UDRŽITELNOST PRO VÝROBU A OBCHOD

Udržitelnost, která se vyplatí

KYBERNETICKÁ BEZPEČNOST V RETAILU A JEHO DODAVATELSKÝCH ŘETĚZCÍCH

JINDŘICH KALÍŠEK

Founder & CEO regfor

kalisek@regfor.cz

WHOIS:

Jindřich Kalíšek

- CEO a architekt compliance nástroje regfor (regfor)
- Advokát (CYBERLAWYER)
- Vysokoškolský učitel (Právnická fakulta UK)

- Člen Sekce pro umělou inteligenci a nové technologie České advokátní komory
- Člen Spolku pro ochranu osobních údajů a předseda Komise pro kyberbezpečnost

RETAIL UŽ NENÍ „JEN OBCHOD“

- Retail dnes stojí na datech, systémech, včasné a efektivní logistice a dodavatelích
- Výpadek IT může znamenat výpadek prodeje, skladů, e-shopu nebo plateb
- Rizikem nejsou jen hackeři, ale i selhání dodavatele, chybné přístupy nebo špatně řízená data

Kyberbezpečnost je klíčové téma provozní, obchodní i reputační

RETAIL A DIGITÁLNÍ REGULATORIKA

- Čtyři vertikály digitální compliance
  - > Kyberbezpečnost a digitální odolnost
  - > Ochrana dat a osobních údajů
  - > Digitální služby a jednání
  - > Umělá inteligence
- Nový zákon o kybernetické bezpečnosti
  - > Účinný od 1. 11. 2025 → **reálné dopady v 2027**
  - > Primární dopady do retailu v potravinářství, logistice, výrobě anebo digitálních službách
  - > Sekundární dopady přes roli v dodavatelském řetězci
  - > Rozhodující je poskytovaná služba, velikost a význam podniku → **samoidentifikace**

CO MUSÍTE UŘÍDIT?

- **Aktiva:** systémy, data, identity, provozy, sklady, e-shop, ERP, pokladní a platební prostředí
- **Rizika:** ransomware, výpadky, únik dat, zneužití účtů, kompromitace dodavatelů
- **Přístupy:** kdo má k čemu přístup, proč, na jak dlouho a jak se oprávnění kontrolují
- **Incidenty:** detekce, eskalace, hlášení, obnova provozu
- **Kontinuita:** zálohy, krizové scénáře, náhradní provoz a testování obnovy

PÁR MÉNĚ ZNÁMÝCH ČÍSEL

$ 53 000	Průměrné náklady na mitigaci kybernetického útoku na organizaci s více než 1 000 zaměstnanci (v USA nebo v Evropě)
4	Průměrný počet kybernetických útoků na organizaci v 1 roce
90 %	Podíl kybernetických incidentů, které jsou výsledkem lidské chyby nebo chování (např. slabá hesla, nerozpoznání phishingu)
98 %	Podíl kybernetických útoků, které využívají sociální inženýrství (např. phishing nebo baiting)

Zdroj: SentinelOne, 15. 1. 2026, online

A PÁR JEŠTĚ MÉNĚ ZNÁMÝCH ČÍSEL

SPOLEČNOST VE FORTUNE 500 MÁ PRŮMĚRNĚ **66 000 ZAMĚSTNANCŮ** A **5 000 DODAVATELŮ**

Zdroj: Team Cymru, 29. 10. 2025, online.

DODAVATELSKÝ ŘETĚZEC JE SLABÉ MÍSTO

- **Proč?** Retail je závislý na IT dodavatelích – v ukládání a zpracování dat (cloud), logistice, platebních službách anebo marketingu
- **Motivace útočníka?** Incident u dodavatele může zastavit provoz stejně efektivně jako útok na cílovou infrastrukturu, ale levněji a s většími dopady
- **Jak ne?** „Stačí“ smlouva a NDA **→ je nutné znát bezpečnostní úroveň klíčových dodavatelů a aktivně řídit jejich rizika**
- **Jak ano?** Aktivní řízení dodavatelských rizik a nadto bezpečnostní záruky ve smlouvách **→ bezpečnostní minimum (nejlépe v několika úrovních)**

HODNOTÍTE DODAVATELE?

- **Kritičnost:** bez kterých dodavatelů nelze prodávat, dodávat nebo obsluhovat zákazníky?
- **Přístup:** má dodavatel přístup k systémům, datům, infrastruktuře nebo zákazníkům?
- **Dopad:** co se stane při výpadku, úniku dat nebo zneužití účtu dodavatele?
- **Kontroly:** certifikace, bezpečnostní dotazník, audit, incident reporting, testování obnovy
- **Smlouvy:** minimální bezpečnostní požadavky, SLA, odpovědnost, subdodavatelé, exit plán

TYPICKÉ MEZERY V RETAILU

- Legacy systémy, procesy a compliance maturity
  - > Morálně zastaralé systémy → **spolehlivě plní své funkce, ale bezpečnostně nevyhovují**
  - > Ve starších smlouvách chybí bezpečnostní požadavky
  - > Neexistující anebo zastaralé vzdělávání v oblasti kyberbezpečnosti
- Slabá evidence dodavatelů a jejich přístupů
- Sdílené nebo historické účty externistů
- Nedostatečně testované zálohy a obnova provozu
  - > Zaměstnanci nejsou dostatečně trénováni na scénáře dlouhodobého kyberbezpečnostního incidentu anebo havárie technologií
- Incident reporting není nacvičený a role nejsou jasné

DIGITALIZACE A AUTOMATIZACE COMPLIANCE

- Evidence služeb, aktiv, dodavatelů a rizik na jednom místě
- Automatizované dotazníky a sběr podkladů od dodavatelů
- Workflow pro schvalování výjimek, nápravných opatření a akceptaci rizik
- Dashboard pro compliance a vedení: kritická rizika, stav opatření, otevřené úkoly

www.regfor.cz

Méně tabulek, více řízení a lepší důkazní stopa

LETNÍ DIGITÁLNÍ COMPLIANCE PROJEKT

- Ověřit, zda podnik poskytuje regulovanou službu
  ← Portál NÚKIB
- Zmapovat kritické systémy, data, procesy a dodavatele
  ← brainstorming / workshop, dotazníkové šetření, řízené rozhovory s vlastníky procesů
- Určit vlastníka programu a zapojit vrcholové vedení
  ← úvodní boardroom trénink
- Provést expoziční / gap analýzu vůči požadavkům nových regulací **← „nějaká je lepší nežli žádná“**
- Nastavit plán opatření podle identifikovaných rizik, ne podle formálního checklistu
  ← „bezpečnost je cesta, ne stav“

MÍT → UMĚT → DOKÁZAT

Kyberbezpečnost a BDŘ jsou součástí řízení provozní odolnosti celého obchodního ekosystému

- Začněte službou, ne směrnicí
- Řiďte dodavatele podle jejich skutečného dopadu
- Automatizujte evidenci, workflow a reporting
- Připravte se na incident dřív, než nastane

UDRŽITELNOST PRO VÝROBU A OBCHOD

Udržitelnost, která se vyplatí

DOTAZY? PŘIPOMÍNKY? POŽADAVKY?

JINDŘICH KALÍŠEK

Founder & CEO regfor

kalisek@regfor.cz