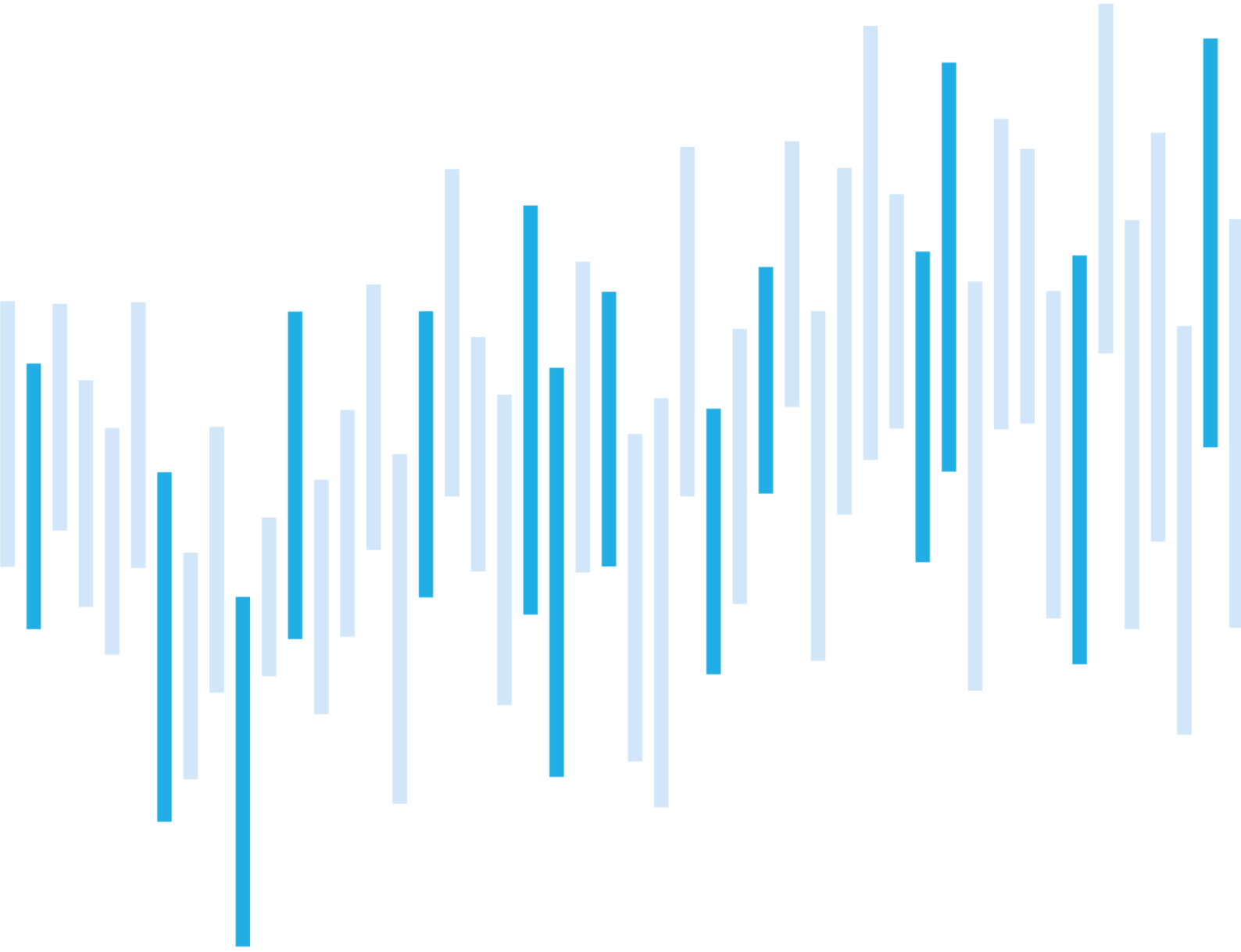
Kybernetické incidenty pohledem NÚKIB

ZÁŘÍ 2024



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

V září NÚKIB evidoval 21 incidentů, oproti oběma letním měsícům tak došlo ke snížení hodnot na průměrné roční hodnoty. Pouze jeden z incidentů byl klasifikován jako významný, zbylých 20 bylo pouze méně významných.

