Záver

Bezpečnosť dodávateľského reťazca nie je byrokracia, ale investícia do stability a reputácie organizácie. Aj silné bezpečnostné opatrenia strácajú účinnosť, ak dodávatelia nedodržiavajú primerané štandardy. **Každá reťaz je len taká silná, ako jej najslabší článok** – a útok cez partnera môže paralyzovať celé odvetvie.

Dobrou správou je, že tieto riziká možno zvládnuť. Ak organizácia pozná svojich dodávateľov, má jasné pravidlá, zmluvné požiadavky a pravidelnú kontrolu, výrazne znižuje pravdepodobnosť incidentu. Systematické riadenie dodávateľov prináša odolnosť, kontinuitu a dôveru klientov.

Relevantné právne predpisy, normy a rámce

- Smernica (EÚ) 2022/2555 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii (NIS2)
- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti
- Vyhláška Národného bezpečnostného úradu č. 227/2025 Z. z. o bezpečnostných opatreniach
- ENISA – Agentúra EÚ pre kybernetickú bezpečnosť: Good practices for supply chain cybersecurity.
- STN ISO/IEC 27036-1:2024 Kyberbezpečnosť. Vzťahy s dodávateľmi. Časť 1: Prehľad a koncepty
- STN ISO/IEC 27036-2:2024 Kyberbezpečnosť. Vzťahy s dodávateľmi. Časť 2: Požiadavky
- STN ISO/IEC 27036-3:2024 Kyberbezpečnosť. Vzťahy s dodávateľmi. Časť 3: Pokyny pre bezpečnosť hardvéru, softvéru a služieb dodávateľského reťazca
- STN EN ISO/IEC 27001:2023 Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Systémy manažérstva informačnej bezpečnosti. Požiadavky
- ISO 28000:2022 Ochrana spoločnosti. Systémy manažérstva bezpečnosti. Požiadavky
- ISO 28004-1:2007 Systémy manažérstva bezpečnosti dodávateľského reťazca – Pokyny pre implementáciu normy ISO 28000 – Časť 1: Všeobecné zásady
- NIST SP 800-161 – Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
- GDPR – Nariadenie (EÚ) č. 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (GDPR)
- Nariadenie (EÚ) č. 2554/2022 o digitálnej prevádzkovej odolnosti finančného sektora (DORA)

www.akb.sk | backoffice@akb.sk | 02 208 67 007

Kybernetická bezpečnosť v dodávateľských vzťahoch

AKB
Asociácia kybernetickej bezpečnosti

Dodávateľské reťazce sa stali jedným z najzraniteľnejších prvkov organizácií. Donedávna bol preferovaný biznis model „všetko pod jednou strechou“. Dnes sa organizácie sústreďujú na svoje hlavné činnosti a podporné úlohy odovzdávajú dodávateľom. Tým sa však rozširuje perimeter – a s ním aj počet prístupových bodov, ktoré môže útočník zneužiť. Menšie firmy s obmedzenými zdrojmi na kybernetickú ochranu pritom často disponujú prístupom k interným systémom, dátam či kritickým procesom svojich odberateľov. Riziká sa netýkajú len IT – ohrozené môžu byť dodávky energií, logistika, servis aj poradenstvo.

Legislatívne požiadavky

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti ukladá prevádzkovateľom základnej služby v súvislosti s dodávateľmi dve hlavné povinnosti:

- analyzovať závislosti aktív, informačných systémov, využívaných produktov IKT a služieb IKT tretích strán v dodávateľskom reťazci a poskytovaných služieb s cieľom identifikovať možné dopady kybernetického bezpečnostného incidentu.
- prijímať bezpečnostné opatrenia pre dodávateľský reťazec

Podrobnosti určuje vyhláška č. 227/2025 Z. z. o bezpečnostných opatreniach. Zavádza konkrétne opatrenia pre riadenie dodávateľského reťazca – od posudzovania dodávateľov pred uzatvorením zmluvy, cez zahrnutie bezpečnostných a notifikačných ustanovení do zmlúv, až po priebežný dohľad, kontrolu a audit počas celého trvania zmluvného vzťahu.

Ešte výraznejší dôraz na bezpečnosť dodávateľského reťazca prináša nariadenie EÚ č. 2554/2022 o digitálnej prevádzkovej odolnosti finančného sektora (DORA). Toto je zamerané najmä na finančný sektor a kladie dôraz na riadenie rizík tretích strán a dohľad nad poskytovateľmi IKT služieb.

Zodpovednosť organizácie za kybernetickú bezpečnosť nekončí na hranici jej vlastných systémov.

