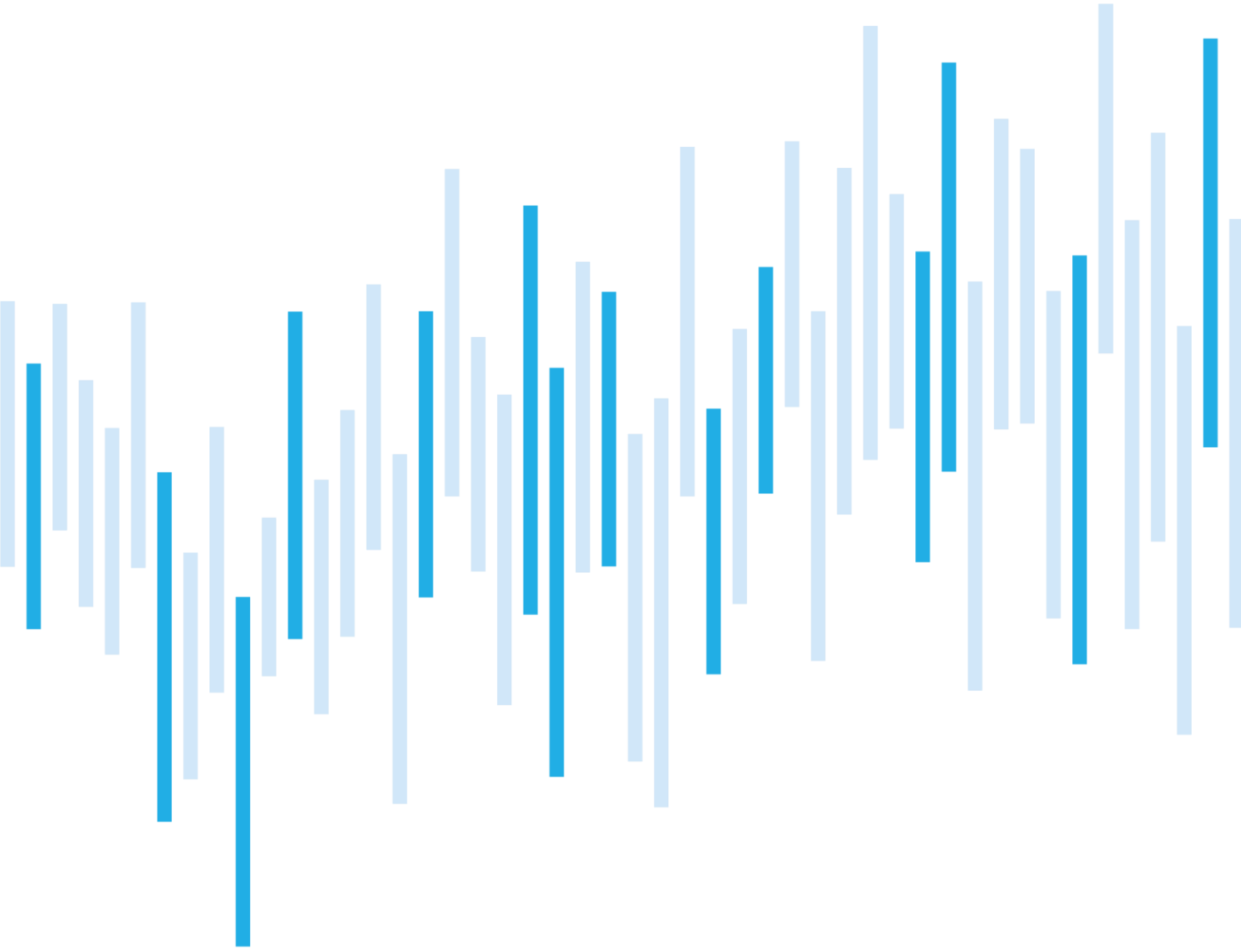
Kybernetické incidenty pohledem NÚKIB

SRPEN 2022



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

Počet kybernetických incidentů se během srpna pohyboval na velmi podprůměrných hodnotách, přestože ve srovnání s měsícem červencem mírně stoupl. NÚKIB obvykle v letních měsících eviduje nižší počet incidentů. Téměř polovina incidentů byla klasifikována jako významná.

V srpnu výrazně převážily incidenty, které hlásily nepovinné subjekty. Podobně jako v předcházejícím měsíci navíc nelze určit více zasažený sektor.

Vzhledem ke skutečnosti, že v září začíná akademický rok, zaměřili jsme se nyní na útoky vůči univerzitám. Ty představují atraktivní cíl z pohledu kybernetické špionáže, neboť často provádějí pokročilý výzkum neveřejného charakteru, ale i kvůli možnosti finančních zisků.

