Slovníček základních pojmů

Krátké vysvětlení nejčastějších pojmů, které se mohou objevit v souvislosti s IT bezpečností na UK.

A

Antivir - program, který chrání zařízení před škodlivým softwarem (viry, spyware). Pravidelně kontroluje systém a blokuje podezřelé soubory.
Autentizace – ověření vaší identity při přihlášení do systému (např. zadání hesla, potvrzení v aplikaci).

D

Digitální identita - soubor údajů, který vás jednoznačně identifikuje v online světě – například váš univerzitní účet.

Dvoufaktorové ověření (2FA) - způsob přihlašování, kdy kromě hesla potvrzujete svou identitu ještě druhým faktorem – např. mobilní aplikací.

Data **(osobní / univerzitní)** – všechny elektronické informace (soubory, dokumenty, e-maily), které mohou obsahovat citlivé údaje a je nutné je chránit.

F

Firewall – „ochranná brána“ mezi vaším zařízením a internetem. Sleduje a filtruje síťový provoz, blokuje nebezpečné připojení.

Fake login / podvržená stránka – web, který se tváří jako oficiální stránka (např. CAS UK), ale snaží se vylákat vaše heslo.

H

Heslo – vaše klíčová ochrana účtu. Mělo by být silné (min. 12 znaků, kombinace písmen, čísel a symbolů) a unikátní

Hoax – poplašná nebo nepravdivá zpráva, která se šíří internetem (např. falešné varování, výzva k přeposlání e-mailu).

I

Incident - jakákoli událost, která může ohrozit bezpečnost systému nebo dat – např. prolomené heslo, ztracený notebook nebo phishingový útok.

M

Malware – škodlivý software, který může poškodit systém nebo ukrást data. Patří sem viry, spyware i ransomware.

P

Phishing – podvodná zpráva (e-mail, SMS, chat), která se snaží získat vaše údaje nebo přimět vás ke kliknutí na nebezpečný odkaz.

PIN / biometrie – způsoby zabezpečení zařízení (číslo, otisk prstu, rozpoznání obličeje).

Patch (aktualizace) – oprava nebo doplněk softwaru, která opravuje chyby nebo zranitelnost v systému.

R

Ransomware – škodlivý program, který zašifruje vaše soubory a požaduje výkupné za jejich obnovení.

Reputace domény – důvěryhodnost webové adresy; stránky s podezřelým obsahem mohou být blokovány bezpečnostním softwarem.

S

Sociální inženýrství – manipulace lidí s cílem získat jejich důvěru a tím i přístup k citlivým údajům.

Spam – nevyžádané e-maily, často s reklamou, odkazy na škodlivé weby nebo podvody.

Spear phishing (cílený phishing) – útočník se zaměří na konkrétní osobu (např. zaměstnance univerzity) a zprávu přizpůsobí tak, aby působila důvěryhodně.

Spyware – program, který tajně sleduje, co na počítači děláte a tato data odesílá útočníkům.

Š

Šifrování (encryption) - proces, který převádí data do nečitelné podoby, dokud nejsou odemčena správným klíčem.

T

Trojský kůň (Trojan) - program, který se tváří jako užitečný, ale po instalaci umožní útočníkovi přístup do systému.

U

Únik dat – situace, kdy se citlivé informace dostanou k neoprávněné osobě. Může vzniknout omylem i útokem.

Útok hrubou silou (brute force) – pokus o prolomení hesla zkoušením všech možných kombinací.

V

VPN **(Virtual Private Network)** – šifrované spojení, které chrání přenos dat při práci na dálku nebo z veřejných sítí.

Virus – program, který se sám šíří a poškozuje soubory či systém.

Vishing/smishing – phishing po telefonu (vishing) nebo přes SMS (smishing).

Z

Zálohování – ukládání kopie dat (např. na univerzitní disk nebo cloud), aby bylo možné je obnovit při ztrátě či útoku.

Zranitelnost – chyba v softwaru, kterou mohou útočníci zneužít.