ELEKTRONICKÝ

SPEDIČNÍ ZPRAVODAJ

VIII/2025

SVAZ SPEDICE A LOGISTIKY ČESKÉ REPUBLIKY
Zapsaný spolek
ASSOCIATION OF FORWARDING & LOGISTICS
OF THE CZECH REPUBLIC-MEMBER OF FIATA

Obsah:

info@svazspedice.cz
Sekretariát Svazu spedice a logistiky ČR, z.s.
1.pluku 8a, 18600 Praha 8 – Karlín
tlf. 224 891 303
Internet: www.svazspedice.cz

TÉMA: Software nejen jako nástroj ke zpracování dat

1. Úvod

Tlak na vyšší efektivitu ze strany speditérů a poskytovatelů logistických služeb roste: Mnoho zákazníků je stále náročnějších. Jejich náklady rostou. Trpí ekonomickou slabostí. I když chybí rentabilní využití kapacit a kompetentní specialisté, due diligence zabírá příliš mnoho času. Řízení rizik, digitální podpora a sdílené znalosti se proto stávají konkurenčními faktory

2. Kvalita softwarového řešení

Když říkáte software, myslíte tím víc než jen programový kód. V logistice to nejsou technologie, které určují pokrok, ale jejich vliv na procesy, lidi a odpovědnost. Digitalizace musí umožnit zvládnutí procesů. Přitom nabízí orientaci a vytváří základ pro důvěru – od jednotlivých objednávek až po celé dodavatelské řetězce. Vlnu digitální transformace již nelze zastavit. Pokud v digitálním prostředí chcete surfovat, potřebujete aplikace, které identifikují rizika v rané fázi, strukturovaně mapují povinnosti a zabezpečují rozhodnutí. Ať už při plánování, manipulaci nebo na rampě: každý, kdo zavádí digitální systémy, zasahuje do rutiny a někdy dokonce přetváří provozní základ obchodní jednotky.

Články v mnoha periodicích ukazují, co dokážou moderní softwarová řešení: jako platforma pro kontakt se zákazníky, jako nástroj pro splnění regulatorních požadavků nebo jako obraz manipulačních procesů v reálném čase. Pomáhají snižovat složitost, zavádět spolehlivost a překlenout úzká místa. Především však vracejí kvalifikovaným pracovníkům to, co jim často nejvíce chybí: přehled, čas a důvěru v jednání. Kvalita softwarového řešení se měří jeho schopností zjednodušit složité procesy v každodenním podnikání. Digitální aplikace se tak staly strategickým zdrojem. Ti, kteří je integrují se smyslem pro proporce, získají více než efektivitu: vytvoří struktury, které nabízejí budoucí bezpečnost v prostředí založeném na datech.

3. Malé a střední podniky musí zlepšit svou bezpečnost IT

Pozorujeme, že naše odvětví se stále více stává terčem kybernetických útoků," uvádí Ralf Wieland, generální ředitel společnosti Emons Spedition se sídlem v Kolíně nad Rýnem. Během

dvouletého projektového období jeho společnost zavedla systém řízení kontinuity podnikání (BCM), který zajišťuje, že poskytovatel služeb může i v případě nouze – tj. v případě selhání IT systémů – nadále plnit své závazky vůči vlastním zákazníkům beze změny. Za tímto účelem vypracoval poskytovatel logistických služeb havarijní plány, vybavil nouzové případy speciálním hardwarem pro poruchy systému a vytvořil redundance, které mohou nahradit produktivní systém se základními funkcemi.

Spolkový svaz speditérů a logistiky DSLV výslovně vítá skutečnost, že směrnice EU o bezpečnosti sítí a informací (NIS-2) nepřináší podle současného stavu německého legislativního procesu pro většinu speditérů žádné přímé povinnosti. Nicméně z pohledu asociace je naprosto vhodné zabývat se účinnými opatřeními pro mimořádné události. "Důrazně doporučujeme přijmout organizační opatření pro krizové řízení – nejen velké společnosti, ale zejména středně velké společnosti," zdůrazňuje Niels Beuck, zástupce generálního ředitele DSLV.

"Mnoho zejména malých podniků zjevně podceňuje rizika," říká Wieland a uvádí osobní příklad: "Když jsme s projektem začínali, nedokázal bych odpovědět na některé jednoduché otázky – například jak se spojit se všemi zaměstnanci po telefonu." Společnost Emons se nyní připravila nejen na kybernetické útoky, ale také na přírodní rizika a další eventuality, jako jsou výpadky proudu. "Díky mobilním technologiím, jako je 5G, můžeme zůstat online, i když nám bagr přeruší datové linky," říká s odkazem na událost, ke které již došlo na několika místech. Na jaře zažil generální ředitel na místě velký výpadek proudu ve Španělsku a Portugalsku. "Ale něco takového by také paralyzovalo počítačové sítě v této zemi," je přesvědčen.

