Курс „Мрежова и информационна сигурност и противодействие на кибератаки“

Модул I: Базово ниво за крайни потребители

Продължителност: **Един ден**

Успешното създаване и имплементиране на политика и правила за управление и защита на информационната сигурност (ИС) в организацията са свързани с промени, които следва да бъдат разпознати и подкрепени от мениджмънта и служителите с цел предпазване от пробиви в сигурността и защита на организационните цели и активи.

Процесите за управление на ИС трябва да бъдат съпроводени със запознаване на служителите на различните нива и отдели с принципите за безопасност при работата с информационни и дигитални ресурси. Във връзка с това организациите трябва да провеждат периодични информационни кампании, за да съхранят и подобрят качеството на процесите по управление на ИС.

Целта на курса „Мрежова и информационна сигурност и противодействие на кибератаки“ е да предостави необходимите знания и умения на обучаемите за защита на информационните активи в организацията. Той е насочен към крайните потребители на една информационна система, които ще придобият базови знания и фундаментално разбиране за различните заплахи за компютърната и мрежова сигурност, като:

- кражба на самоличност
- загуба на поверителна информация и злоупотреба с откраднати данни
- банкови, имейл и фишинг измами в публичните мрежи
- вируси, задни врати и троянски коне
- онлайн шпиониране
- хакерски атаки и социално инженерство

Курсистите ще придобият компетенции за предприемане на необходимите стъпки за противодействие и смекчаване на последствията от кибератака и ще подобрят цялостната си кибер хигиена.

Курсът цели да подпомогне дейността на звената и на служителите, отговарящи за мрежовата и информационна сигурност (в частта им за организиране на обучение на служителите им, съгласно Наредбата за минималните изисквания за мрежова и информационна сигурност), както и на всички ангажирани с безпроблемното протичане на съпътстващите процеси в организацията.

Обучението завършва със сертификат за участие и възможност за продължаване в следващо ниво.

Програма

Тема 1: Въведение: Обикновеният потребител-най-уязвимото звено в системата за киберсигурност.	Представени са: етапите на изграждане на системата за киберсигурност; ролята на различните служители в тази система и техните отговорности; най-често срещаната архитектура на система за киберзащита; важността на крайните потребители за успешно функциониране на системата.
Тема 2: Какво представлява социалното инженерство и как да се предпазим от него.	Концепции и цели на социално инженерство; въздействие на атаките извършвани със социален инженеринг; фактори, които правят компаниите уязвими за социален инженеринг; фази на атаката свързана със социално инженерство; техники за социален инженеринг и как да се предпазим от тях.
Тема 3: Компрометиране на потребителски акаунти и компютри, признаци и защита.	Етапи на компрометиране на една информационна система; видове зловреден софтуер и как компрометират те системите; техники за защита.
Тема 4: Добрата политика за паролите: важен фактор за осигуряване на киберсигурността на една организация.	Механизми за автентикация в Windows операционни системи; механизъм за хакване на пароли; добри политики използвани за защита на пароли.
Тема 5: Видове фишинг атаки и как да им противодействаме.	Представяне на различните видове фишинг атаките; как да се предпазим от фишинг техники и подходи; как да защитим електронната си поща; как да откриваме зловредните писма; политика за безопасна работа с електронната поща и с електронния календар.
Тема 6: Заплахи свързани с използване на политиката BYOD и на мобилни устройства.	Представяне на политиката – BYOD (донеси своето лично устройство), използвана от все повече съвременни компании; предимства и рискове на използване на BYOD; уязвимости, които носят мобилните устройства, когато се използват в корпоративни мрежи; как да защитим мобилните си устройства.
Тема 7: Атаки извършвани с USB устройства.	Основни типове хакерски атаки с използване на USB; описание на извършването на различни видове USB атака; как да открием атаки, извършвани чрез USB порта на нашето устройство, и как да се предпазим от тях.
Тема 8: Уязвимости при сърфиране в Интернет.	Архитектура на услугите, предоставяни в публичните мрежи; описание на най-често извършваните уеб атаки към потребителите; как да се предпазим и противодействаме на уеб атаки; как да проверяваме дали уеб сайтовете, които посещаваме са зловредни.
Тема 9: VPN – възможности и ограничения.	Какво представлява VPN: архитектури и как се прилагат в корпоративните мрежи; предимства и причини да се използва VPN; какво не може да прави VPN и какви уязвимости има.
Тема 10: Използвани техники за атака в публичните wifi мрежи и начини за защита от тях.	Използвани техники за хакерски атаки в wifi мрежите; какви техники за защита трябва да се използват при работа в публичните wifi мрежи.
Тема 11: Митове и реалност в киберсигурността	Представяне на общоприети „истини“ и „митове“ за киберсигурността и каква е реалността всъщност.

TechnoLogica
ул. “Червена стена” 46
1421 София, България
тел: (+359 2) 91 91 2 / в. 161
мобилен: (+359 888) 618 012
www.technologica.com
pandreeva@technologica.com