Kyberbezpečnost – pohled auditora účetní závěrky

Ing. Martina Křížová Chrámecká, FCCA

Povinnost auditora

- Auditor vydává výrok o tom, zda účetní závěrka společnosti poskytuje ve všech materiálních ohledech věrný a poctivý obraz její finanční pozice (aktiv a pasiv) a finanční výkonnosti (náklady, výnosy a hospodářský výsledek).
- Auditor je zodpovědný za získání dostatečných důkazních informací, které mu poskytují přiměřenou jistotu pro učinění závěru.
- Auditor se nevyjadřuje k účinnosti a vhodnosti nastavení vnitřního kontrolního systému společnosti.

Povinnost auditora

Auditor je povinen:

- identifikovat a vyhodnotit rizika materiální nesprávnosti v účetní závěrce, ať už je způsobena chybou nebo podvodem – ISA 315R;
- seznámit se s vnitřním kontrolním systémem společnosti v takovém rozsahu, aby mohl navrhnout vhodné auditorské postupy – ISA 315R;
- naplánovat a provést auditní postupy, které snižují identifikované riziko materiální nesprávnosti na přijatelnou úroveň – ISA 330.

Vztah zajištění kyberbezpečnosti a správnosti účetní závěrky

- Data pro sestavení účetní závěrky pochází z IT systémů/aplikací.
- V některých případech může nedostatečné zabezpečení proti kybernetickým útokům zvyšovat riziko nesprávnosti v účetní závěrce
  - Lze se na data v IT systémech spolehnout (integrita dat, neautorizované změny systému)?
  - Budou data dostupná?

Povinnost vedení společnosti

- Vedení společnosti odpovídá:
  - za sestavení účetní závěrky podávající věrný a poctivý obraz v souladu s českými účetními předpisy;
  - za takový vnitřní kontrolní systém, který považují za nezbytný pro sestavení účetní závěrky tak, aby neobsahovala významné nesprávnosti způsobené podvodem nebo chybou;
  - za identifikaci a řízení podnikatelských rizik včetně rizik vyplývajících z používání IT zařízení a aplikací.

Typická rizika související s kybernetickými útoky

- Nedostupnost dat/ztráta dat
  - Pokuty/penále
  - Předpoklad nepřetržitého trvání
  - Ztráta zákazníků – snížení hodnoty aktiv
  - Nemožnost sestavit účetní závěrku
- Zcizení majetku
- Zneužití informací
  - Pokuty/penále
  - Předpoklad nepřetržitého trvání
  - Ztráta zákazníků – snížení hodnoty aktiv
- Ohrožení dobrého jména společnosti
  - Ztráta zákazníků – snížení hodnoty aktiv

Rizika související s kybernetickými útoky

- Auditor je považuje za ostatní podnikatelská rizika a vyhodnocuje, zda mohou způsobit **materiální nesprávnost** v účetní závěrce.
- Obvykle je riziko materiální nesprávnosti v souvislosti s kyberbezpečností vyhodnoceno jako nízké/žádné, ale závisí na sektoru a způsobu podnikání společnosti.
- Riziko podvodu v účetní závěrce (ISA 240):
  - Zúčtování neexistujících transakcí,
  - Manipulace s peněžními zůstatky, databází dodavatelů (platby na jiný účet) - phishing,
  - Zcizení aktiv nehmotné povahy (patenty).
- Riziko porušení zákonných povinností (např. ochrana osobních údajů).

IT prostředí s vyšším rizikem pro audit

- online transakce (přes webové rozhraní),
- transakce využívající rozhraní třetích stran,
- automatické kalkulace,
- automatizované transakce,
- transakce využívající elektronických peněz,
- vysoce customizovaný SW,
- využívání třetích stran pro zajišťování významných/klíčových služeb či významných systémů IT

Povinnost auditora v souvislosti s IT prostředím společnosti – ISA 315R

- Porozumění IT prostředí.
- Identifikovat IT systémy/aplikace relevantní pro účetní závěrku, u nich identifikovat a vyhodnotit rizika vyplývající z používání IT definovaná ISA 315R:
  - Riziko ohrožující integritu informací v informačních systémech (úplnost, platnost, správnost, neměnnost);
  - Riziko neúčinnosti aplikační kontroly/automatického procesu (neoprávněné programové změny);
  - Potenciálně i riziko nepřetržitého trvání.
- Požadavek pro **IT aplikace relevantní pro ÚZ :** popsat a vyhodnotit nastavení obecných IT kontrol.
- IT systémy/aplikace bez vazby na účetní závěrku nejsou auditorem nijak pokrývány.

Příklady obecných IT kontrol posuzovaných auditorem z hlediska jejich nastavení

- nastavení přístupových práv do systému/aplikace,
- možnost přístupu do zdrojového kódu a právo jeho modifikace (změnové řízení),
- možnost přístupu do zdrojové databáze (ochrana dat),
- zálohování (ztráta dat),
- nákup, vývoj a údržba aplikačních systémů
- kontroly nad transfery dat …..

- Auditor využívá především následující přílohy ISA 315R
  - Přílohu 5 - Aspekty relevantní pro seznámení s informačními technologiemi,
  - Přílohu 6 - Aspekty relevantní pro seznámení s obecnými IT kontrolami.

Oblasti ITGC související s kybernetickou bezpečností

- Privilegovaná přístupová práva,
- Řízení IT rizik (identifikace, vyhodnocení, reakce…),
- Monitoring incidentů (identifikace, vyšetření, reporting, nápravná opatření),
- Zálohování,
- Aktualizace (patch management).

Povinnost auditora komunikovat významné nedostatky ve vnitřním kontrolním prostředí s vedením společnosti.

Dopad narušení kybernetické bezpečnosti

- Dopad kybernetického útoku:
  - Nedostupnost dat,
  - Krádež dat/aktiv společnosti,
  - Manipulace s daty/změna dat.
- Auditor má povinnost zvážit dopad útoku na účetní závěrku
  - Tvorba rezerv (soudní spory, pokuty, penále….),
  - Tvorba opravných položek,
  - Odúčtování aktiv,
  - Předpoklad nepřetržitého trvání.

Děkuji za pozornost

KOMORA AUDITORŮ ČESKÉ REPUBLIKY