Aby se zajistil proti svým řizikům, poskytovatel služeb se sídlem v Kolíně nad Rýnem investoval značné prostředky, vysokou šestimístnou částku do projektu na zřízení BCM a od té doby pětimístnou měsíční částku za provoz nadbytečného produktivního prostředí. Společnost Emons se také spoléhá na podporu externích poskytovatelů služeb: poskytovatel školení Sosafe zvyšuje citlivost zaměstnanců na vědomé řešení situace hrozeb, poskytovatel IT služeb

Eikona udržuje nouzové řešení připravené k použití a průběžně kontroluje operační systém na zranitelnosti.

4. Bezpečnostní situace se zhoršuje

Sdružení Cargoline také zpřesnilo své chápání bezpečnosti kvůli skutečným útokům. Konkrétním spouštěčem byl dlouhotrvající kybernetický incident v partnerské společnosti před lety, který byl nápomocný při vývoji vlastního systému krizového řízení. "Každému musí být jasné, že neexistuje žádná 100% ochrana – rozhodujícím faktorem je, jak se vypořádat se zbytkovým rizikem," zdůrazňuje člen představenstva Cargoline Sebastian Grollius. Situace s hrozbami se podle něj změnila nejen kvantitativně, ale i kvalitativně. Zatímco dříve převládaly plošné útoky, počet cílených útoků na určité regiony nebo skupiny firem nyní znatelně roste. Z tohoto důvodu je systém BCM společnosti Cargoline zcela oddělen od primárního IT, aby fungoval bez narušení v případě nouze.

Taková mimořádná situace zasáhla německý obchod Švýcarské pošty v oblasti všeobecné nákladní dopravy na jaře v závodě Aldingen v Bádensku-Württembersku. Kromě Cargoline je tamní společnost aktivní i v další spolupráci v oblasti všeobecné nákladní dopravy. Protože však posledně jmenovaná, na rozdíl od Cargoline, neprovozuje nouzový systém, musela Švýcarská pošta prozatím přerušit spolupráci v oblasti Schwarzwaldu. "To, že společnost zůstala v provozu, pro nás bylo zásluhou BCM," říká Grollius.

Jeho síť pravidelně testuje nouzový systém, který pochází i od Eikony: Každý partner v síti je povinen každé tři měsíce používat záložní technologii v ostrém provozu – včetně připraveného náhradního hardwaru. Jedině tak lze zabránit tomu, aby se na systém "prášilo ve skříni a nikdo nevěděl, jak jej v den X používat".

Grollius zdůrazňuje, že efektivní BCM je úloha řízení, která má velký význam: "Redundance představuje přibližně 35 procent našeho rozpočtu na IT."

5. Pojišťovny chtějí důkaz

Pro malé a střední speditéry může kybernetický útok ohrozit jejich existenci, pokud se nepřipravili preventivními opatřeními. Sedmimístné ztráty nejsou v případě nouze nic neobvyklého, říká Thomas Wicke, generální ředitel pojišťovací makléřské společnosti Schunck Group, která se specializuje na dopravu a logistiku, a sám oběť kybernetického útoku. Nejdůležitější ochranou proti útoku není ani technologie, ani pojištění. Pak rozhoduje dobrá

organizace. "Pokud víte, kteří poskytovatelé služeb pomohou v případě nouze a rychle zahájí krizové řízení, nejlepším způsobem, jak se dostat přes útok, je udělat to," poznamenává Wicke. "Ti, kteří nepoužívají současné systémy, neumí dokázat řízení aktualizací nebo neprezentují krizové a restartové plány, jsou často odmítáni," uvádí šéf Schuncku.

Pro úspěšné žádosti by proto měly být zapojeny také partnerské sítě a poskytovatelé krizových služeb. Ti, kteří tyto požadavky splní, se však mohou pojistit za zvládnutelné náklady: U 90 procent klientů Schunck se pojistné v kybernetickém pojištění pohybovalo mezi 10 000 a 100 000 eury ročně, v závislosti na složitosti použitých IT systémů a jejich standardu technické ochrany. Spolupráce s pojišťovnou pak poskytuje nejen finanční podporu, ale také nabízí přístup k profesionální nouzové pomoci, "od forenzních expertů zajišťujících důkazy až po specialisty na vyjednávání o výkupném," říká Wicke

6. Logistika potřebuje datovou strategii

EU vytváří nová pravidla pro přístup k údajům a jejich využívání. S nařízením (EU) 2023/2854, tzv. aktem o datech, vstoupí od 12. září 2025 v platnost ambiciózní soubor pravidel, který se dotkne zejména logistického průmyslu v jeho síťově propojené struktuře založené na datech. To, co na první pohled zní jako právní teorie, má v praxi značné důsledky: Podniky, které používají propojené produkty, budou muset v budoucnu zajistit, aby data o produktech, která v tomto procesu vzniknou, mohla být k dispozici buď přímo uživateli, nebo třetím stranám. To platí také pro systémy poskytovatelů logistických služeb, od nákladních vozidel s telematickými systémy až po inteligentní nosiče nákladu. Zákon o ochraně osobních údajů tak specifikuje nejen technické požadavky, ale definuje i právní nárok na využití údajů – například obchodními partnery nebo poskytovateli služeb v dodavatelském řetězci. Vyžaduje nejen dodržování pravidel, ale stává se i tvrdým nástrojem obchodního práva.

