Inštaláciu aktualizácií je možné načasovať a vykonať automaticky; Trendy, historické prehľady a štatistiky z pohľadu aplikácií, staníc, komunikácie, bezpečnostných incidentov sú grafický a tabuľkovo zobrazené v GUI dohľadovej konzoly; Prehľady a štatistiky v dohľadovej konzole je možné filtrovať podľa času, typu incidentov, aplikácií, koncových staníc; V centrálnej dohľadovej konzole je možné vytvárať reporty manuálne a podľa časového harmonogramu; Pre reporty je možné definovať template definujúci formát a obsah reportu; Pre template reportov je možné definovať premennej, ktoré sa premietnu v aktuálnom reporte. V grafickom rozhraní dohľadovej konzoly je možné definovať dashboardy typu top-N; Dashboardy použité v GUI je možné použiť v reportoch; Centrálna dohladová konzola musí byť schopná exportovať reporty do formátov ako PDF, HTML, CSV, apod.; Možnosť integrácie s Microsoft AD pre vytváranie bezpečnostných politík podľa používateľa a skupiny používateľov; Podpora korelácie udalostí na centralizované dohľadovej konzoly s definíciou odpovedajúcich akcii, napr. zaslať korelované udalosti na SIEM, generovanie mailu, lokálne udalosti, a pod; Podpora posielania udalostí formou syslog, email, SNMP na externé platformy; Podpora Event Streamer API (eStreamer) na zdielanie informácií s externými systémami (ArcSight, Splunk) Podpora SMTP autentifikácie pre správy odchadzájúce prostredníctvom SMTP; Podpora JDBC API pre prístup z externých systémov k databázam centralizovaného managementu; Podpora riadeného prístupu podľa rolí administrátorov; Definícia dostupných funkcií v GUI podľa role administrátora; Možnosť založiť „ticket" pre daný incident priamo v manažment GUI; Workflow pre predávanie „ticketov" medzi administrátormi; Možnosť definície politík pre sledovanie parametrov „zdravia" systémov na senzoroch a centralizovanej konzoly (CPU, pamäť, hdd, komunikácia s cloudovými službami, apod.); Zákaznícky definovateľné limity a akcie spojené s ich prekročením pri vyhodnotení sledovaných parametrov „zdravia" systému.; Rôzne politiky pre sledovanie „zdravia" systému možno aplikovať na rôzne senzory, alebo centralizovaný management; Odkaz na CVE a dokumentáciu k známym bezpečnostným incidentom priamo hyperlinkovým odkazom z danej bezpečnostnej udalosti; Možnosť vyhľadávania typu signatúry v centrálnej databáze dodávateľa podľa typu a závažnosti útoku; Podpora vrstiev IPS politík s možnosťou voliť preddefinované politiky v základnej vrstve orientované na bezpečnosť, alebo minimalizáciu falsepositive; Možnosť aplikácie vrstvy doporučených politík, ktorú generuje samotný systém podľa pasívneho sledovania lokálneho prostredia. Možnosť definície používateľskej vrstvy politík; Politiky možno zdieľať a aplikovať na rôzne senzory; Zobrazenie trajektórie malware – pohyb, mutácie, prenosy v sieti medzi stanicami priamo v management GUI.	SW-B	x	x
		2. Dva kusy prepínačov, každý prepínač má min. požiadavky: 24 x 10/100/1000 RJ45 portov a 8 x 10Gbps SFP+ uplink portov. Prepínacia kapacita prepínača musí byť minimálne 200 Gbps, s priepustnosťou minimálne 150 Mpps . Počet VLAN IDmin. 4000, MAC adries min. 32000; Pre daný typ je požadovaná možnosť zapojiť až 8 24 alebo 48 portových prepínačov rovnakého typu do stohu (stack) – jedného logického prepínača alebo ekvivalent v podobe napájania externými napájacími zdrojmi.; Priepustnosť stohovacej zbernice min. 480 Gbps; Pre daný typ je požadované osadenie dvomi napájacími zdrojmi s možnosťou stohovania napájacích zdrojov naprieč prepínačmi v stacku. Prepínač musí podporovať: použitie separátnej inštancie Spanning Tree pre každú VLAN, IEEE 802.1s Multiple Spanning Tree Protocol (MSTP); zamedzenie floodingu broadcastovovej prevádzky na trunkových portoch, automatickú konfiguráciu QoS pre hlas, protokol na automatické vyjednanie trunk portu; protokol zabezpečujúci detekciu jednosmernej linky a jej následné vypnutie; L3 služby: funkcionalitu vysoko výkonného IP smerovania v hardvéri vďaka jeho architektúre; konfiguráciu statického a možnosť použitia dynamického routovania; protokoly používané v redundantných topológiach na zvýšenie dostupnosti predvolenej brány pre klientské stanice; konfiguráciu DHCP Servera a DHCP relay funkcionality; V rámci bezpečnostných funkcionalít musí podporovať: konfiguráciu protokolu IEEE 802.1x - VLAN, ACL Assignment; protokol CoA, Podpora IEEE 802.1x Multi-Domain Auth with Voice VLAN Assignment; Podpora IEEE 802.1x RADIUS Accounting Podpora IEEE 802.1x with Port Security; Podpora Secure Shell SSH Version 2 Client Support; Podpora IGMP v3 Snoopingu; Podpora mechanizmov na garanciu konzistencie mapovanie MAC adries a IP adries pridelených prostredníctvom DHCP; Podpora ACL (access control list) zoznamov aplikovaných na VLAN a na fyzický port, podpora MACSec protokolu s kryptovanim komunikácie v HW protokolom AES 256.	HW-B	x	x
		3. Router s asynchronnými rozhraniami: Smerovač L3 pre IP sieť. S parametrami ekvivalentnými, alebo lepšími: Hustota portov 2 x 10/100/1000 (1 SFP); 32 asynchronných rozhraní s káblami ukončenými koncovkami RJ45, 1 x ISC slot.	HW-B	x	x

		4. Diskové pole: Univerzálne diskové pole SAN/NAS, s momentálnym využitím pripojenia cez iSCSI protokol. Riadiaca jednotka poľa je osadená redundatne dvomi kontrolermi, ktoré sú v klastrovom prepojení, čím vytvárajú ucelený prvok. Pole je osadené internými 24x 1,2TB SAS diskami. Toto riešenie zaberá najviac 2RU. V prípade potreby do budúcnosti sa musí dať pole rozšíriť o ďalšie SSD, SAS alebo NL-SAS disky. Architektúra diskového poľa má dovoliť voliteľnú kombináciu rýchlych SSD diskov a rotačných diskov. Podpora diskov s kapacitou min. 900GB, 1.2TB, 1.8TB SAS, 960GB, 3.84TB, 15.3TB SSD, 800GB SSD, 3.8TB SSD, 1.8TB 10K RPM AES-256, FIPS 140-2 compliant, prípadne iné typy diskov s rozširujúcimi policami. Požadovaná konektivita je 4 x 10Gb SFP+ na každom kontroleri, s možnosťou voliteľne definovať režim portov FC alebo Ethernet súčasne. Onboard 2x12Gb SAS/kontroler Redundantné napájacie zdroje a chladiace ventilátory. Pri voliteľnej konfigurácii poľa možnosť dosiahnuť až 99,999% dostupnosť. S funkciou automatickej obnovy dát v prípade výpadku diskovej jednotky. Systémová polica v prevedení 2RU a s kapacitou min.24 diskov v kombinacii SSD a SAS Možnosť voliteľného rozšírenia kapacity poľa až na 1243 TB pri rozšírení o diskové police. Možnosť voliteľne rozširovať počet