



G - Audit

Audit bezpečnosti

Ako je zabezpečený majetok vašej firmy?
Chránite automobily imobilizérom, alarmom,
pagerom či ochranným mikročipovým označením?

A ako je zabezpečený
váš informačný systém?

G - Audit

Audit bezpečnosti informačného systému

Spoločnosť GORDIAS vám ponúka Audit bezpečnosti informačného systému. Audit sa týka všetkých komponentov a úrovni bezpečnosti systému (fyzickej, logickej, organizačnej, legislatívnej).

Pri realizácii auditu spoločnosť GORDIAS postupuje podľa overených štandardov a odporúčaní. Implementácia kontrolných mechanizmov vychádza z celosvetovo akceptovanej metodológie COBIT (Control Objectives for Information and Related Technology), ktorá zahŕňa technické štandardy (vrátane noriem ISO a EDIFACT), kvalifikačné kritériá (vrátane TCSEC, ITSEC resp. Common Criteria) aj profesionálne štandardy pre internú kontrolu a audit (vrátane štandardov ISACA a CPA). Audit zodpovedá najnovšej verzii britskej normy BS7799 (t. j. ISO 17799).

Záverečná správa Audit bezpečnosti informačného systému identifikuje a posudzuje z hľadiska bezpečnosti:

- používané technologické platformy a subsystémy vrátane ich vzájomných závislostí,
- oblasti, ktoré sú outsourcované,
- používané komponenty systému (hardvér, softvér, aplikácie, periférne zariadenia),
- používané a poskytované služby,
- dáta a dátové toky,
- sieťovú infraštruktúru,
- organizačné a personálne zabezpečenie,
- fyzické zabezpečenie systému,
- aktuálny stav a možnosti zvyšovania informačnej bezpečnosti z globálneho hľadiska.

Záverečná správa

Záverečná správa Audit bezpečnosti informačného systému vám podá naozaj komplexnú informáciu o stave bezpečnosti vášho systému.

Audit bezpečnosti informačného systému spoločnosti GORDIAS je optimálnym východiskom na ceste k vysokej bezpečnosti vášho informačného systému.

Osnova záverečnej správy:

1. Konceptia bezpečnosti systému
bezpečnostné plánovanie, bezpečnostná politika, riadenie bezpečnosti a kompetencie, priority ochrany
2. Plánovanie a vývoj systému
konceptia rozvoja systému, informačné potreby, zavádzanie produkčných aplikácií a technického vybavenia do ostrej prevádzky, zmenové konania
3. Technické a programové vybavenie systému
bezpečnosť prostredia operačných systémov, databázového prostredia, pracovných staníc, servera, periférnych zariadení
4. Počítačové siete a sieťová komunikácia
ochrana prenášaných údajov v LAN a WAN, dostupnosť sieťových služieb a aplikácií, vzdialený prístup k informáciám a službám, komunikácia s externými subjektami
5. Prevádzka a správa systému
ochrana údajov počas spracovávania, zabezpečenie spoľahlivosti spracovania, bezpečná správa a prevádzka systému, dostupnosť dát a služieb systému
6. Fyzická a režimová ochrana systému
ochrana spracovaných dát v elektronickej a papierovej forme, riadenie fyzického vstupu, režimová bezpečnosť, EPS, EZS
7. Zálohovanie, archivácia a likvidácia údajov systému
bezpečnosť elektronických informácií a ich nosiče
8. Havarijné plány a plánovanie obnovy systému
náhradné postupy pre prípad výpadku systému, postupy pre obnovu činnosti systému
9. Organizačná a personálna bezpečnosť systému
kontrolné prvky bezpečnosti, pracovné náplne, povinnosti a zodpovednosti, smernice pre prácu so systémom, spolupráca s tretími stranami - externí experti, servisné firmy