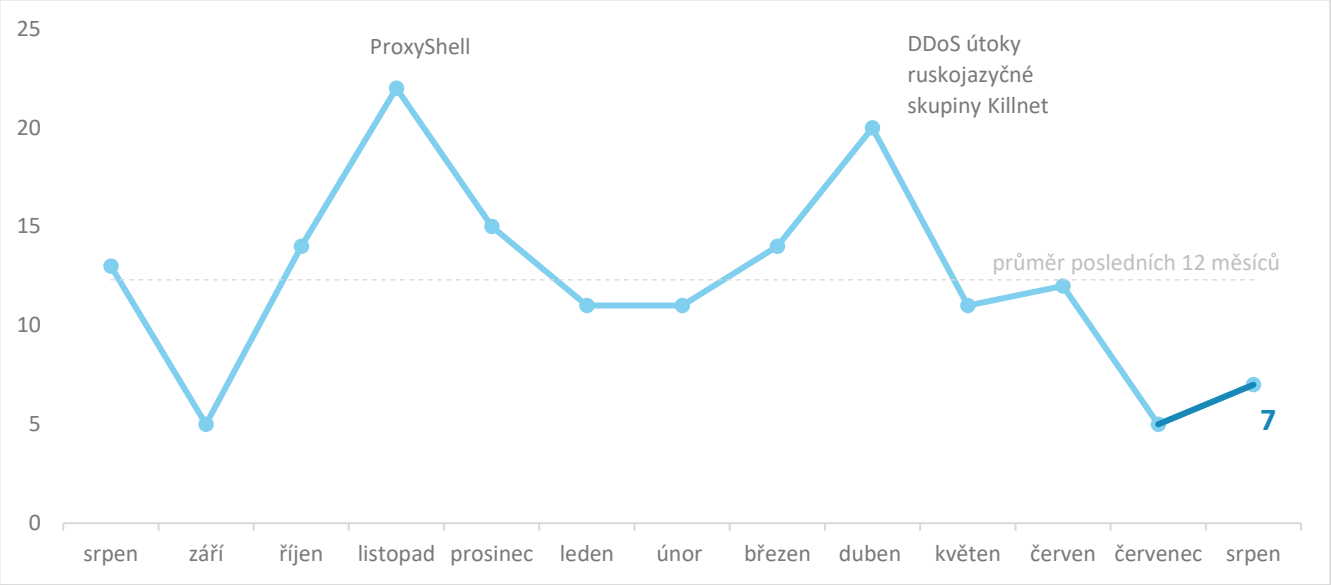
Obsah

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

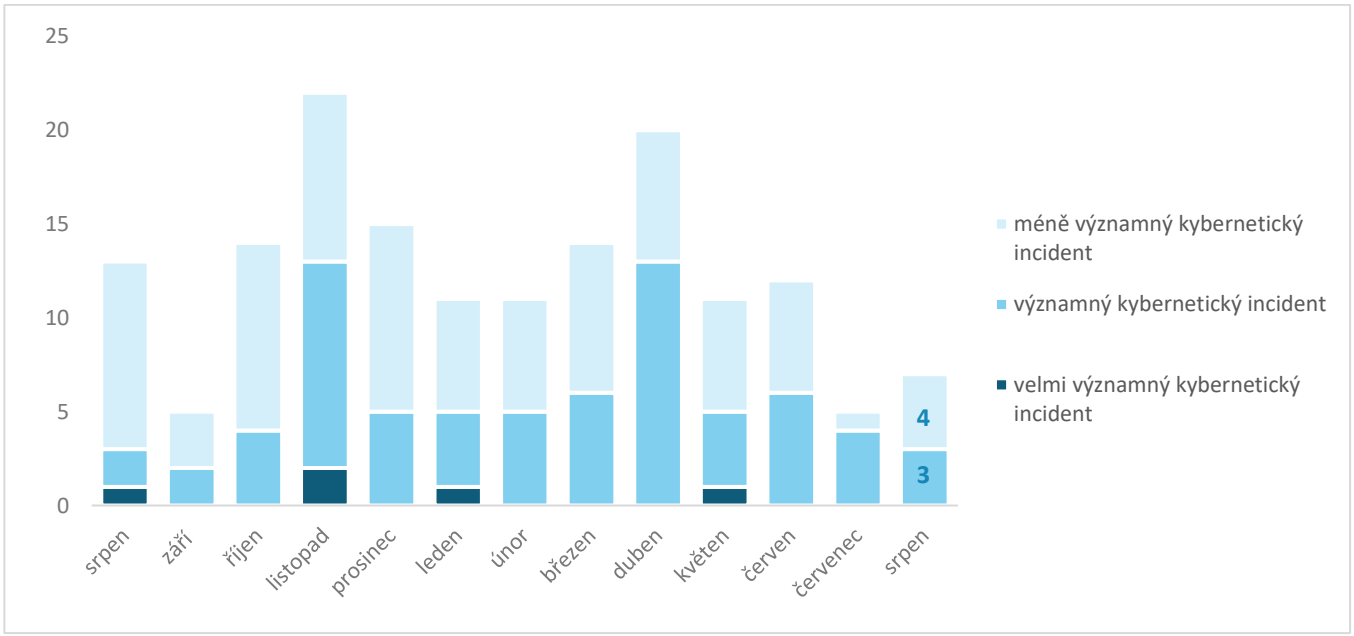
Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