I nadále hlavní kategorií zůstává Dostupnost. V září ji však tvořily zejména incidenty spojené s technickou závadou, v některých případech ve spojitosti s výpadky elektrických dodávek během záplav či přímo jejich vlivem.

V kapitole Zaměřeno na hrozbu se tentokrát věnujeme odhalení phishingové kampaně vůči účastníkům mezinárodní bezpečnostní konference IISS – Prague Defence Summit, která je vedena dosud neznámým útočníkem. Nicméně vzhledem k významnosti události nelze vyloučit (40–50 %), že je vedena státním aktérem s cílem získat zpravodajské informace.

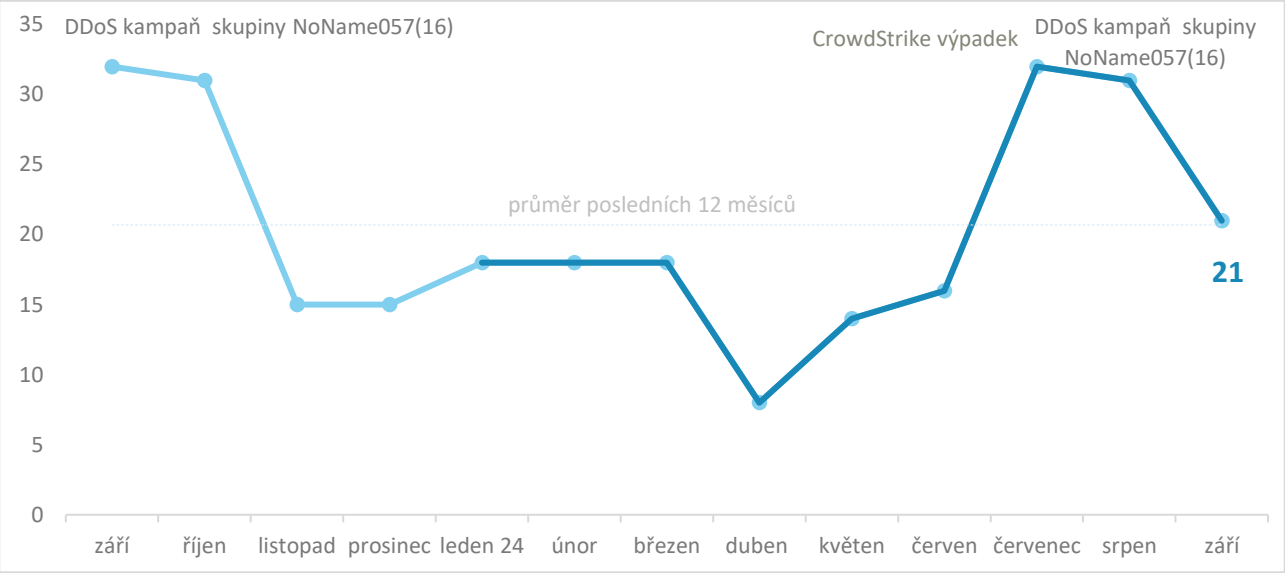
Obsah

Následující report shrnuje dění měsíce. Data, informace a závěry v něm obsažené primárně vychází z kybernetických incidentů nahlášených NÚKIB. Pokud report v některých částech obsahuje informace z otevřených zdrojů, je vždy uveden původ těchto informací.

