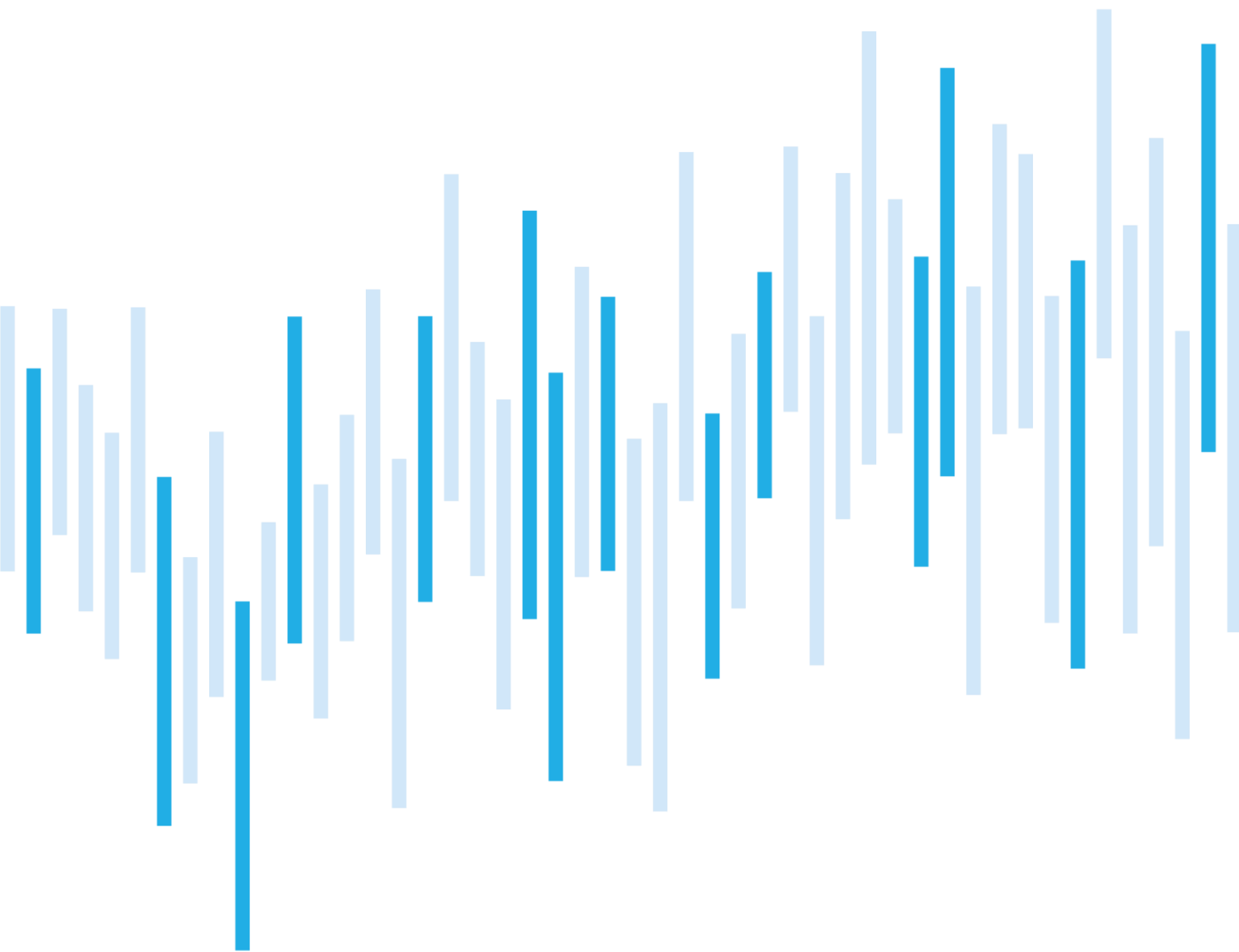


Kybernetické incidenty pohledem NÚKIB

BŘEZEN 2025



Shrnutí měsíce

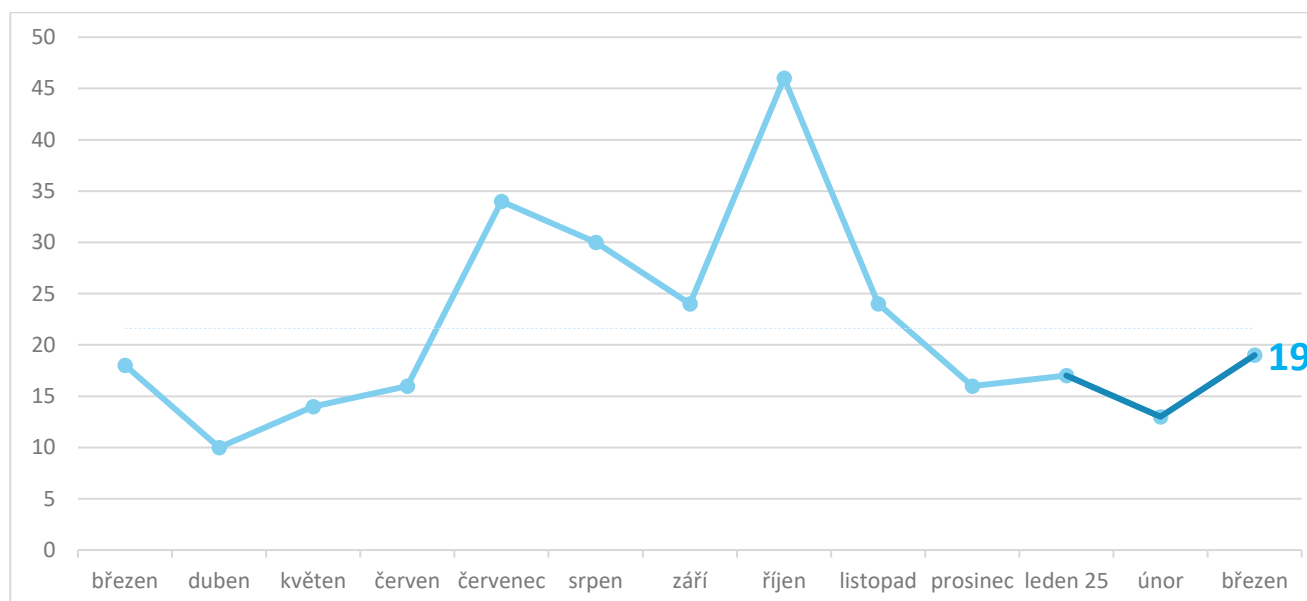
Během března NÚKIB evidoval 19 kybernetických bezpečnostních incidentů. Oproti únoru se tak jedná o mírný nárůst. Nejvíce zastoupenou kategorií byla Informační bezpečnost (7), následována kategorií Průnik (4). Tradičně nejpočetnější kategorie Dostupnost byla v březnu zastoupena pouze třemi incidenty, ve všech případech se jednalo o DDoS útoky. Dále NÚKIB evidoval dva incidenty kategorie Škodlivý kód, dva případy Podvodu a jeden Pokus o průnik.

Kategorie Informační bezpečnost byla v březnu tvořena šesti ransomwarovými útoky a jednou exfiltrací dat s následným vydíráním oběti. Hlavním trendem března tak byl nárůst počtu ransomwarových útoků. Stejně jako koncem minulého roku se však jednalo o rozdílné aktéry, nikoliv ucelenou kampaň.

Pohledem závažnosti byl jeden ransomwarový útok klasifikován jako významný, jelikož směřoval na městskou samosprávu. Ačkoliv úspěšný, data bylo možné obnovit ze zálohy. Jako velmi významný incident byl poté klasifikován ransomwarový útok na systémy Hasičského záchranného sboru ČR, konkrétně v Královéhradeckém a Zlínském kraji. Zbylých 17 incidentů bylo vyhodnoceno jako méně významné.

Kybernetických událostí bylo v březnu evidováno pět. Ve čtyřech případech se jednalo o neúspěšné pokusy o phishing či spear-phishing, vesměs s cílem finančního zisku či sběru přihlašovacích údajů. Pátá událost se týká úniku dat společnosti Oracle, na který jsme upozornili na [Portálu NÚKIB](#).