diskov až do 144 diskov pri kombinácií rôznych typov políc. Špecifikácia (Active-Active Dual Controller) Minimum supported drives (HDD/SSD) 144 Minimum supported raw capacity 1243TB Minimum onboard NVMe Flash 1TB Minimum supported SSD-based cache 24TB Maximum Controller form factor 2U Minimum ECC memory 64GB Minimum NVRAM 8GB Min. Onboard I/O: UTA 2 (8/16Gb FC/FCoE/10GbE/1GbE) 8 Onboard I/O: 10GbE 4 Minimum Onboard I/O: 12Gb SAS 4 Storage protocols supported FC, FCoE, iSCSI, NFS, pNFS, CIFS/SMB Host/client operating systems supported Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows XP, Linux, Sun Solaris, AIX, HP-UX, Mac OS, VMware, ESX x x Diskové pole musí podporovať: - Akceleráciu read operácií formou dedikovanej onboard flash pamate s velkosťou min 1TB. - Automaticlý tiering v reálnom čase, čo znamená, okamžité vyhodnocovanie a ukladanie HOT blokov na dedikované SSD disky až do kapacity 24TB bez potreby zásahu administrátora. - Možnosť automatického tieringu do cloudu cez S3 protokol. - Virtualizáciu kontrolerov poľa, čo znamená, že umožňuje pridať ďalšie pole do klastra, obe polia sa potom voči administrátorovi budú správať ako jedno jediné pole. Zároveň umožňuje vytvárať virtuálne storage kontrolery s priradenými dátovými volumami, protokolom, IP adresou, nezávislým administrátorským prístupom, nadefinovanými QoS parametrami. Umožňuje tak vytvárať bezpečné a izolované „multitennant prostredie". - Podpora min. 1023 snapshotov/volume bez ovplyvnenia výkonu poľa. - Podporované protokoly: FC, FCoE, iSCSI, NFS, pNFS, CIFS/SMB - Podpora škálovatelnosti - klastrovanie: Pre NAS/ SAN.....min. 4 polia(8 kontrolerov) - Podpora snapshotov a klonov volumov prostriedkami diskového poľa. - Podpora používania viacerých komunikačných protokolov súčasne - Podpora Thin-provisioned volumov - In-line deduplikácia, kompresia a kompakcia. - Možnosť využitia SSD časti ako cache - Podpora on-line zvyšovania kapacity už existujúcich volumov - Redundantné kontrolery na zariadeniach s podporou pripojenia aktiv/aktiv - Pevné disky, zdroje napájania a ventilátory musia byť vymeniteľné za chodu (HotSwap) - Redundantné napájanie z rackového PDU Podpora RAID – level : - RAID-TEC™ - alebo podobné (ochrana vysoko kapacitných diskov , proti výpadku 3 diskov) - RAID 6 (RAID-DP®) - RAID 4 - RAID 6 + RAID 1 or RAID 4 + RAID 1 x x Požadovaná rýchlosť I/O operácií na úrovni RAID 10 pri zachovaní ochrany dát proti výpadku ľubovoľných dvoch diskov. Pri veľkokapacitných diskoch (4TB a väčšia kapacita jedného disku) ochrana proti výpadku troch ľubovoľných diskov Príslušné licencie a všetky podporované dátové protokoly musia byť súčasťou ponuky bez kapacitného obmedzenia. Podporované operačné systémy: Windows® 2000, Windows Server® 2003, Windows Server 2008, Windows Server 2012, Windows XP, Linux®, Oracle® Solaris, AIX, HP-UX, Mac® OS, VMware®, ESX	HW-B	x	x
		5. a) 10 Gbps káble : 6 x 10GBASE-CU SFP+ Cable 3 Meter; 4 x 10GBASE-CU SFP+ Cable 5 Meter;	-	x	x
		6. SW licencie: VM – zabezpečenie web komunikáci, VM – zabezpečenie elektronickej pošty , Advanced Malware Portection – koncové zariadenia. Musí umožňovať inštaláciu až 10 inštancií VM. a) web systém: VM: zabezpečenie komunikácie užívateľov na web servery, kontrola reputácie cieľovej URL v cloude, možnosť kontroly malwaru prostredníctvom dvoch nezávislých Anti-Malware systémov, URL filtering, možnosť definovania vlastných URL kategórii, rozpoznávanie komunikácie na základe user-agent hlavičky, možnosť obmedzovania komunikácie na požadovanú rýchlosť na média (napríklad YouTube), možnosť riadenia komunikácie na web aplikácie (napríklad systém musí umožňovať blokovať upload fotiek na Facebook Licenčná politika musí podporovať súčasnú inštaláciu systému až na 10 pracovísk. b) e-mail systém : VM – zabezpečenie elektronickej pošty. Systém musí rozpoznávať Spam na základe reputácie IP adresy (kontrola reputácie sa vykonáva v cloude) a vstavaný anti-spamovým enginom. Systém musí podporovať možnosť kontroly poštových správ viacerými nezávislými Anti-Malware systémami, z ktorých aspoň jeden bude mať možnosť kontrolovať malware na základe vzoriek, ktoré sa nachádzajú priamo na systéme a aspoň jeden podporovaný Anti-malware system bude typu „cloud-based". Systém musí vedieť kontrolovať a v prípade požiadavky blokovať rôzne súbory prenášané elektronickou poštou. Systém musí vedieť vyhodnotiť odkazy URL, ktoré môžu byť súčasťou elektronickej správy prostredníctvom URL filtering funkcionality a URL reputácie. Licenčná politika musí podporovať súčasnú inštaláciu systému až na 10 pracovísk. c) Advanced Malware Portection - Ochrana pracovných staníc : Anti-Malware systém pre koncové stanice musí umožňovať prezentáciu funkcionality na základe offline vzoriek a aj na základe vyhodnocovania vzoriek voči cloudovej službe. Systém musí tiež poskytovať „retrospektívne" informácie (systém musí mať možnosť dodatočnej identifikácie malwaru v súbore, ktorý pôvodne systém nevedel ohodnotiť či obsahuje malware alebo nie a poskytnúť tieto informácie administrátorovi). Systém musí umožňovať zobrazenie činnosti malwaru na pracovnej stanici, prípadne výskyt súboru obsahujúceho malware na ďalších pracovných staniciach.	SW-B	x	x
		7. Server pre spúšťanie centrálnych VM: Dvojsoketový rackmount server s x86 architektúrou procesora s možnosťou osadiť len jeden socket jedným procesorom. HW špecifikácia osadených komponentov s min. požiadavkami: osadený 2 x 12 jadrový CPU s clockrate s minimálne 2.60GHz s publikovanou hodnotou PassMark High End CPU benchmarku https://www.cpubenchmark.net/ aspoň 19500 CPU Mark ku dňu vydania výzvy, 128GB DDR4 2666 MHz RAM, 3 x 2.5" 12G 1.2TB SAS HDD disk s10K RPM, 2 x 2.5" 12G 300GB HDD SAS disky s 10K RPM, sieťová konektivita 2x 40Gbps QSFP , 2x AC zdroj, 1x RAID controller s 12Gbps rýchlosťou pripojenia na disky a minimálne podporou RAID 5,6,50,60 a možnosťou riadenia až 16 SAS/SATA diskov, Vstavaná management webová aplikácia poskytujúca vzdialený manažment servera, virtuálne KVM (KVM over IP) a virtuálne médium (vCD, vDVD) za účelom vzdialenej inštalácie operačného systému, 2 x 1Gbit vstavané ethernetové sieťové porty, 2 x USB 3.0 port, VGA video port DB-15, sériový port RJ-45, 1 x 1Gbps management port pre Out-of-Band pripojenie na vstavanú management webovú aplikáciu servera, 2 sloty pre vymeniteľné AC zdroje bez potreby vypínania servera (hot-swap), 8 slotov pre 2,5" HDD disky s podporou výmena HDD disku bez potreby vypnutia servera (hot-swap), 2x slot pre SD karty s minimálnou podporovanou kapacitou SD karty 32GB, Podpora RAID controllera s rýchlosťou aspoň 12Gbps, prevedenie maximálne 1RU s kořajnicami umožňujúcimi vysunutie servera z dátovej skrine, na prednej strane servera osadený KVM konektor s ponúkanou konektivitou aspoň 2x USB (aspoň 2.0), 1x VGA a 1x sériový port. Súčasťou servera musí byť OS. Pre zabezpečenie funkcionality celkového riešenia je potrebné navrhnúť OS pre testovací server tak, aby umožnil vykonať požadovanú funkcionalitu podľa špecifikácie učebných tém.	HW-B	x	x