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

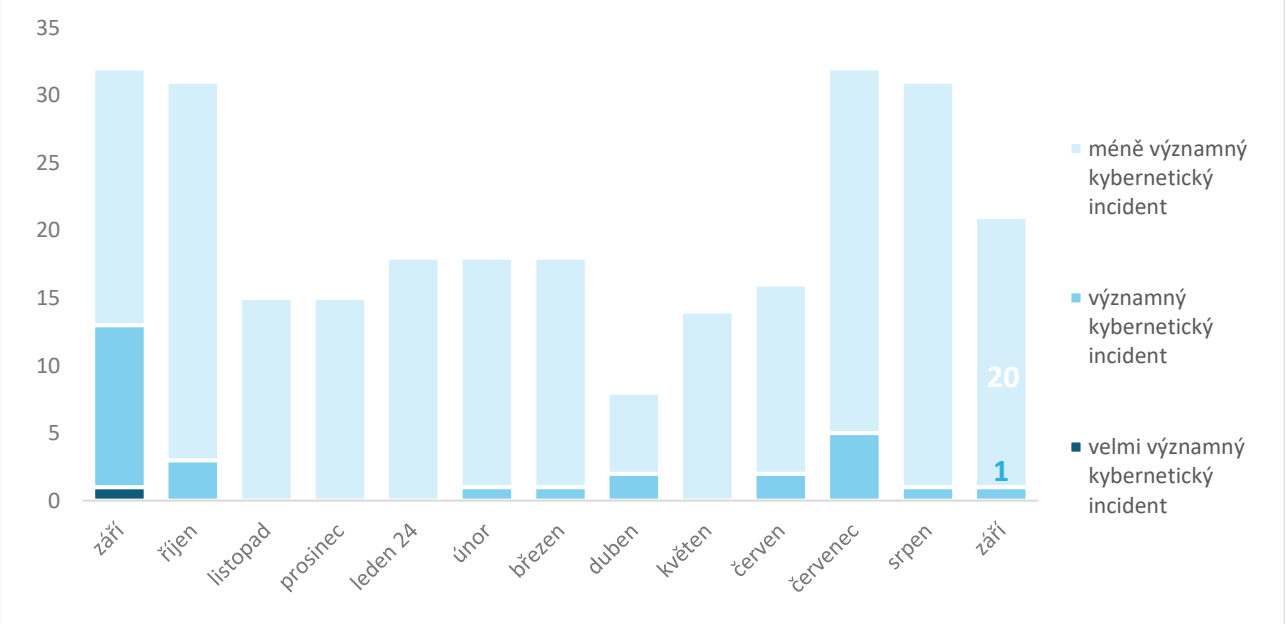
Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

Během září došlo k poklesu evidovaných incidentů na výslednou hodnotu 21, oproti oběma letním měsícům tak došlo ke snížení hodnot na průměrné roční hodnoty.



Závažnost řešených kybernetických incidentů[1]

Obdobně jako v srpnu byl pouze jeden incident vyhodnocen jako významný, zbylých 20 spadalo do kategorie méně významných.



