

Kyberbezpečnosť vo firmách

Ako si firmy dávajú overovať svoju digitálnu bezpečnosť

1. Prečo firmy riešia kyberbezpečnosť

Firmy dnes používajú počítače, servery, cloud, internet a databázy, v ktorých majú:

- osobné údaje zákazníkov,
- finančné informácie,
- heslá a prístupové údaje,
- dôležité firemné dokumenty.

Ak by sa k týmto údajom dostal útočník, firma by mohla:

- prísť o peniaze,
- porušiť zákon (napr. GDPR alebo NIS2)
- stratiť dôveru zákazníkov,
- poškodiť svoju reputáciu.

Preto nestačí mať len antivírus – firmy si **platí špecializované bezpečnostné firmy**, ktoré preverujú, či sú ich systémy dostatočne zabezpečené.

2. Externé bezpečnostné firmy

Čo sú externé bezpečnostné firmy

Sú to **odborné firmy alebo tímy expertov na kyberbezpečnosť**, ktoré:

- nie sú súčasťou firmy, ktorú kontrolujú,
- majú špecializované znalosti a skúsenosti,
- používajú profesionálne nástroje a postupy.

Ich úlohou je **nájsť bezpečnostné slabiny skôr, než ich zneužije hacker**.

3. Bezpečnostný audit

Čo je bezpečnostný audit

Bezpečnostný audit je systematická kontrola digitálnej bezpečnosti firmy.

Počas auditu sa kontroluje napríklad:

- kto má prístup k systémom,
- ako sú chránené heslá,
- či sú systémy aktualizované,
- ako firma zálohuje údaje,
- či zamestnanci dodržiavajú bezpečnostné pravidlá.

Výsledok auditu

Na konci auditu firma dostane:

- správu o zistených problémoch,
 - hodnotenie úrovne bezpečnosti,
 - odporúčania, ako sa zlepšiť.
-

4. Penetračné testovanie (etický hacking)

Čo je penetračný test

Penetračný test je riadený kybernetický útok, pri ktorom:

- bezpečnostná firma sa snaží „nabúrať“ do systémov,
- robí to legálne a so súhlasom firmy,
- simuluje správanie skutočného hackera.

Tento proces vykonávajú **etickí hackeri** (white hat hackeri).

Čo sa testuje

- webové stránky,
- firemné siete,
- Wi-Fi siete,
- zamestnanecké účty,
- emailové systémy.

Cieľom je zistiť, **dokáže sa útočník dostať dovnútra a čo by mohol urobiť.**

5. Sociálne inžinierstvo v testovaní

Nie všetky útoky sú technické. Často sa testuje aj správanie ľudí.

Príklady sociálneho inžinierstva:

- falošné emaily (phishing),
- telefonáty vydávajúce sa za IT podporu,

- snaha dostať sa do budovy firmy.

Cieľom je overiť, či:

- zamestnanci klikajú na podozrivé odkazy,
 - prezrádzajú heslá,
 - dodržiavajú bezpečnostné pravidlá.
-

6. Certifikácie a normy

Niektoré firmy chcú oficiálne potvrdenie, že majú dobrú kyberbezpečnosť.

Príklady:

- bezpečnostné normy (napr. ISO/IEC 27001),
- certifikáty o splnení bezpečnostných štandardov.

Tieto certifikáty:

- zvyšujú dôveryhodnosť firmy,
 - sú často vyžadované pri spolupráci s inými firmami.
-

7. Prečo si firmy platia externistov

Firmy si neoverujú bezpečnosť samy, pretože:

- vlastní zamestnanci môžu prehliadnuť chyby,
- externá firma má nadhľad a skúsenosti,
- testovanie je objektívnejšie,
- odborníci poznajú aktuálne hrozby.

Externá kontrola je podobná ako: **technická kontrola auta** alebo **kontrola účtovníctva audítorm**

8. Prínos pre firmu

Overovanie digitálnej bezpečnosti pomáha firme:

- predchádzať kyberútokom,
- chrániť údaje zákazníkov,
- splniť zákonné povinnosti,
- zvýšiť bezpečnostné povedomie zamestnancov.

9. NIS2 – prečo je dnes ešte dôležitejšia bezpečnosť

NIS2 je európska smernica o kybernetickej bezpečnosti, ktorá platí pre členské štáty EÚ (vrátane Slovenska).

Čo NIS2 prináša firmám:

- rozširuje okruh firiem, ktoré **musia riešiť kyberbezpečnosť povinne**,
- kladie väčší dôraz na:
 - riadenie rizík,
 - ochranu systémov a dát,
 - školenie zamestnancov,
 - nahlásovanie kybernetických incidentov,
- zavádza **prísnejšie kontroly a sankcie** za nedodržiavanie pravidiel.

NIS2 sa týka najmä:

- IT a digitálnych služieb,
- energetiky, dopravy, zdravotníctva,
- výrobných a priemyselných firiem,
- poskytovateľov cloudových a sieťových služieb.

1Kybernetická bezpečnosť v praxi – čo hrozí firmám

<https://www.youtube.com/watch?v=2VhlHpwcVDM>

2.Kyberbezpečnosť v ICT firmách – audit, prevencia, ľudský faktor

<https://www.youtube.com/watch?v=-ztpWFVcq4>

3. What Is Penetration Testing? (Ethical Hacking)

<https://www.youtube.com/watch?v=I7eCSxkApUI>