		8. Server pre spúšťanie VM pracovísk: Dvojsoketový rackmount server s x86 architektúrou procesora s možnosťou osadiť len jeden socket jedným procesorom. HW špecifikácia osadených komponentov s min. požiadakami: osadený 2 x 16 jadrový CPU s clockrate s minimálne 2.60GHz s publikovanou hodnotou PassMark High End CPU benchmarku https://www.cpubenchmark.net/ aspoň 27500 CPU Mark ku dňu vydania výzvy, 6x 32GB DDR4 2666 MHz RAM, 2 x 2.5" 12G 2TB HDD disk s 7,2K RPM, 2 x 2.5" 12G 300GB HDD disky s 10K RPM, sieťová konektivita 2x 40Gbps QSFP , 2x AC zdroj, 1x RAID controller s 12Gbps rýchlosťou pripojenia na disky a minimálne podporou RAID 5,6,50,60 a možnosťou riadenia až 16 SAS/SATA diskov. Vstavaná management webová aplikácia poskytujúca vzdialený manažment servera, virtuálne KVM (KVM over IP) a virtuálne médium (vCD, vDVD) za účelom vzdialenej inštalácie operačného systému, 2 x 1Gbit vstavané ethernetové sieťové porty, 2 x USB 3.0 port, VGA video port DB-15, sériový port RJ-45, 1 x 1Gbps management port pre Out-of-Band pripojenie na vstavanú management webovú aplikáciu servera, 2 sloty pre vymeniteľné AC zdroje bez potreby vypínania servera (hot-swap), 8 slotov pre 2,5" HDD disky s podporou výmena HDD disku bez potreby vypnutia servera (hot-swap), 2x slot pre SD karty s minimálnou podporovanou kapacitou SD karty 32GB, Podpora RAID controllera s rýchlosťou aspoň 12Gbps, prevedenie maximálne 1RU s kořajnicami umožňujúcimi vysunutie servera z dátovej skrine , na prednej strane servera osadený KVM konektor s ponúkanou konektivitou aspoň 2x USB (aspoň 2.0), 1x VGA a 1x sériový port. Súčasťou servera musí byť OS. Pre zabezpečenie funkcionality celkového riešenia je potrebné navrhnúť OS pre testovací server tak, aby umožnil vykonať požadovanú funkcionalitu podľa špecifikácie učebných tém.	HW-B	x	x
		9. VM - AAA server : Typ : Min. 1 x VM prevádzkované v prostredí VMware ESX/ESXi 5.x, hardvérové nároky na server podľa odporúčaní výrobcu Výkonnostné parametre: Licencia pre všetky požadované funkcie pre min. 100 používateľov Bezpečnosť : Plnohodnotná AAA funkcionalita – autentizácia používateľov, machine authentication, autorizácia a logovanie činnosti Integrované funkcie AAA pre pripojenie z LAN, Wifi aj VPN Podpora bezpečnostných politík na princípe používateľských rolí a ich oprávnení Autorizácia prístupu do siete kombináciou min. nasledujúcich parametrov – identita (meno/heslo, certifikát) pripájajúceho sa používateľa, identita (MAC adresa, profilácia, certifikát) pripájajúceho sa zariadenia, čas pripojenia do siete, miesto pripojenia do siete a spôsob pripojenia do siete (wifi/LAN/VPN) Kategorizácia zariadení na základe min. RADIUS, DHCP, HTTP, NMAP, SNMP, DNS Musí obsahovať preddefinované kategórie zariadení (min. IP telefóny, bezdrôtové prístupové body, windows desktop, MAC, Linux, iPhone. iPAD, Android, atď.) Podpora RADIUS, RADIUS Proxy a RADIUS CoA (Change of Authorization) Podpora min. týchto databáz identít – LDAP, Active Directory, RSA tokeny a RADIUS kompatibilných token serverov Podpora Guest prístupu z LAN aj Wifi Podpora kontroly obsahu koncovej stanice, MDM Dedikovaný portál pre správcu guest účtov Dedikovaný portál pre webovú autentifikáciu guest používateľov Podpora LDAP cez SSL Podpora min. týchto EAP metód – EAP-MSCHAPv2, EAP-TLS, PEAP, EAP-MD5, EAP-GTC Podpora autentifikácie pre klientov nepodporujúcich 802.1x (MAB, webová autentifikácia) Podpora kombinovanej funkcionality pre AAA, Guest Access, registráciu koncových zariadení (aj s vydaním certifikátu) v jednom a tom istom softvéri Manažment: Manažment cez HTTPS Podpora API rozhrania z možnosťou CRUD (create, read, update, delete) operácií Podrobný reporting - min. pripojené zariadenia a ich používatelia, autorizovaní aj neautorizovaní používatelia a ich zariadenia, guest používatelia a ich doba pripojenia v sieti, systémové zdroje Logovanie činnost, úspešných aj neúspešných pokusov o prihlásenie v reálnom čase Pre každý pokus o prihlásenie musí systém uchovať presné a podrobné informácie o priebehu pripojenia od počiatočného pokusu (napr. EAPoL-Request-Identity) až po povolenie/zakázanie pripojenia (napr. RADIUS Access-Accept/Access-Reject) Podpora vyhľadávania v systéme Podpora auditu konfigurácií NAD zariadení v súlade s "best practise" odporúčaniami	SW-B	x	x
		10. Dokumentácia. Musí byť vytvorená a odovzdaná v podobe PDF súborov na digitálnom nosiči v slovenskom jazyku a v podobe webovej aplikácie v slovenskom jazyku. Celkový počet požadovaných labov je min. 18. Pod pojmom LAB sa rozumie učebná téma. Každý LAB musí mať rozdelenie na teoretickú a praktickú časť. Teoretická časť labov musí min. obsahovať: · popis zraniteľných miest sieťových a aplikačných systémov, · teoretický popis útokov na zraniteľné miesta, · popis praktickej realizácie útokov na uvedené zraniteľné miesta, · popis spôsobu ochrany voči týmto útokom spolu s názornými príkladmi konfigurácie sieťových a bezpečnostných systémov. Praktická časť labov musí min. obsahovať: · Stručný popis každého testovaného scenára (labu) a jeho cieľ · Topológiu labu · Presný postup realizácie labu: o popis zapojenia labu, o popis prípravných prác, o popis krokov pre samotnú realizáciu labu (kroky popisujúce prácu s aplikáciami, konfiguráciu zariadení, testovanie funkcionality a podobne) Prípravné práce na jednotlivých laboch : Príprava imagov OS serverov a pracovných staníc pre jednotlivé laby (príprava OS pre pracovné stanice a pre virtuálne prostredie), príprava konfiguračných súborov na jednotlivé sieťové zariadenia a systémy pre jednotlivé laby. Laby a ich tématický obsah: 1. Útoky a ich eliminácia na druhej vrstve OSI modelu – 2 laby a. Útok na DHCP a ARP protokol a ochrana. Ukážka útoku „man-in-the-middle" b. Útok na CAM table prepínačov a útok na VLAN siete 2. Riadenie komunikácie na hranici sieti – 1 lab a. Scanovanie siete, identifikácia spustených služieb, zariadení a operačných systémov b. Komunikačné pravidlá a ich dôležitosť pre elimináciu možných útokov 3. Útoky na e-mail komunikáciu a zabezpečenie e-mail komunikácie – 2 laby a. SPAM a ochrana užívateľov pred nevyžiadanou poštou b. Podvrhnutie e-mail komunikácie c. Phishing a Pharming d. Šírenie malwaru cez e-mail komunikáciu x x 4. Zabezpečenie komunikácie na web stránky – 2 laby a. Problém nerideného prístupu na web stránky, hrozba infiltrácie malwarom b. Kontrola prístupu k súborom cez http a HTTPS protokoly – kontrola „downloadu" c. Zraniteľné miesta web prehliadačov d. Útoky cez „aktívny" obsah web stránok – Java aplikácie, Flash aplikácie, možnosť blokovania aktívneho obsahu 5. Útoky na zraniteľné miesta bežne používaných sieťových služieb – 2 laby a. Zraniteľné miesta aplikácii – ukážka BOF útoku na web server a získanie prístupu útočníka na tento server b. Ochrana pred BoF útokmi – Intrusion Prevention Systems 6. Útoky na aplikácie prevádzkované na web serveroch – 1 lab a. Útoky na web aplikácie a ich špecifikácie b. Ochrana web aplikácii použitím aplikačných firewallov 7. Útoky na „clear textové" protokoly – 2 laby a. Odpočúvanie komunikácie, „man-in-the-middle" útoky, prenos údajov cez nezabezpečenú sieť b. Princípy dôveryhodnosti, zachovania integrity a autentičnosti prenášaných údajov c. Kryptovanie komunikácie, IPSec protokol 8. DoS útoky – 1 lab a. Druhy DoS a DDoS útokov b. Testovanie IP spoofing a Syn flood útokov c. Ochrana pre DoS útokmi 9. Autentifikácia prístupu užívateľov, auditovateľnosť prístupov - 2 laby a. Dôležitosť používania silných autentifikačných metód pri prístupe k dôležitým aktívam b. „Lámanie" hesiel na operačných systémoch a sieťových zariadeniach c. Používanie certifikátov 10. Útoky na wifi siete – 1 lab a. Zabezpečené vs nezabezpečené wifi siete b. Testovanie neautorizovaného prístupu do wifi siete c. Odporúčané protokoly pre prevádzkovanie wifi siete x x 11. Malware – 1 lab a. Spôsoby infikovania OS počítačov, druhy malwaru b. Trendy v zabezpečení voči malwaru 12. BOT siete – 1 lab a. Popis BOT sietí b. Spôsob identifikácia počítačov komunikujúcich s BOT sieťou. **Pod pojmom LAB sa rozumie učebná téma. Obsahovú náplň okruhov učebných tém tvorí nasledovný opis:**	-	x	x
		1. Útoky a ich eliminácia na druhej vrstve OSI modelu Všeobecný popis útokov na L2 vrstve a útok na DHCP protokol, ktoré je možné realizovať na vnútornej LAN sieti v prípade, že nie sú korektne nakonfigurované sieťové prepínače a ostatné aktívne prvky LAN siete. Útok na ARP protokol a možnosti jeho eliminácie. Útok na tabuľku MAC adries a možnosti eliminácie útoku. Ďalšie útoky na VLAN siete a ich eliminácia. Útoky na Spanning Tree protokol a zabezpečenie tohoto protokolu. Téma: Útok na DHCP a ARP protokol a ochrana. Ukážka útoku „man-in-the-middle" 1 hodina teória, 2 hodiny praktická časť Návod na realizáciu útokov na DHCP a ARP protokoly vrátane ich praktickej realizácie. Konfigurácia prepínača za účelom eliminácie útokov na DHCP a ARP protokoly. Otestovanie zabezpečenia. Téma: Útok na CAM table prepínačov a útok na VLAN siete 1 hodina teória, 2 hodiny praktická časť Popis realizácie VLAN hopping útoku a VLAN spoofing útoku. Návod na realizáciu útoku na CAM tabuľku a jeho praktické otestovanie. Konfigurácia prepínača za účelom eliminácie útokov na CAM tabuľku. Otestovanie zabezpečenia.	-	x	x
		2. Riadenie komunikácie na hranici sieti Čo sa môže stať ak pripojíme vnútornú LAN sieť do siete Internet na priamo, bez zabezpečenia? Aké služby sú bežne zapnuté na Microsoft Windows serveri vo funkcii doménového kontroléra? Prehľad najčastejších a najkritickejších zraniteľnosti na Windows serveroch, stručný prehľad. Popis ako je možné tieto zraniteľnosti zneužiť. Význam riadenia komunikácie na hranici LAN siete a siete Internet. Druhy firewallov a ich použitie. Téma: Scanovanie siete, identifikácia spustených služieb, zariadení a operačných systémov 1 hodina teória, 2 hodiny praktická časť Oboznámenie sa s nástrojmi na scanovanie siete. Techniky scanovania sietí, spustených služieb a operačných systémov. Praktické scanovanie dostupných zariadení na sieti a služieb Windows servera. Interpretácia výsledkov. Téma: Komunikačné pravidlá a ich dôležitosť pre elimináciu možných útokov 1 hodina teória, 2 hodiny praktická časť Aké služby sú bežne zapnuté na Microsoft Windows serveri vo funkcii doménového kontroléra? Prehľad najčastejších a najkritickejších zraniteľnosti na Windows serveroch, stručný prehľad. Popis ako je možné tieto zraniteľnosti zneužiť. Význam riadenia komunikácie na hranici LAN siete a siete Internet. Druhy firewallov a ich použitie. Ukážka prieniku do siete, ktorá nie je chránená hraničným zariadením. Praktická ukážka zneužitia zraniteľnosti windows servera. Aplikovanie komunikačných pravidiel medzi LAN sieťou a vonkajšou sieťou. Scanovanie siete po aplikovaní pravidiel, opätovné overenie zraniteľnosti Windows servera.	-	x	x

		3. Útoky na e-mail komunikáciu a zabezpečenie e-mail komunikácie Email komunikácia ako jeden z hlavných zdrojov infiltrácie. Druhy útokov realizovaných prostredníctvom emailovej komunikácie. Spôsoby a metódy zabezpečenia email komunikácie. Téma: SPAM a ochrana užívateľov pred nevyžiadanou poštou. Podvrhnutie e-mail komunikácie. 1 hodina teória, 2 hodiny praktická časť Popis bežne používaných anti SPAM riešení a praktická ukážka ich konfigurácie. Ukážka podvrhnutia email komunikácie. Prevencia pred podvrhnutím mailovej komunikácie, vysvetlenie pojmov SPF, DKIM, DMARC Téma: Phishing a Pharming útoky. Šírenie malwaru cez e-mail komunikáciu. 1 hodina teória, 2 hodiny praktická časť Vysvetlenie útokov Phishing a Pharming. Praktická ukážka Phishing mailu. Blokovanie malwaru v mailovej komunikácii. Praktické otestovanie blokovania malwaru v správe.	-	X	X