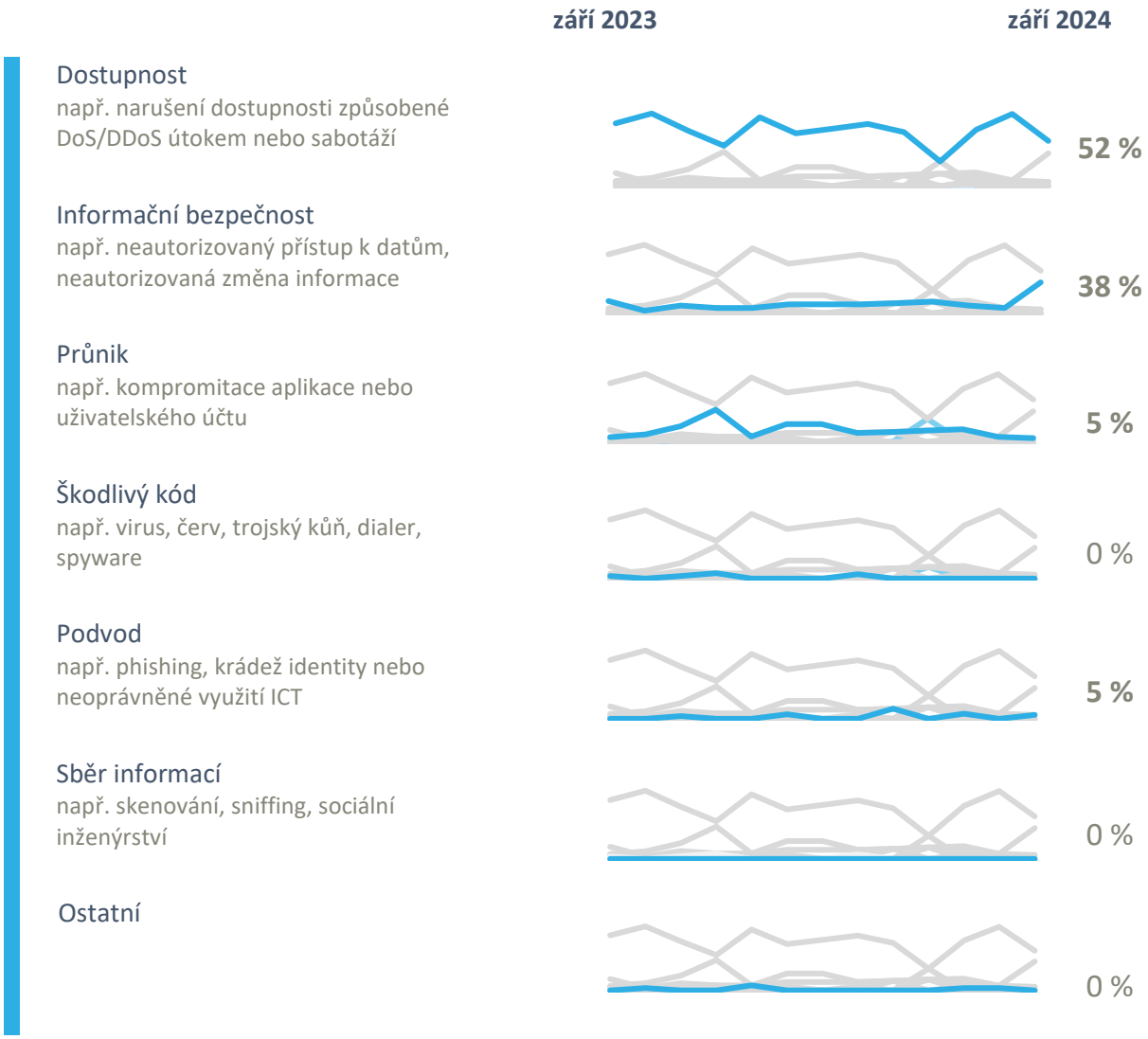
[1] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, a v interní metodice NÚKIB.

Klasifikace incidentů nahlášených NÚKIB[2]

Nejpočetnější kategorií incidentů i nadále zůstává Dostupnost. V září však byla většinou tvořena výpadky služeb v důsledku technických závad či miskonfiguracemi, v několika případech i v důsledku povodní. Přesto však NÚKIB evidoval i pět DDoS útoků.

NÚKIB dále řešil incidenty ve třech kategoriích:

- Osm incidentů spadá do kategorie Informační bezpečnost, přičemž tři z nich představují ransomwarové útoky. Dále se jednalo o zneužití přihlašovacích údajů do informačního systému a také různé úniky interních dat.
- V rámci kategorie Průnik evidoval NÚKIB jeden incident prolomení uživatelských účtů.
- Poslední kategorií byl Podvod, ve které NÚKIB evidoval jeden případ phishingu. Neznámý útočník se při něm snažil přesměrovat platbu skrze zneužití identity napadené společnosti. Informace potřebné k zacílení útoku získal právě skrze phishing.



[2] Klasifikace kybernetických incidentů je založena na taxonomii ENISA: Reference Incident Classification Taxonomy — ENISA (europa.eu).

Trendy v kybernetické bezpečnosti za září pohledem NÚKIB[3]

Phishing, spear-phishing a sociální inženýrství

NÚKIB v září evidoval jeden incident, při němž byl využit phishing. Neznámý útočník nejprve skrze phishing získal přístup k e-mailové korespondenci napadené společnosti, přičemž tyto informace posléze použil ve snaze přesvědčit klienta této společnosti k přesměrování platby na jeho účet. K tomu zneužil i identitu napadené společnosti.

Malware

V září podobně jako v uplynulých měsících probíhaly kontinuální aktivity v oblasti malwarové analýzy v souvislosti s některými dříve evidovanými incidenty.

Zranitelnosti

Během září NÚKIB pokračoval v publikaci zranitelností skrze sociální síť X.

Byly zde zveřejněny informace například o kritické zranitelnosti v aplikaci Gitlab či dvou zranitelnostech služeb WMware.

