



AUDIT KYBERNETICKEJ BEZPEČNOSTI

podľa zákona č. 69/2018 Z. z.
o kybernetickej bezpečnosti



Čo je audit podľa zákona o kybernetickej bezpečnosti?

Podľa zákona o kybernetickej bezpečnosti č. 69/2018 Z. z. je audit kybernetickej bezpečnosti procesom hodnotenia úrovne kybernetickej bezpečnosti organizácie. Jeho cieľom je identifikovať slabé miesta a riziká v informačných systémoch a infraštruktúre organizácie a poskytnúť odporúčania na zlepšenie bezpečnosti.

Audit sa zameriava na rôzne aspekty, vrátane riadenia bezpečnosti, technických opatrení, riadenia rizík a personálnej bezpečnosti. Výsledkom je správa s odporúčaniami na zlepšenie bezpečnosti organizácie.

Čo je cieľom auditu?

Cieľom auditu je hodnotiť a overiť úroveň kybernetickej bezpečnosti organizácie a súlad s požiadavkami zákona o KB a súvisiacimi vyhláškami NBÚ. Audit identifikuje slabé miesta, nedostatky a riziká v informačných systémoch a infraštruktúre a poskytuje odporúčania na ich zlepšenie. Hlavné ciele auditu kybernetickej bezpečnosti zahŕňajú:

- Identifikácia slabých miest: Audit sa zameriava na identifikáciu slabých miest v bezpečnosti informačných systémov, procesoch a infraštruktúre organizácie. Tieto slabé miesta môžu predstavovať riziko pre kybernetické útoky alebo neoprávnený prístup k citlivým údajom.
- Hodnotenie súladu s bezpečnostnými štandardmi: Audit overuje, či organizácia dodržiava stanovené bezpečnostné politiky, normy a právne predpisy týkajúce sa kybernetickej bezpečnosti. Tým sa zabezpečuje súlad s požiadavkami a odporúčaniami bezpečnostných štandardov.
- Riadenie rizík: Audit sa zaobera aj procesom riadenia rizík organizácie, čím pomáha identifikovať potenciálne riziká a navrhuje opatrenia na ich riadenie a minimalizáciu.
- Poskytovanie odporúčaní na zlepšenie: Na základe zistení auditu sa vypracováva správa s odporúčaniami na zlepšenie kybernetickej bezpečnosti. Tieto odporúčania slúžia ako usmernenia pre organizáciu pri prijímaní opatrení na posilnenie svojej bezpečnosti.

Audit kybernetickej bezpečnosti je nástrojom, ktorý umožňuje organizáciám získať prehľad o ich bezpečnosti a poskytuje odporúčania na zlepšenie. Je dôležitý pre všetky organizácie, ktoré si vážia ochranu svojich údajov a chcú minimalizovať riziká kybernetických hrozieb.



Čo je výstupom auditu KB?

Výstupom auditu kybernetickej bezpečnosti je audítorská správa obsahujúca zistenia, analýzu a odporúčania vyplývajúce z hodnotenia bezpečnosti organizácie. Táto správa je základným výstupom auditu a poskytuje nasledujúce informácie:

- Zistenia a hodnotenie: Správa obsahuje zistenia auditu, teda identifikované slabé miesta, nedostatky a riziká v oblasti kybernetickej bezpečnosti organizácie. Tieto zistenia sú podložené dôkazmi získanými počas auditu. Ďalej je poskytnuté hodnotenie úrovne bezpečnosti na základe zhodnotenia všetkých relevantných aspektov.
- Odporúčania na zlepšenie: Správa obsahuje odporúčania na zlepšenie kybernetickej bezpečnosti organizácie. Tieto odporúčania sú vytvorené na základe identifikovaných nedostatkov a rizík. Cieľom odporúčaní je poskytnúť konkrétné usmernenia a opatrenia, ktoré organizácia môže prijať na zvýšenie svojej bezpečnosti a ochrany pred kybernetickými hrozobami.
- Vyhodnotenie súladu: Správa môže obsahovať aj vyhodnotenie súladu organizácie s bezpečnostnými štandardmi, právnymi požiadavkami alebo internými politikami týkajúcimi sa kybernetickej bezpečnosti. Toto vyhodnotenie poskytuje informácie o tom, do akej miery organizácia spĺňa požadované normy a pravidlá.

Pre koho je audit povinný?

Audit kybernetickej bezpečnosti je teda povinný pre každého úradom registrovaného prevádzkovateľa základných služieb.

Navyše audit je nutné opakovane vykonávať každé dva roky, pričom výslednú auditnú správu je nutné odovzdať úradu.

Výstupom auditu je teda audítorská správa, ktorá organizácii poskytuje pohľad na jej aktuálnu úroveň kybernetickej bezpečnosti, identifikuje slabé miesta a riziká a navrhuje opatrenia na ich zlepšenie.

Tieto odporúčania slúžia ako usmernenie pre organizáciu pri plánovaní a realizácii opatrení na posilnenie kybernetickej bezpečnosti.

Popis služby

Audit kybernetickej bezpečnosti podľa zákona o kybernetickej bezpečnosti č. 69/2018 Z. z. a súvisiacich vyhlášok NBÚ je odborná – konzultačná služba, ktorá umožňuje organizáciám preskúmať a hodnotiť úroveň bezpečnosti v kybernetickom prostredí.

Počas auditu sú identifikované slabé miesta, nedostatky a riziká v informačných systémoch a infraštukture organizácie a posúdzuje sa súlad so zákonom o kybernetickej bezpečnosti. Správa s odporúčaniami na zlepšenie je výsledkom tohto procesu.



Viac informácií

Web: www.secom.sk

E-mail: security@secom.sk