Počet kybernetických bezpečnostních incidentů evidovaných NÚKIB



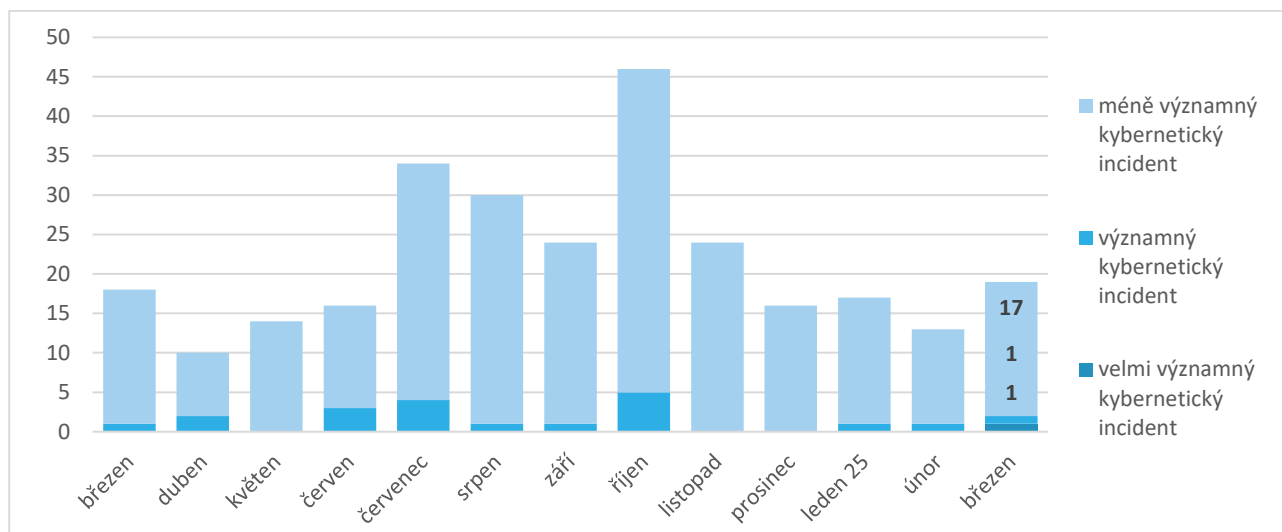
Následující přehled shrnuje dění za daný měsíc. Data, informace a závěry v něm obsažené primárně vychází z evidence NÚKIB. Pokud přehled v některých částech obsahuje informace z otevřených zdrojů, je původ těchto informací vždy uveden.

V některých případech může zpětně docházet k rekválifikaci hodnot v rámci evidence incidentů, může tedy dojít ke změně historických údajů v zobrazovaných grafech.

Připomínky a náměty na zlepšení reportu můžete posílat na adresu komunikace@nukib.gov.cz.

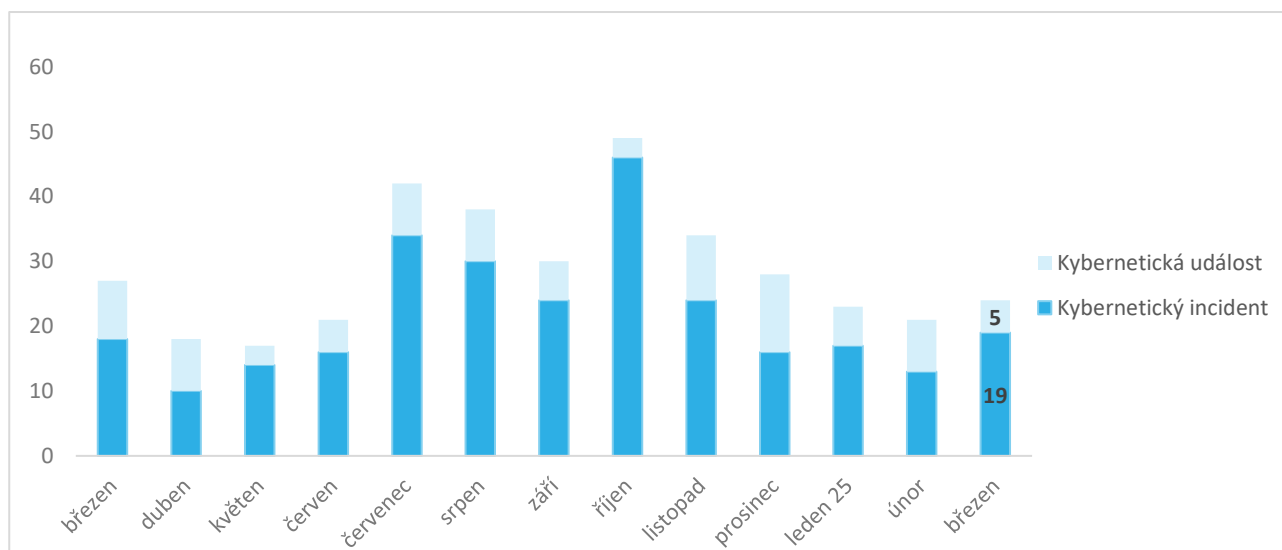
Závažnost evidovaných kybernetických incidentů

Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, a v interní metodice NÚKIB.