		4. Zabezpečenie komunikácie na web stránky Účel a význam web proxy serverov. Popis používaných bezpečnostných funkcionalít web proxy serverov. Účel URL filteringu. Zabezpečenie komunikácie na HTTPS stránky. Téma: Problém neriadeného prístupu na web stránky, hrozba infiltrácie malwarom. Kontrola prístupu k súborom cez HTTP a HTTPS protokoly – kontrola „downloadu“ 1 hodina teória, 2 hodiny praktická časť Účel a význam web proxy serverov Praktické otestovanie blokovania prístupu na nežiadúce web stránky prostredníctvom URL filter funkcionality. Praktické otestovanie blokovania downloadu vybraných typov súborov. Praktické otestovanie downloadu súboru obsahujúceho malware. Zabezpečenie prístupu na HTTPS stránky. Téma: Zraniteľné miesta web prehliadačov, útoky cez „aktívny“ obsah web stránok – Java aplikácie, Flash aplikácie, možnosť blokovania aktívneho obsahu 1 hodina teória, 2 hodiny praktická časť Praktická ukážka možnosti spustenia škodlivého kódu pri prístupe na web stránku bez interakcie užívateľa.	-	X	X
		5. Útoky na zraniteľné miesta bežne používaných sieťových služieb Príklady zraniteľností bežne používaných sieťových služieb a aplikácii. Oboznámenie sa s dostupnými databázami zraniteľností, ich význam a použitie. Ochrana pred útokmi na známe zraniteľnosti služieb a aplikácii. Téma: Zraniteľné miesta aplikácii – ukážka BOF útoku na web server a získanie prístupu útočníka na tento server 1 hodina teória, 2 hodiny praktická časť Popis buffer over flow útoku na vybranú aplikáciu alebo službu. Praktické otestovanie BOF útoku. Téma: Ochrana pred BoF útokmi – Intrusion Prevention Systems 1 hodina teória, 2 hodiny praktická časť Úvod do Intrusion Prevention Systémov. Konfigurácia IPS systému na NGFW za účelom blokovania známych zraniteľností. Praktické otestovanie zabezpečenia, ukážka zablokovania útoku IPS systémom.	-	X	X
		6. Útoky na aplikácie prevádzkované na web serveroch Popis komunikačných protokolov HTTP a HTTPS. Popis najčastejších útokov na web aplikácie. Spôsoby zabezpečenia web serverov a aplikácii. Téma: Útoky na web aplikácie a ich špecifikácie b. Ochrana web aplikácii použitím aplikačných firewallov 1 hodina teória, 2 hodiny praktická časť Popis komunikačných protokolov HTTP a HTTPS. Popis najčastejších útokov na web aplikácie. Spôsoby zabezpečenia web serverov a aplikácii. Praktické otestovanie útokov SQL injection a Cross site scripting na web aplikáciu. Realizácia zabezpečenia web aplikácie prostredníctvom web aplikačného firewallu. Praktické overenie zabezpečenia.	-	X	X
		7. Útoky na „clear textové“ protokoly Bežne používané „clear textove“ aplikácie, služby a ich zraniteľnosti. Popis možností zneužitia prenášaných informácii pre účely útočníka. Význam pojmov integrita a dôveryhodnosť. Aplikácie a služby využívajúce autentifikovaný a kryptovaný prenos údajov. Téma: Odpočúvanie komunikácie, „man-in-the-middle“ útoky, prenos údajov cez nezabezpečenú sieť 1 hodina teória, 2 hodiny praktická časť Bežne používané „clear textove“ aplikácie, služby a ich zraniteľnosti. Popis možností zneužitia prenášaných informácii pre účely útočníka Praktická časť: Ukážka „man in the middle“ útoku a získanie citlivých informácii z odchytených nezabezpečených prenášaných údajov. Téma: Princípy dôveryhodnosti, zachovania integrity a autentičnosti prenášaných údajov. Kryptovanie komunikácie, IPSec protokol 1 hodina teória, 2 hodiny praktická časť Praktická ukážka používania kryptovanej komunikácie a služieb. Význam pojmov integrita a dôveryhodnosť. Aplikácie a služby využívajúce autentifikovaný a kryptovaný prenos údajov.	-	X	X
		8. DoS útoky Popis cieľov DoS (Denial of service) a DDoS (Distributed denial of service) útokov. Uvedenie a popísanie najznámejších druhov DoS a DDoS útokov. Príklady Dos a DDos útokov z praxe. Realizácia Ochrana pred DoS a DDoS útokmi. Téma: Druhy DoS a DDoS útokov, testovanie IP spoofing a Syn flood útokov, Ochrana pre DoS útokmi 1 hodina teória, 2 hodiny praktická časť Popis cieľov DoS a DDoS útokov. Uvedenie a popísanie najznámejších druhov DoS a DDoS útokov. Praktické otestovanie DoS útoku na server s OS Windows. Testovanie SynFlood útoku . Praktická ukážka realizácie zabezpečenia voči SynFlood útokom.	-	X	X
		9. Autentifikácia prístupu užívateľov, auditovateľnosť prístupov Popis bežne používaných autentifikačných protokolov. Používané princípy na zabezpečenie hesiel v rôznych operačných systémoch. Metódy a nástroje používané na „password cracking“. Popis dvojfaktorovej a viacfaktorovej autentifikácia. Používanie certifikátov pre prístup k aplikáciam a službám. Téma: Dôležitosť používania silných autentifikačných metód pri prístupe k dôležitým aktívam, „lámanie“ hesiel na operačných systémoch a sieťových zariadeniach 1 hodina teória, 2 hodiny praktická časť Popis bežne používaných autentifikačných protokolov. Používané princípy na zabezpečenie hesiel v rôznych operačných systémoch. Metódy a nástroje používané na „password cracking“. Praktická ukážka získania hesla pri Telnet protokole použitím „man in the middle“ útoku. Nástroje a metódy používané pre „lámanie“ hesiel. Praktická ukážka „crackovania“ hesla v OS windows Téma: používanie certifikátov pre autentifikáciu a autorizáciu 1 hodina teória, 2 hodiny praktická časť Popis dvojfaktorovej a viacfaktorovej autentifikácia. Používanie certifikátov pre prístup k aplikáciam a službám. Praktická časť Vygenerovanie žiadosti o vydanie certifikátu Otestovanie importu a exportu certifikátov Autentifikácia prostredníctvom certifikátov pri vzdialenom prístupe do LAN siete použitím RA VPN klienta.	-	X	X
		10. Útoky na wifi siete Všeobecný popis zabezpečenia wifi sietí. Porovnanie protokolov WEP, WPA, WPA2 a WPA3. Používané spôsoby autentifikácie pri prístupe do wifi sietí. Téma: Zabezpečené vs nezabezpečené wifi siete. Testovanie neautorizovaného prístupu do wifi siete. Odporúčané protokoly pre prevádzkovanie wifi siete 1 hodina teória, 2 hodiny praktická časť Všeobecný popis zabezpečenia wifi sietí. Porovnanie protokolov WEP, WPA, WPA2 a WPA3. Používané spôsoby autentifikácie pri prístupe do wifi sietí. Praktická konfigurácia zabezpečenia wifi siete protokolom WEP. Ukážka útoku na wifi sieť používajúcu WEP protokol. Konfigurácia zabezpečenia wifi siete protokolom WPA. Ukážka útoku na wifi sieť používajúcu WPA protokol.	-	X	X

		11. Malware História malwaru a jeho vývoj. Zoznámenie sa s rôznymi druhmi malwaru. Techniky identifikácie malwaru. Anti malwarové systémy. Téma: Spôsoby infikovania OS počítačov, druhy malwaru, trendy v zabezpečení voči malwaru 1 hodina teória, 2 hodiny praktická časť História malwaru a jeho vývoj. Zoznámenie sa s rôznymi druhmi malwaru. Techniky identifikácie malwaru. Anti malwarové systémy. Praktická časť Spôsoby infikovania operačných systémov malwarom. Ukážka detekovania malwaru AV systémom nainštalovanom na počítačoch. Detekovanie malwaru cloudovou službou.	-	x	x