Ransomware

V září byly evidovány tři případy ransomwarových útoků. Jednalo se o ransomware Akira, DORRA a LockBit 3.0, přičemž pouze jeden byl veden vůči regulovanému subjektu. Všechny tři však byly úspěšné a zašifrovaly část dat obětí.

Útoky na dostupnost

V průběhu září NÚKIB evidoval pět DDoS útoků. Většina z nich byla provedena ruskojazyčnou skupinou NoName057(16). Oproti více než dvacítce podobných útoků ze srpna se však jednalo o razantní snížení jejich frekvence.

[3] Vývoj ilustrovaný šipkou je vyhodnocován ve vztahu k předešlému měsíci.

Zaměřeno na hrozbu: Phishingová kampaň cílí na účastníky mezinárodní bezpečnostní konference IISS Prague Defence Summit

Bezpečnostní výzkumníci platformy Hunt.io objevili phishingovou kampaň, která cílí primárně na účastníky listopadové mezinárodní konference IISS Prague Defence Summit pořádané britským think tankem Mezinárodní institut strategických studií (IISS). Této významné akce pořádané v Praze se zúčastní vysocí vládní představitelé, představitelé obranného průmyslu, analytici či média. Klíčovými tématy summitu budou obranně-průmyslová spolupráce, pokroky ve vojenských aplikacích nových technologií, jakož i otázky spojené s řešením významných konfliktů. Podle analýzy Hunt.io spočívá phishingový útok v zaslání ZIP souboru obsahujícího škodlivý soubor i reálnou pozvánku na konferenci. Po jeho spuštění dochází k vytvoření persistence v síti oběti a nastavení C2 komunikace se serverem útočníka.

Obr. 1: Program chystané konference IISS Prague Defence Summit, jakožto součást phishingové zprávy (větší rozlišení)

IISS PRAGUE DEFENCE SUMMIT
8 – 10 November 2024

As at 13 June 2024

OUTLINE AGENDA

All events will take place at the Prague Marriott Hotel,
V Celnici 8, 110 00 Prague, Czech Republic,
except for dinner on Saturday evening, which will be held at the Žofín Palace

All sessions will be on-the-record

FRIDAY 8 NOVEMBER

All day	BILATERAL MEETINGS BETWEEN GOVERNMENT DELEGATIONS
14:30 – 15:30	PRESENTATION OF IISS PRAGUE DEFENCE SUMMIT RESEARCH REPORT
16:00 – 17:30	SIMULTANEOUS SPECIAL SESSIONS
	Session I: **PROCURING FOR NATIONAL REQUIREMENTS**
	Session II: **INNOVATING AT SPEED**
	Session III: **DEFENCE PLANNING AND OPERATIONAL NEEDS**
18:30 – 19:30	WELCOME RECEPTION
	MINISTERIAL RECEPTION (BY INVITATION ONLY)
19:30 – 21:30	KEYNOTE ADDRESS & OPENING DINNER

SATURDAY 9 NOVEMBER

08:55 – 09:00	OPENING OF THE SUMMIT AND WELCOME REMARKS
09:00 – 10:30	FIRST PLENARY SESSION **RETHINKING EUROPEAN DEFENCE REQUIREMENTS AND CAPACITY**
10:30 – 11:00	*Refreshment Break*
11:00 – 12:30	SECOND PLENARY SESSION **TOWARDS A NEW ERA OF TECHNOLOGY SHARING**

Zdroj: hunt.io

Ačkoli analýza nezahrnuje následnou činnost útočníka v síti oběti, lze předpokládat, že cílem útočníků je sběr zpravodajsky významných informací. Řada indikátorů obsažených v analýze Hunt.io odkazuje na potenciální zapojení čínského státem sponzorovaného aktéra Mustang Panda. Jedná se zejména o využití backdooru Toneshell, který byl v minulosti evidován u několika kampaní této skupiny či využití protokolu TCP maskovaného jako protokol TLS. Některé zaznamenané techniky však v menší míře odpovídají dřívějším aktivitám skupiny APT-Q-27, která v minulosti prováděla útoky v jihovýchodní Asii.

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	20–35 %
Velmi nepravděpodobně	0–15 %

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 sdílená 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.