

Riskujete, že o lidech ve svých dodavatelských řetězcích **nic nevíte?**

Dochází u vašich externích IT specialistů k podivným aktivitám? Co víte o lidech zaměstnaných třetími stranami, se kterými spolupracujete? Nejen vaši zaměstnanci, ale také vaši kontraktori, obchodní partneři a všechny společnosti, kteří jsou součástí vašeho dodavatelského řetězce, by měli být důkladně prověřeni.

Jste chráněni před těmito riziky?

Bezpečnostní hrozby

Bez řádného ověření minulosti mohou do dodavatelského řetězce proniknout pracovníci se záznamem v trestním rejstříku nebo spojením se zločineckými organizacemi. To může vést ke krádežím, sabotážím a neoprávněnému přístupu k citlivým informacím.

Narušení provozuschopnosti

V kritických činnostech dodavatelského řetězce, jako jsou činnosti zahrnující zboží podléhající rychlé zkáze nebo výrobu "just-in-time", mohou mít i drobná narušení dopad na celý dodavatelský řetězec.

Porušování předpisů

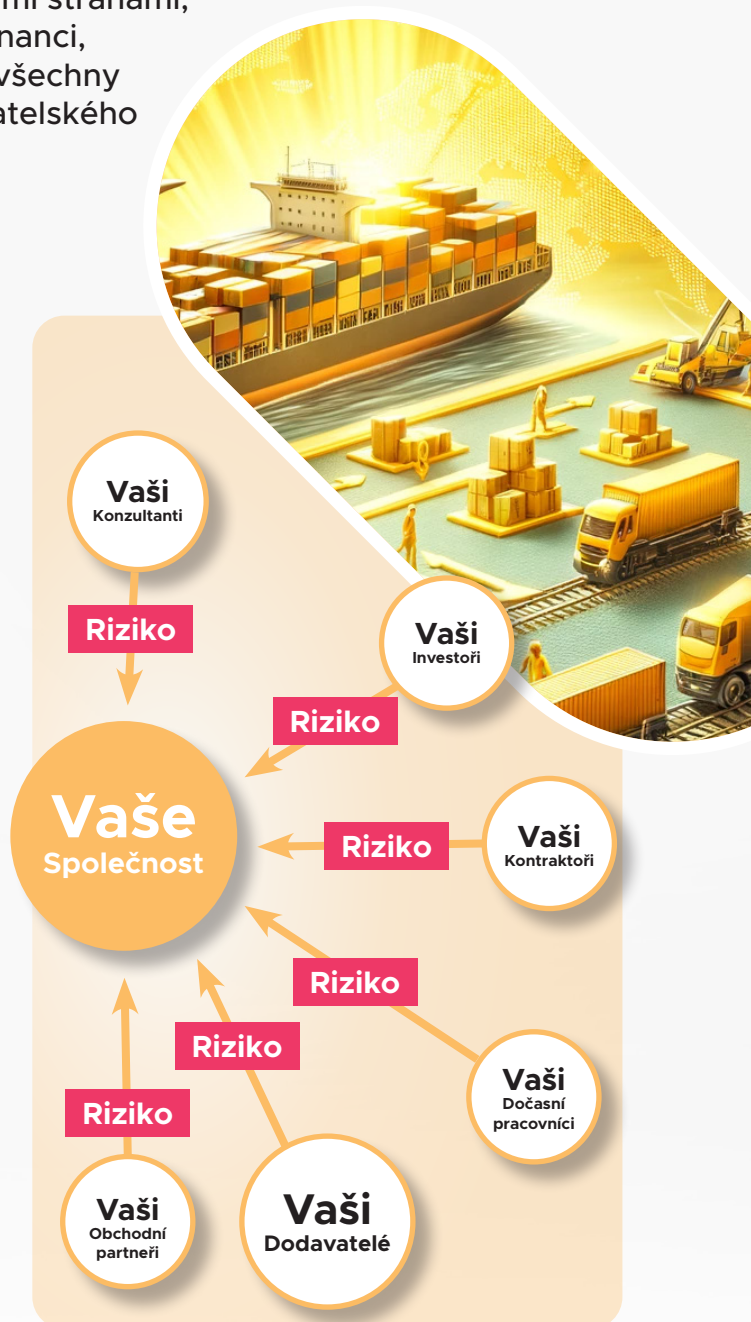
Zaměstnávání osob bez příslušného pracovního oprávnění nebo osob, které v minulosti porušily právní předpisy, může společnost vystavit významným právním rizikům.