		12. BOT siete Čo sú BOT siete? Účel BOT sietí. Ako pracujú BOT siete. Príklady BOT sietí. Téma: Popis BOT sietí a spôsob identifikácia počítačov komunikujúcich s BOT sieťou 1 hodina teória, 2 hodiny praktická časť Čo sú BOT siete? Účel BOT sietí. Ako pracujú BOT siete. Praktické vytvorenie BOT siete a následné otestovanie jej funkcionality.	-	x	x
		Webová aplikácia: V navrhnutom riešení sa požaduje najmä publikovanie a správu obsahu vzdelávacích kurzov. Požadované riešenie predpokladá zabezpečenie centralizácie obsahu. Prostredníctvom systému bude umožnené jednoducho publikovať a spravovať obsah vzdelávacích kurzov.. V rámci budovania interaktívnej príručky je potrebné dodržiavať základné architektonické princípy, ktoré budú jednoznačne definovať pravidlá pre procesy, dáta, aplikácie, technológie a bezpečnosť. Pre zabezpečenie požadovaného stavu je potrebné dodržať minimálne nasledovné princípy: • Prístup k obsahu – používatelia majú k dispozícii obsah a služby dostupné v rozsahu pridelených prístupových oprávnení. • Otvorený obsah – určitý obsah bude zverejňovaný ako otvorený. Takýto obsah je voľne dostupný komukoľvek na použitie bez obmedzení autorských práv. Funkčné požiadavky Interaktívna príručka musí obsahovať statický, textový obsah (texty, dokumenty, obrázky, a pod.), interaktívny obsah (interaktívne videá, sekvencie, hovorené slovo, a pod.) a možnosti riadenia vzdelávacích kurzov pre rôzne kategórie používateľov a možnosti ich systematického a efektívneho vzdelávania. Požaduje sa dodanie funkcionalít a obsahu interaktívnej príručky. Interaktívna príručka bude samostatná webová aplikácia pre učiteľov aj študentov. Bude predstavovať grafické webové rozhranie (GUI) prístupné používateľom systému. Verejná časť Verejná časť interaktívnej príručky je určená pre neautentifikovaných anonymných používateľov. V tejto časti sa zobrazujú všeobecne dostupné informácie a obsah vzdelávacích kurzov. Správa obsahu verejnej časti má byť umožnená používateľsky prívetivým spôsobom pomocou redakčného nástroja (Content Management System – CMS). Obsah celej verejnej časti, vrátane mazania a vytvárania nových sekcií musí byť editovateľný intuitívnym a používateľsky prívetivým spôsobom cez CMS bez znalosti webových technológií a jazykov (HTML, JavaScript a pod.) Privátna časť Privátna časť interaktívnej príručky je určená pre editorov (učitelia) a administrátorov systému. Prístup do tejto časti podlieha autentifikácii a následnej autorizácii. Používateľ dostáva právo prístupu len k tým častiam privátneho portálu na ktoré bol autorizovaný na základe jemu priradených rolí. V privátnej časti portálu je možné vykonávať najmä: • upload súborov • download súborov • úpravy a doplňanie obsahu podľa jednotlivých rolí • mazanie dokumentov len administrátor Obsah privátnej časti musí byť editovateľný intuitívnym spôsobom cez CMS bez znalosti webových technológií a jazykov (HTML, JavaScript a pod.) Pre získanie prístupu do privátnej časti bude potrebná registrácia používateľa. Pre prihlásenie do privátnej časti je potrebné zadať platné používateľské údaje – prihlasovacie meno a heslo	-	x	x
		CMS CMS (Content Management System) je komponent alebo systém na správu obsahu, ktorý zabezpečí vkladanie obsahu, úpravu textu a prezentácie obsahu na stránkach Interaktívnej príručky. Všetky úpravy obsahu interaktívnej príručky budú realizované pomocou komponentu CMS. Manažment obsahu (DMS) DMS bude predstavovať komponent správy a riadenia súborov interaktívnej príručky. Bude udržovať všetky súbory na jednom mieste a poskytne ku nim jednoduchý a rýchly prístup bez ohľadu na formát obsahu. Zabezpečí efektívnu podporu používania a bezpečného uchovávania elektronických súborov ako aj funkcie pre správu verzií. Autentifikácia a autorizácia Autentifikácia a autorizácia v interaktívnej príručke umožní kontrolu prístupových práv na úrovni používateľských rolí alebo oprávnení. Nakoľko v interaktívnej príručky bude potrebné riadiť prístup k jednotlivým častiam systému. Súčasťou riešenia musí byť systém na: • vytváranie a evidenciu používateľských profilov, • definovanie a správu používateľských rolí: o editor o administrátor Nefunkčné požiadavky Architektonické požiadavky na návrh riešenia Navrhované riešenie by malo zohľadňovať tieto aspekty: • Doplnenie ďalších funkcií, ktoré nie sú predmetom tohto zadania • Softvérové riešenie nad technológiami s otvoreným zdrojovým kódom • Nezávislosť na platforme na strane klientskych počítačov	-	x	x
		Grafický návrh • Grafický dizajn a HTML kódovanie stránky a jej podstránok (návrh webových stránok a splnenie najnovších štandardov HTML5/XHTML) • Responzívny dizajn s prístupom desktop-first optimalizovanie stránky pre rôzne prehliadače (posledné aktualizované verzie) • Viacjazyčnosť stránky sa nepožaduje • Redakčný systém na správu obsahu webovej stránky obstarávateľom • Tlačidlá pre zdieľanie správ a ďalšieho obsahu na Facebooku a pre zaslanie e-mailom • Zálohovanie všetkých údajov • CMS v slovenskom Jazyku • Zabezpečenie CMS konta užívateľa aspoň 8-znakovým heslom • Logovanie všetkých prístupov (užívateľ, administrátor, neplatné pokusy) do redakčného systému Automatické zablokovanie prístupu do CMS a na FTP po desiatich neúspešných pokusoch • Vyhľadávanie s možnosťou hľadať podľa podstránok Požiadavky na nasadenie do prevádzky Súčasťou dodávky riešenia je zabezpečenie kompletnej inštalácie riešenia do produkčného prostredia obstarávateľa. Od riešenia sa očakáva, že sa výkonnostne nadimenzuje tak, aby dokázal plnohodnotne obslúžiť používateľov podľa nasledovného rozdelenia: • Používatelia privátnej zóny max. 20. • Používatelia verejného portálu sú všetci študenti, ktorí využívajú funkcionalitu daného riešenia, ich počet nie je možné inak obmedziť.	-	x	x