Suverenita a dostupnost dat Akt o datech s sebou přináší zásadní posun: od výlučné kontroly nad daty ze strany výrobců nebo poskytovatelů platforem směrem k ekonomice sdílení dat s jasnými pravidly, právy a povinnostmi. Pro logistiku jsou důležité zejména tři aspekty:

■ Přístup k údajům o používání: Nařízení ukládá výrobcům povinnost technicky umožnit přístup k datům a zpřístupnit je uživateli zdarma – například prostřednictvím standardizovaných rozhraní. Oprávněným třetím stranám, jako jsou provozovatelé vozových parků a poskytovatelé logistických služeb, může být účtován přiměřený poplatek.

■ Povinnosti držitelů dat: Každý, kdo získá přístup k datům, musí dodržovat přísná pravidla s důvěrností, omezením účelu a zákazem vyvíjet z nich vlastní konkurenční produkty. To vytváří důvěru, ale také vyžaduje struktury řízení.

■ Povinnosti příjemců údajů: Každý, kdo obdrží údaje, například pro optimalizaci přepravních řetězců nebo pro prediktivní údržbu, musí zaručit jejich ochranu a správné použití.

Požadavky zákona o ochraně osobních údajů nejsou v rozporu s ochranou osobních údajů podle obecného nařízení o ochraně osobních údajů (GDPR). Soubor pravidel je složitý, ale sleduje jasný cíl, kterým je umožnit inovace prostřednictvím sdílení dat za spravedlivých podmínek. Aby se tato transformace podařila, je zapotřebí most mezi právními předpisy a logistickou praxí. A právě zde přichází na řadu Open Logistics Foundation.

Jako neutrální základ a znalostní platforma připravuje regulační vývoj praktickým způsobem pro své členy a celé odvětví. To zahrnuje konkrétní pokyny pro činnost a pomůcky pro rozhodování. Právě proto, že mnoho podniků si stále není jisto, na co si dát pozor při používání síťových systémů a uzavírání odpovídajících smluv v souladu s požadavky zákona o datech, potřebují se orientovat.

Týká se to všech společností, a proto by si měly již dnes začít odpovídat na následujících pět otázek:

■ Kdo a kde používá které propojené produkty?

■ Jaké údaje jsou v něm zpracovávány?

■ Kdo vlastní a používá data v mém ekosystému?

■ Kdo by měl mít přístup k údajům – a kdo ne?

■ Jak lze smluvně zabezpečit výměnu údajů se všemi zúčastněnými stranami?

Zejména vyhledávání propojených produktů musí být přesné. Rozhodující je, že se jedná o síťový produkt ve smyslu zákona o datech, který je připojen k internetu nebo jiným sítím a systematicky přenáší data.

V logistice je jich spousta, a to nejen vozidla s telematickými systémy nebo výše zmíněné chytré nosiče nákladu a nakládací zařízení. Mobilní zařízení řidičů, síťově propojené závory, teplotní senzory ve skladu a mnoho dalších mohou také splňovat definici a podléhat nařízení. Aktem o datech, aktem o správě dat pro bezpečné datové toky ve sdílených datových prostorech, aktem o umělé inteligenci o bezpečnosti, kontrole a odpovědnosti za umělou inteligenci a dalšími projekty vytváří EU digitální vnitřní řád. Tento vývoj se dotýká všech společností, od speditérů přes výrobce vozidel nebo produktů až po IT platformy. Každý, kdo v této souvislosti jedná izolovaně, se vystavuje riziku, že ztratí kontakt nebo mu vzniknou

vysoké následné náklady. Aktéři proto musí rozvíjet nové formy spolupráce pod neutrálním deštníkem, který spojuje jak technické know-how, tak právní porozumění.

Meziodvětvové, neutrální platformy, jako je Open Logistics Foundation, mohou k tomu poskytnout vhodnou strukturu. Organizace nejen podporuje své členy technickým otevřeným zdrojovým kódem, ale také včas rozpoznává právní požadavky, činí je srozumitelnými a společně vypracovává řešení.

Zákon o datech vytváří novou realitu v logistice. Ti, kteří se tomu nepřizpůsobí, riskují zbytečné tření, ztráty nebo dokonce smluvní konflikty. Kdo se včas chopí iniciativy, může nejen ochránit sebe, ale také si zajistit konkurenční výhody díky transparentním datovým strukturám, procesům v souladu s právními předpisy a novým digitálním obchodním modelům. Za tímto účelem by společnosti měly doplnit svou strategii digitalizace o konkrétní datovou strategii, která jim umožní implementovat Akt o datech a jeho evropské sesterské předpisy.

7. Závěr

Opět se potvrzuje jedno nepříjemné pravidlo: Evropská komise má za vlastní zregulovat podnikání v regionu, jak jen to bude možné. Velké korporace se samozřejmě opět s tímto nařízením popasují, ale segment SME (malé a střední podniky) budou opět o stupeň více ohroženy. Snad i ony najdou cestu …

Konec VIII. čísla

Příjemné pokračování léta vám přeje Redakce SZ SSL