Vnitřní hrozby

Zaměstnanci se špatnými úmysly mohou zneužít své přístupové údaje ke způsobení škody. Může jít o únik důvěrných dat, manipulaci s procesy za účelem osobního prospěchu nebo spolupráci s konkurencí.

Reputační riziko

Ať už jde o únik dat, stažení výrobku z trhu nebo pokutu od regulačních orgánů, důsledky zaměstnávání neproověřených pracovníků mohou být dlouhodobé a poškodit obraz společnosti na veřejnosti.



Měli byste trvat na ověřování všech pracovníků ve vašem dodavatelském řetězci. To zahrnuje prověřování minulosti a průběžný monitoring.

Kontaktujte nás ještě dnes.

Příklad z praxe: 2024 Incident

Začátkem roku 2024 se světový lídr v oblasti biotechnologií s kanceláři v České republice dozvídá o IT vývojáři, který pracuje pod falešnou identitou na jeho citlivém projektu.

Tento kontraktor body-shoppingové agentury, placený prostřednictvím startupu EoR Ruul v kryptoměnách, měl po dobu osmi měsíců před odhalením přístup k citlivým informacím a systémům. Takové incidenty zdůrazňují zásadní potřebu důsledného ověřování minulosti, aby se předešlo podvodům a zajistila se bezpečnost firemních aktiv.



Zohlednění nových regulačních požadavků

Se zavedením nových regulačních nařízení jako směrnice o síťových a informačních systémech (NIS2), směrnice o odolnosti kritických subjektů (CER) a místních zákonů, jako je německý zákon o náležité péči v dodavatelském řetězci, je pro společnosti nezbytné začlenit tyto požadavky do svých výběrových řízení a procesů výběru dodavatelů. Tyto předpisy zdůrazňují potřebu zvýšených bezpečnostních opatření, průběžného hodnocení rizik a přísných postupů kontroly.

Zajištění toho, aby dodavatelé dodržovali tyto normy, pomáhá nejen zmírnit rizika, ale také zajišťuje dodržování právních předpisů a podporuje odolnost dodavatelských řetězců. Zahrnutí ustanovení, která nařizují dodržování těchto regulačních požadavků, do smluv a hodnocení dodavatelů významně posílí ochranu vaší společnosti před potenciálními bezpečnostními hrozbami a narušením provozu.

Skutečná cena nezajištěného outsourcingu

Čím větší je význam a produktivita vašeho dodavatelského řetězce, tím větší je potřeba chránit jej před potenciálními riziky, jejichž důsledky jsou rozsáhlé:

- Ztráta smluv se zákazníky
- Regulační pokuty
- Krádeže dat / duševního vlastnictví
- Trestněprávní odpovědnost
- GDPR pokuty

Screening pomáhá předcházet podvodům v dodavatelském řetězci.

Kontrolní seznam dodavatelského řetězce:

Před angažováním třetí strany proveďte následující:

- ☐ **Ověření oprávněnosti podnikání:** Ověřte si, zda je společnost třetí strany řádně registrovaná a má dobrou pověst.
- ☐ **Provádějte komplexní kontroly minulosti:** Požadujte, aby dodavatelé prověřovali všechny klíčové pracovníky z hlediska trestní minulosti, finančních rizik a dalších relevantních faktorů.
- ☐ **Ověřte si oprávnění k práci:** Ujistěte se, že všichni pracovníci mají legální oprávnění pracovat v dané zemi.
- ☐ **Monitorování dodržování předpisů:** Provádějte monitoring, abyste zachytili jakékoli změny stavu nebo chování.
- ☐ **Kybernetická bezpečnost:** Ověřte, zda externí dodavatelé mají zavedeny robustní protokoly kybernetické bezpečnosti.
- ☐ **Vyhodnocení finanční stability:** Zkontrolujte finanční stav externích zdrojů, abyste předešli narušením v důsledku finančního selhání.
- ☐ **Posouzení souladu s právními předpisy:** Zajistěte, aby všechny třetí strany dodržovaly příslušné regulace a normy.
- ☐ **Provádění pravidelných auditů:** Naplánujte pravidelné audity pro udržení vysokých standardů a včasnou identifikaci všech hrozeb.