16	**Žiacke pracoviská**	Žiacke pracovisko musí obsahovať min.: 1. Prepínač pre pripojenie pracoviska a testovanie s min. parametrami: 12 x 10/100/1000 portov; 2 x uplink porty 1GE SFP v kombinácii s 10/100/1000 portami; Prepínacia kapacita minimálne 32 Gbps fullduplex, s priepustnosťou minimálne 23,8 Mpps; Počet VLAN ID min. 4000 z toho VLAN aspoň 1000; Podpora jumbo frame až do 9198 bajtov; Napájací zdroj do napájacej siete 230V / 50Hz ; L2 služby: Podpora IEEE 802.1D Spanning Tree; Možnosť použitia separátnej inštancie Spanning Tree pre každú VLAN; Podpora IEEE 802.1s Multiple Spanning Tree Protocol (MSTP); Podpora pre zamedzenie floodingu broadcastovovej prevádzky na trunkových portoch; Automatická konfigurácia QoS pre hlas s automatickou detekciou IP telefónov ktorá automaticky klasifikuje prevádzku a nakonfiguruje výstupnú frontu; Podpora protokolu na automatické vyjednanie trunk portu; Podpora protokolu detekujúceho jednosmernú linku a jej následné vypnutie; L3 služby: Podpora statického a dynamického routovania Podpora protokolu používaného v redundantných topológiach na zvýšenie dostupnosti predvolenej brány pre klientské stanice; Podpora DHCP Servera a DHCP relay; Bezpečnosť: Podpora IEEE 802.1x - VLAN Assignment; Podpora IEEE 802.1x Authenticator Podpora IEEE 802.1x Multi-Domain Auth with Voice VLAN Assignment; Podpora IEEE 802.1x RADIUS Accounting; Podpora IEEE 802.1x with Port Security; Podpora Secure Shell SSH Version 2 Client Support; Podpora IGMP v3 Snoopingu; Podpora mechanizmov na garanciu konzistencie mapovania MAC adries a IP adries pridelených prostredníctvom DHCP; Podpora ACL (access control list) zoznamov aplikovaných na VLAN a na fyzický port;	HW-B	súbor	10
		2. Prepínač pre testovanie L2 útokov: Kompaktný prepínač L2 8 portový PoE s parametrami ekvivalentnými, alebo lepšími: - verzia s 8 x 10/100/1000 portami s podporou PoE+ ; - 2 GigabitEthernet SFP uplink porty + 2 x 10/100/1000 combo porty ; - priepustnosť 24 Gbps full duplex, resp. 17,9 Mpps; - počet aktívnych VLAN min. 255, VLAN ID 4000; - napájací zdroj do napájacej siete 230V / 50Hz ; - 512MB RAM, 128MB Flash pamäť; Manažment cez nástroj s grafickým rozhraním, alebo cez príkazový riadok, vrátane šifrovaného spojenia SSH. Podpora štandardov • IEEE 802.1D Spanning Tree Protocol • IEEE 802.1p CoS Prioritization • IEEE 802.1Q VLAN • IEEE 802.1s • IEEE 802.1w • IEEE 802.1x • IEEE 802.1AB (LLDP) • IEEE 802.3ad	HW-B	x	x
		3. Firewall – IPS funkcionalitou s min . parametrami: 8 x 10/100/1000 RJ-45; 1 x konzolový sériový port; Firewall musí mať možnosť centrálneho GUI menežmentu; Podpora IPSec VPN (Remote Access aj Site-toSite); Podpora SSL VPN (VPN klient) licencia pre 25 klientov; Rozšírenie o URL filtering a Antimalware funkcionalít iba pridaním licencie; Podpora L7 aplikačnej inšpekcii; Podpora IEEE 802.1q, 802.3ad; Podpora min. 5 VLAN; Podpora transparentného režimu; Podpora OSPFv2, OSPFv3, BGP; Podpora PIM-SM; Podpora IGMPv2 alebo IGMPv3; Podpora IKEv1 aj IKEv2; Podpora SHA-2 (256, 384 aj 512 bitový hash); Podpora dvojfaktorovej autentifikácie; Podpora IPSec SuiteB (RFC 6379); Mapovanie VPN klientov do VLAN na základe skupinovej politiky; Podpora IPv6 a filtrovanie IPv6 prevádzky; Natívna podpora IPv6 pre IPSec a SSL VPN; Podpora NAT44, NAT46, NAT64, NAT66; Podpora inšpekcie min. týchto protokolov – DCERPC, DNS, FTP, H.323, HTTP, ICMP, LDAP, SIP, SMTP/ESMTP; Selektívne priradenie dátových tokov rôznym inšpekčným "engine" pre maximálnu efektivitu využitia výkonu firewall-u; Ochrana proti IP Spoofing; Nastavovanie parametrov jednotlivých spojení s min. podporou nasledujúcich parametrov – max počet spojení jedného klienta, max počet „embryonic" spojení jedného klienta, nastavenie doby trvania jednotlivých spojení jedného klienta; Podpora TCP normalizácie, TCP intercept a randomizácie TCP sekvenčných čísiel; Podpora „identity-based" firewall spolu s Windows AD alebo LDAP; Filtrovanie na základe geolokácie, objektov a bezpečnostných zón; Podpora aplikačnej inšpekcie a rozpoznávania min. 3000 rôznych aplikácií. Definície nových aplikácií sú dostupné bezplatne počas trvania servisnej zmluvy; Firewall musí mať možnosť rozpoznávať serverové aj klientské operačné systémy, aplikácie na serveroch aj klientských staniciach, sieťové protokoly, otvorené TCP a UDP porty, ako aj prihlásených používateľov. Odomknutie IPS funkcií aplikovaním licencie; Podpora reputačného filtrovania IP adries a domén s možnosťou integrácie na reputačné zoznamy tretích strán; Podpora IDS aj IPS režimu; Rozpoznávanie útokov od sieťovej až po aplikačnú vrstvu referenčného modelu OSI pre IPv4 aj IPv6; Podpora signatúr písaných pre Snort; Mapovanie signatúr na CVE (Common Vulnerabilities and Exposures); False positive menej ako 1%; Podpora Indications of Compromise Podpora normalizácie protokolovými dekódermi pre DCE/RPC, DNS, FTP, HTTP, SIP, IMAP, POP, SMTP, SSH a SSL; Na základe informácií o bezpečnostných slabinách operačných systémov a aplikácií rozpoznaných v sieti musí centrálny manažment navrhnúť, ktoré signatúry majú byť zapnuté, aby bolo prostredie aktívne chránené; Centrálny manažment musí rozpoznať, ktoré signatúry nie je potrebné aktivovať a ich vypnutím docieliť lepšie využitie výkonu sond pre aktívne používané signatúry; Centrálny manažment musí byť schopný kategorizovať prebiehajúce útoky tak, aby bol administrátor prednostne upozornený na útoky vedené voči zraniteľným systémom; Signatúry musia byť k dispozícii do 48 hodín od zverejnenia bezpečnostnej chyby ; IPS musí chrániť prostredie od známych aj tzv. "day-zero" útokov (IPS musí analyzovať správanie sa dátových tokov, aby bolo možné detekovať aj útoky, ktoré sa bežnými mechanizmami nedetekujú); Typy odpovedí na detekované útoky zo strany IPS sond - min. alarm do centrálneho manažmentu, ukončenie spojenia, zahadzovanie paketov, ukladanie obsahu paketov, interaktívna HTTP odpoveď; Manažment musí umožniť definovanie korelačných politík pre automatické upozornenie administrátora IPS, že sa útočník snaží zneužiť bezpečnostnú dieru v systéme, ktorú ešte správca napadnutého systému nestihol zaplátať. Manažment musí upozorniť správcu aj v prípade, že pripojené koncové zariadenie je v správe CnC (Command-and-Control) servera v Internete; Výsledkom korelačnej politiky je min. Syslog, email a NMAP sken. Manažment musí podporovať integráciu s remediačnými nátrojmi tretích strán; Podpora vlastných IPS signatúr; Podpora min. týchto QoS funkcií – policing, priority queueing; On box management pre základnú konfiguráciu pri single box nasadení; Firewall priepustnosť pri L7 aplikačnej inšpekcii min.: 250 Mbps ; VPN priepustnosť: 100 Mbps; Počet IPSec/SSL VPN peerov: 50; Počet súčasných spojení min.: 20 000; Počet nových spojení pri L7 aplikačnej inšpekcii za sekundu: 3 000; min. 1 x AC napájací zdroj; Montovateľný do 19 palcového racku; Výška max. 1 RU; Správa IPS funkcionality musí byť zabezpečovaná vstavaným menežment systémom, ktorý je nainštalovaný na samotnom firewalle.	HW-B SW-B	x	x