Bezpečnosť dodávateľského reťazca podľa normy

Medzinárodná technická norma ISO 28000:2022 chápe bezpečnosť dodávateľského reťazca ako súčasť celkového systému riadenia organizácie – nie izolovanú aktivitu, ale trvalý proces hodnotenia, kontroly a zlepšovania. Tento proces zahŕňa:

- **Identifikáciu procesov a aktivít** – organizácia má presne určiť, ktoré činnosti a služby sú kľúčové pre fungovanie dodávateľského reťazca a kde by incident mohol spôsobiť kritické škody.
- **Analýza rizík** – pre každý kritický prvok reťazca je potrebné posúdiť pravdepodobnosť hrozby a dopady, ak by sa dodávateľ alebo jeho služby stali nedostupnými či ohrozenými.
- **Zavedenie opatrení** – od technických cez organizačné až po fyzické a personálne.
- **Riadenie externých poskytovateľov** – norma kladie dôraz na to, aby organizácia mala kontrolu nad procesmi a službami subdodávateľov, ktorí môžu ovplyvniť úroveň kybernetickej bezpečnosti.
- **Neustále zlepšovanie** – proces riadenia bezpečnosti nie je jednorazová úloha, ale cyklický prístup, ktorý sa opiera o meranie výkonnosti, audity, testovanie a aktualizáciu opatrení.

Cieľom je dosiahnuť, aby celý dodávateľský reťazec fungoval ako odolný systém, kde aj v prípade incidentu u jedného článku nedôjde k dominovému efektu s vážnymi dôsledkami na organizáciu.

Kľúčové zásady

Riadenie dodávateľských vzťahov musí byť systematické a založené na jasne definovaných postupoch. Nasledujúce zásady predstavujú minimálny štandard, ktorý by mala každá organizácia dodržiavať.

Analýza rizík

Pred spoluprácou si overte úroveň bezpečnosti dodávateľa. Posúďte jeho procesy, certifikácie, skúsenosti a referencie – rovnako, ako by ste preverili partnera, ktorému zverujete dôležitú časť svojho biznisu.

Zmluvné požiadavky

Zmluva má jasne určiť bezpečnostné pravidlá: povinnosť hlásiť incidenty, udržiavať systémy aktuálne, umožniť audit a dodržiavať stanovené štandardy.

Obmedzenie prístupov

Dodávateľ má mať prístupové práva len tam, kde je to nevyhnutné. Menej prístupov znamená menšie riziko.

Priebežné overovanie

Podpisom zmluvy posudzovanie úrovne bezpečnosti nekončí. Spoluprácu treba pravidelne kontrolovať – cez reporty, testy alebo audity – a včas riešiť zistené nedostatky.

Pripravenosť na incidenty

Nulové riziko neexistuje. Incidenty sa stávajú. Spoločný plán reakcie a jasná komunikácia urýchlia riešenie a minimalizujú škody.

Kompatibilita a aktualizácie

Nové systémy musia fungovať s existujúcimi riešeniami a mať zabezpečené pravidelné aktualizácie počas celej životnosti služby.

Praktický návod – ako začať

Prechod k systematickému riadeniu dodávateľov nevyžaduje zložité procesy. Stačí postupovať krok za krokom:

Zmapujte dodávateľov a stanovte priority

Vytvorte prehľad všetkých partnerov a služieb, ktoré poskytujú, a určte ich dôležitosť pre fungovanie vašej organizácie. Kritickým dodávateľom venujte pozornosť ako prvým. Takto môžete už v krátkom čase znížiť najväčšie riziká.

Posúďte úroveň bezpečnosti dodávateľov

Zistite, aké majú dodávatelia implementované bezpečnostné opatrenia. Pomôže dotazník, audit alebo hodnotiace skóre.

Stanovte minimálne požiadavky

Definujte základné technické štandardy na bezpečnosť – napríklad šifrovanie komunikácie, viacfaktorovú autentifikáciu, hlásenie incidentov.

Zahrňte kyberbezpečnosť do zmlúv

Bezpečnostné a oznamovacie povinnosti musia byť súčasťou zmluvy. Pri jej zmene pravidelne kontrolujte, či zostávajú aktuálne.

Monitorujte a vyhodnocujte

Nastavte pravidelné hodnotenie dodávateľov – napríklad raz ročne alebo po väčšej zmene systému či služby.

Priebežne zlepšujte proces

Na základe skúseností a auditov aktualizujte hodnotiace kritériá aj zmluvné požiadavky.