Poměr evidovaných kybernetických incidentů a kybernetických událostí¹

NÚKIB v rámci své činnosti přijímá, zpracovává a vyhodnocuje hlášení kybernetických incidentů. Na základě provedené analýzy může být hlášení klasifikováno jako kybernetický incident, kybernetická událost nebo jako nerelevantní podnět. Graf níže ukazuje poměr kybernetických incidentů a kybernetických událostí.



¹ Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.

Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.

Oba pojmy definuje [zákon o kybernetické bezpečnosti](#).

Klasifikace incidentů nahlášených NÚKIB

Klasifikace kybernetických incidentů je založena na taxonomii ENISA: [Reference Incident Classification Taxonomy — ENISA \(europa.eu\)](#). Grafy zobrazují procentuální zastoupení jednotlivých kategorií v daných měsících za uplynulý rok. Procentuální číselná hodnota zobrazuje poměr dané kategorie vůči ostatním v tomto měsíci.

2024

2025

Dostupnost – např. narušení dostupnosti způsobené DoS/DDoS útokem nebo sabotáží



Informační bezpečnost – např. neautorizovaný přístup k datům, neautorizovaná změna informace



Průnik – např. kompromitace aplikace nebo uživatelského účtu



Škodlivý kód – např. virus, červ, trojský kůň, dialer, spyware



Podvod – např. phishing, krádež identity nebo neoprávněné využití ICT



Ostatní

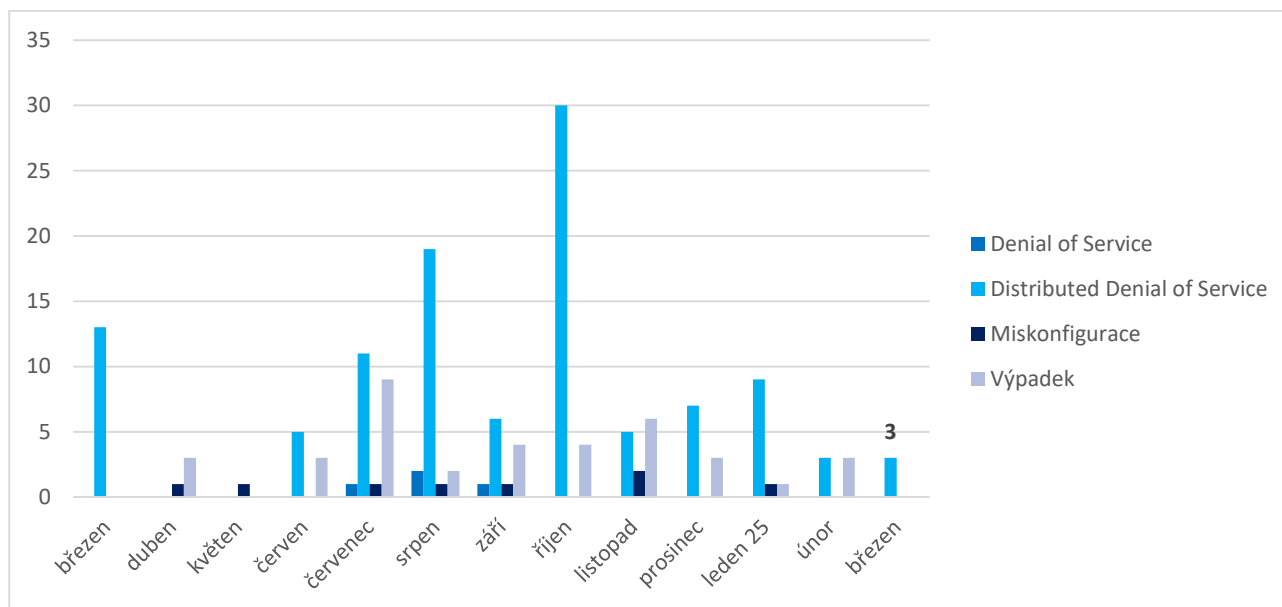


Počet evidovaných incidentů ve vybraných kategoriích

Níže uvedené kategorie jsou vybrány zejména z důvodu jejich dlouhodobé četnosti (Dostupnost) či závažnosti (Informační bezpečnost).