		4. Wireless systém : musí poskytovať možnosť vytvorenia zabezpečenej wifi siete v pásmach 2,4Ghz a 5 GHz a spĺňať štandardy EN 300.328 a EN 301.893. Systém musí minimálne podporovať IEEE štandard 802.11ac Wave 2 3x3 MIMO. Wifi systém musí tiež podporovať protokol 802.1x a umožňovať autentifikáciu minimálne protokolmi PEAP-MSCHAPv2, PEAP-GTC, EAP-FAST a EAP-TLS. Systém musí podporovať PoE napájanie vyhovujúce normám 802.3af/802.3at. Systém musí umožňovať centrálne riadenie (vrátane konfigurácie, pridelovania RF kanálov pre jednotlivé AP, riadenie výkonu vyžarovaného signálu a podobne) až pre 50 kusov access-pointov.	HW-B	x	x
		5. VM - IP LTM a aplikačný firewall s min. parametrami: L4 priepustnosť 10 Mbps; Podpora skriptovacieho jazyka umožňujúceho správu a modifikáciu dátovej komunikácie spracovávanej zariadením, možnosť použitia externých JavaScript knižníc v tomto skriptovacom jazyku; Detekcia a potlačenie L7 DoS útokov aj sieťových DoS/DDoS útokov; Detekcia a potlačenie najčastejších útokov z OWASP (OWASP Top 10); XML Firewall; Ochrana WebSocket komunikácie pomocou WAF; Podpora pre pasívny Fingerprinting zariadení a klientov Detekcia a ochrana voči tz. headless bot-om; SSH Proxy ochrana; Podpora pre tzv. Black Hole filtering pomocou BGP pre IP adresy identifikované ako zdroje útoku; Podpora pre klientsku autentifikáciu pomocou SAML (2.0), Radius, LDAP, MS AD, dvojfaktorovou autentifikáciou; Podpora pre SSO cez viacero domén; Podpora pre Kerberos ticketing; Široká podpora pre natívnych VPN klientov rôznuch operačných systémov (iOS, Mac OS, Windows, Linux, Android); DNS firewall s inšpekciou a validáciou DNS protokolu. Podpora kompletného podpisovania DNSSEC prechádzajúcej komunikácie; Podpora behu autoritatívneho a rekurzívneho DNS servera;	SW-B	x	x

17	**Inštalácia a konfigurácia, zaškolenie pre položky 1 až 14**	Inštalačné a konfiguračné práce a zaškolenie zahŕňajú: (48 h) Rozbalenie a kontrola tovaru podľa dodacieho listu (3 h) Osadenie a rozmiestnenie PC a notebookov v učebniach, pripojenie na LAN sieť (prepojovacie káble nie sú súčasťou dodávky) (8 h) Krátke zaškolenie s robotom, vizualizérom, kamerou a tlačiarňou (4 hod) Štandartná inštalácia a konfigurácia interaktívnyc tabúľ a dataprojektorov do učební (32 h) Zaškolenie práce s interaktívnou tabuľou a dataprojektorom (1 hod)	-	súbor	1
18	**Inštalácia a konfigurácia, školenie pre položky 15 a 16**	Inštalačné práce zahŕňajú: (8h) Rozbalenie a kontrola podľa dodacieho listu Osadenie centrálnej časti sieťových prvkov (2 x prepínač, 1 x centrálny firewall, terminálový server) do dátovej skrine a ich pripojenie na elektrické napätie Osadenie servera a diskového poľa do dátovej skrine a ich pripojenie na rozvod elektrického napätia Osadenie aktívnych prvkov na jednotlivé pracoviská Prepojenie jednotlivých aktívnych prvkov pre zabezpečenie požadovanej dátovej komunikácie	-	súbor	1
		Konfiguračné práce zahŕňajú : (99h) Konfigurácia centrálneho firewallu – konfigurácia bude zabezpečovať oddelenie topológie kybernetického laboratória od LAN siete školskej siete a tiež bude zabezpečovať prístup do siete Internet. Konfigurácia IPS systému na centrálnom firewalle – IPS systém bude kontrolovať prechádzajúcu dátovú komunikáciu na potenciálne útoky a rozpoznané útoky bude blokovať. Konfigurácia centrálnych prepínačov – zabezpečuje dátové pripojenie jednotlivých pracovísk s centrálnou časťou siete kybernetického laboratória. Konfigurácia terminálového servera. Konfigurácia diskového poľa Konfigurácia centrálneho servera a jeho prepojenie na diskové pole Inštalácia a konfigurácia virtualizačného prostredia na centrálny server Príprava jednotlivých „imagov" operačných systémov potrebných pre realizovanie jednotlivých učebných tém Príprava imagu pre OS na serveroch , príprava imagu pre aplikačný firewall Príprava imagu pre ochranu mailovej prevádzky systému, príprava imagu pre ochranu webovej pravádzky Príprava konfiguračných súborov pre jednotlivé pracoviská Príprava konfiguračného súboru pre firewall, príprava konfigurácie pre IPS systém Príprava konfiguračných súborov pre prepínače • Konfigurácia centrálnych prepínačov, prepojenie zariadení, spustenie zariadení – 12 hod • Konfigurácia centrálneho firewall a terminálového servera – 8 hod • Konfigurácia serverov – 8 h • Konfigurácia virtuálnych serverov pre jednotlivé tématické okruhy – 24 hod • Konfigurácia centrálneho diskového úložiska – 16 h • Konfigurácia zariadení pre jednotlivé pracoviská – 24 hod • Základné testovanie komunikácie medzi pracoviskami a centrálnym bodom, dodatočné ladenie konfigurácie – 4 hod • Otestovanie funkčnosti tématických okruhov na žiackom pracovisku – 3 hod	-	x	x
		Školenie (48 h): Školenie pedagógov zahŕňa : školenie troch vyučujúcich v rozsahu 6 praconých dní x 8 hod (48h). Predmetom školenia bude oboznámenie sa s obsahom jednotlivých učebných tém (naučiť sa ako zabezpečiť informačný systém, údaje a aj užívateľov proti reálnym útokom, ich dopadom a zneužitiu) s dôrazom na zabezbečenie kvalitného pedagogického procesu v rámci výuky žiakov v prostredí kybernetického laboratória.	-	x	x

Minimálna špecifikácia servisnej podpory:

P.č.	Kategória položky	Popis požiadavky na servisnú podporu
1	**HW-A**	Servisná podpora pre HW : V prípade nefunčnosti HW telefonická a e-mailová komunikácia v režime od 8 h do 17 h počas pracovných dní s dobou odozvy do nasledujúceho pracovného dňa a na obdobie 3 rokov. V prípade nefunkčnosti HW je požadovaná výmena HW do 3 pracovných dní. Nevzťahuje sa na inštalačné a konfiguračné zmeny HW a OS. Servisná podpora sa nevzťahuje na nefunkčnosti HW spôsobené OS a inými aplikáciami.
2	**HW-B**	Servisná podpora pre HW : Aktualizácia firmware. V prípade nefunčnosti HW telefonická a e-mailová komunikácia v režime od 8 h do 17 h počas pracovných dní s dobou odozvy do nasledujúceho pracovného dňa a na obdobie 5 rokov. V prípade nefunkčnosti HW je požadovaná výmena HW do 3 pracovných dní. Nevzťahuje sa na inštalačné a konfiguračné zmeny HW.
3	**SW-B**	Servisná podpora pre SW : SW aktualizácie - update . V prípade updatou SW musí byť zabezbečená telefonická a e-mailová komunikácia v režime od 8h do 17h počas pracovných dní s dobou odozvy do nasledujúceho pracovného dňa a na obdobie 5 rokov. Nevzťahuje sa na inštalačné a konfiguračné zmeny SW.