PTS s.r.l.

SOLUZIONI PER LA SCUOLA
E PER L'UFFICIO

Laboratorio di Cybersecurity

PROGETTO PER LA REALIZZAZIONE DI UN LABORATORIO DIDATTICO INNOVATIVO	NEXT GENERATION LAB Feb. 2023
La Missione 4 del PNRR ITALIA (Potenziamento dell'offerta dei servizi di istruzione dagli asili nido alle università), nell'investimento 3.2 è prevista la creazione di laboratori volti alle professioni digitali del futuro. I laboratori sono pensati per le scuole secondarie di 2°grado che verranno dotate di spazi e di attrezzature digitali avanzate per l'apprendimento di quelle competenze che si acquisiscono durante gli anni di indirizzo.	

Target

Il numero indicato in tabella rappresenta un rating (da 1 a 5) indicativo del potenziale interesse del singolo indirizzo. 1= scarso interesse, 5= molto interessante

Livello di interesse per indirizzo

Liceo classico e scienze umane	Liceo linguistico	Liceo artistico, musicale e coreutico	Liceo scientifico	Istituto Tecnico - indirizzo tecnologico	Istituto Tecnico - indirizzo economico	Istituto professionale
3	3	3	5	5	4	5

Descrizione generale e obiettivi:

Il laboratorio di Cyber Security si presenta come un'occasione per andare ad acquisire nuove competenze nel campo delle nuove tecnologie informatiche che, oggigiorno, sono sempre più pervasive e necessarie al fine di consentire la sicurezza dei dati industriali e personali.

Attraverso una didattica learning by doing, ovvero una metodologia interamente esperienziale, questo laboratorio si pone come obiettivo principale quello di fornire agli studenti le competenze e le conoscenze fondamentali necessarie per affrontare tutte le sfide che il mondo della tecnologia moderna ci presenta sia in ambito lavorativo che nella vita di tutti i giorni.

Il laboratorio di Cyber Security consentirà agli studenti di familiarizzare e conoscere la strumentazione specifica necessaria per perseguire gli obiettivi didattici in modo stimolante, coinvolgente ma soprattutto innovativo.

Attraverso attività esperienziali attive e collaborative, sarà possibile comprendere tutti gli aspetti fondamentali delle infrastrutture di rete e di comunicazione in uso nel modo reale, in particolar modo sarà possibile conoscere e studiare i protocolli di autenticazione, di comunicazione e di protezione dagli accessi non autorizzati, i dispositivi utilizzati e le best practice consigliate.

Finalità didattiche

- Fornire una formazione specifica volta a conferire competenze e strumenti applicabili in un futuro contesto professionale e lavorativo
- Acquisire competenze riguardanti le tecnologie e gli apparati utilizzati dalle nuove tecnologie per la comunicazione
- Sviluppare competenze riguardanti i protocolli più comunemente in uso nel mondo contemporaneo
- Favorire l’apprendimento di nozioni rivolte a contesti lavorativi in continuo sviluppo
- Potenziare una metodologia di apprendimento attraverso il fare (learning by doing)
- Valorizzare le abilità e le potenzialità di tutti gli alunni stimolando la loro partecipazione attiva e la cooperazione all’interno della classe
- Favorire lo sviluppo di competenze digitali
- Sviluppare capacità di problem solving

Cosa include

All’interno di questo laboratorio, si trova una stazione facilmente trasportabile che integra quattro sezioni modulari rappresentanti:

- il *client*, ovvero il fruitore di servizi telematici e/o dati
- l' *infrastruttura*, ovvero la serie di apparati atti alla raccolta, il trasporto e la consegna di tali dati

- uno o più *server* in grado di produrre e mettere a disposizione i dati e/o l'elaborazione dei medesimi
- un *hostile*, ovvero un soggetto non autorizzato all'accesso da cui, a mezzo del laboratorio, verrà spiegato come difendersi

Inoltre sono inclusi:

N. 3 PC "Server" Linux con (ciascuno):

- 64GB RAM
- Processore i9
- 2TB HD SSD
- 4 Porte GB Ethernet

Sistema Operativo Linux RPM Based con kernel 6.x (open source)

VMware Workstation Player / Workstation Pro 17+ (licenza a pagamento)

Macchine virtuali multiple con:

- S.O. Linux RPM Based, Kernel 6.x (open source)
- Server WEB Apache 2.x (open source)
- Server WEB/Proxy NGINX 1.x (open source)
- Server SMTP Postfix 3.x (open source)
- Server IMAP/POP3 Dovecot 2.x (open source)
- Server DNS Bind 9.x (open source)
- Server SSH OpenSSH 9.x (open source)
- Server SQL MariaDB 10.x (eq. MySQL) (open source)
- Software di backup Timeshift e Amanda (open source)

La generazione dei contenuti dinamici utilizza:

- PHP 8.x (open source)
- Python 3.x (open source)
- CMS PHP Wordpress 6.x (open source)
- Framework Python Web2Py 2.2x (open source)

Le pagine WEB e le e-mail utilizzano:

- CSS 3
- HTML 5
- ECMAScript 2018 (ES6)

N. 2 SAN Synology Diskstation per la conservazione dei backup dei dati e delle macchine virtuali

N. 5 PC Laptop "Client" Linux con:

- Sistema Operativo Linux RPM Based con kernel 6.x (open source)
- Oracle VirtualBox 6.x (open source)

Macchine virtuali con:

- S.O. Linux RPM Based, Kernel 6.x (open source)
- Web Browser Chrome (open source)
- Web Browser Firefox (open source)
- Mail Client Thunderbird (open source)
- Python 3.x (open source)
- PHP 8.x (open source)
- Software di backup Timeshift e Amanda (open source)

N. 1 Switch Fortinet Fortiswitch Secure Access 24 Porte

N. 1 Firewall Fortinet Fortigate 5 porte

N. 1 Access Point 802.11acn (TP-Link o D-Link)

CONTATTATECI PER INFORMAZIONI O PER ACQUISTARE QUESTO LABORATORIO

PTS s.r.l.

Via Emilia Est, 1741/G - 41122 Modena

Tel: 059/285520 - Fax: 059/280415 - www.ptssrl.it - info@ptssrl.it

Cap. Soc. € 95.000 i.v. - Cod. Fisc. e P. IVA 02221640366 - CCIAA 274937