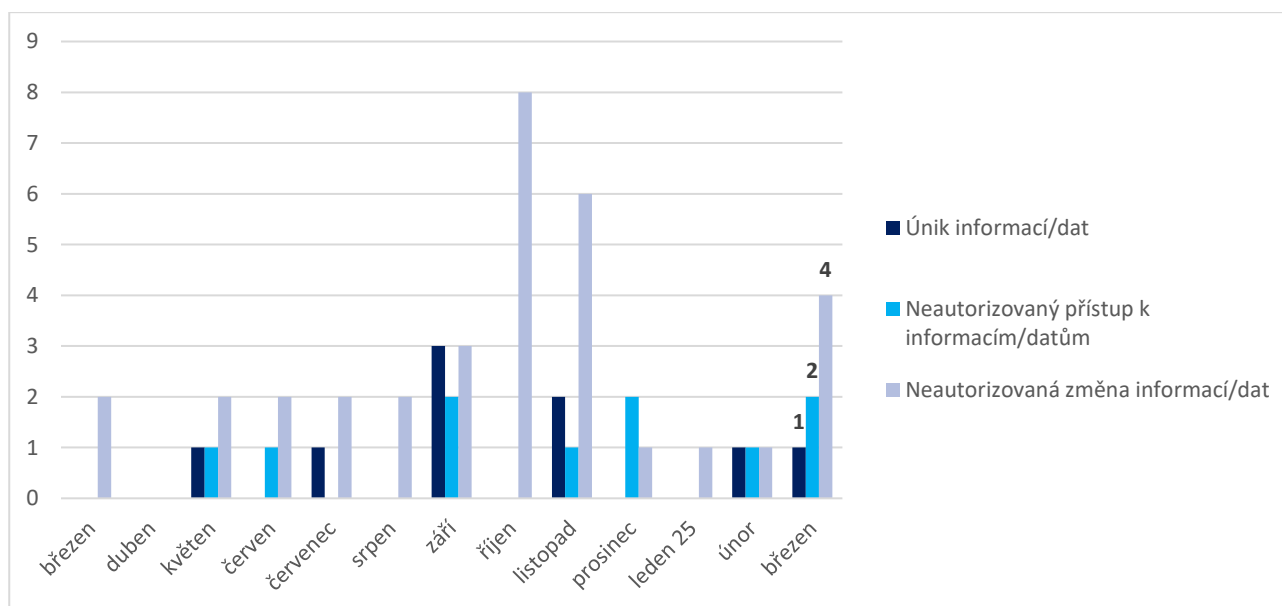
Dostupnost

Kategorie Dostupnost je primárně tvořena DDoS a DoS útoky, nicméně obsahuje i výpadky dostupnosti způsobené technickou závadou či miskonfigurací a neoprávněnou manipulací.



Informační bezpečnost

Kategorie Informační bezpečnost je tvořena primárně ransomwarovými útoky (zpravidla řazenými do podkategorie Neautorizovaná změna informací/dat), nicméně obsahuje také podkategorie i Neautorizovaný přístup k datům a systémům či Únik informací.



Použité pravděpodobnostní výrazy

Pravděpodobnostní výrazy a vyjádření jejich procentuálních hodnot:

Výraz	Pravděpodobnost
Téměř jistě	90–100 %
Velmi pravděpodobně	75–85 %
Pravděpodobně	55–70 %
Nelze vyloučit/Reálná možnost	40–50 %
Nepravděpodobně	15–35 %
Velmi nepravděpodobně	0–10 %

Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách nukib.gov.cz). Informace je označena příznakem, který stanoví podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
TLP:RED	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
TLP:AMBER+STRICT	Informace může být sdílena pouze v rámci organizace příjemce, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
TLP:AMBER	Informace může být sdílena v rámci organizace příjemce a jejím partnerům, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
TLP:GREEN	Informace může být sdílena v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
TLP:CLEAR	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.