Počet incidentů se v měsíci srpnu držel na velmi podprůměrných hodnotách. Přesto ve srovnání s červencem došlo k mírnému nárůstu.[1]



Závažnost řešených kybernetických incidentů[2]

Během měsíce srpna velice mírně převažovaly méně významné incidenty nad významnými. Velmi významný incident opět nebyl evidován, přičemž naposledy k němu došlo v květnu.



[1] Dva incidenty nahlásily NÚKIB povinné osoby dle zákona o kybernetické bezpečnosti. O zbylých pěti incidentech pak NÚKIB informovaly zákonem neregulované subjekty.
[2] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, a v interní metodice NÚKIB.

Klasifikace incidentů nahlášených NÚKIB[3]

Srpnové kybernetické incidenty NÚKIB zařadil do čtyř kategorií:

- Nadále docházelo k útokům na dostupnost, které jsou trvalým trendem. Ve dvou případech šlo o DDoS útok, naopak ransomware stál za jednou ze způsobených nedostupností.
- Trvajícím trendem jsou i průniky, jejichž počet se od června drží na stejné hodnotě.
- Po měsíční pauze byl evidován incident typu škodlivý kód. Konkrétně šlo o ransomware, který je známý jako Loki Locker.
- Podobně byl po měsíční pauze evidován incident typu podvod. Jednalo se o phishing v nizozemském jazyce, který byl téměř jistě nasazen pro sběr přihlašovacích údajů.

	srpen 2021		srpen 2022
Dostupnost např. narušení dostupnosti způsobené DoS/DDoS útokem nebo sabotáží	31 %		**43 %**
Průnik např. kompromitace aplikace nebo uživatelského účtu	23 %		**29 %**
Podvod např. phishing, krádež identity nebo neoprávněné využití ICT	15 %		**14 %**
Škodlivý kód např. virus, červ, trojský kůň, dialer, spyware	15 %		**14 %**
Informační bezpečnost např. neautorizovaný přístup k datům, neautorizovaná změna informace	15 %		**0 %**
Pokus o průnik např. pokus o zneužití zranitelnosti, pokus o přihlášení apod.	0 %		**0 %**
Sběr informací např. skenování, sniffing, sociální inženýrství	0 %		**0 %**
Urážlivý obsah např. spam, kyberšikana, nevhodný obsah	0 %		**0 %**
Ostatní	0 %		**0 %**

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

Trendy v kybernetické bezpečnosti za srpen pohledem NÚKIB[4]

Phishing, spear-phishing a sociální inženýrství

Phishing nebo pokusy o něj jsou permanentní trend. Během srpna byl nejzajímavějším případem nizozemsky psaný phishing, který byl téměř jistě nasazen za účelem sběru přihlašovacích údajů.

Malware

NÚKIB na základě dat ze srpnových incidentů žádný malware neanalyzoval.

Zranitelnosti

Během srpna vydal NÚKIB dvojici upozornění. Prvním bylo upozornění na sadu zranitelností týkajících se softwaru VMware a platformy VMware vRealize Operations. Zranitelností bylo celkem deset a dle standardu CVSSv3 obdržely skóre od 4.7 do 9.8 (9-10 značí kritickou zranitelnost). Na konci srpna bylo vydáno druhé upozornění na phishingovou kampaň, jejímž cílem je zneužít bankovní identitu. Motivem je nabídka příspěvku od Ministerstva práce a sociálních věcí.

Ransomware

Trend vyděračských útoků pokračoval i v srpnu. Počet evidovaných útoků pak zůstal na stejných hodnotách, přičemž šlo o ransomwary Hive a Loki Locker.

Útoky na dostupnost

Poprvé od měsíce dubna byly evidovány DDoS útoky. V jednom případě šlo o SYN Flood, kdy bylo dotčeno okolo 10 tisíc uživatelů. Ve druhém případě pak byla detekována kombinace útoků typu TCP SYN Flood, DNS Flood či ICMP Flood.

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

Technika měsíce: Network Denial of Service

NÚKIB kybernetické incidenty vyhodnocuje mj. na základě rámce MITRE ATT&CK, jenž slouží jako přehled známých technik a taktik používaných při kybernetických útocích. V tomto měsíci jsme se vzhledem k opětovnému výskytu DDoS zaměřili na techniku T1498: Network Denial Service.

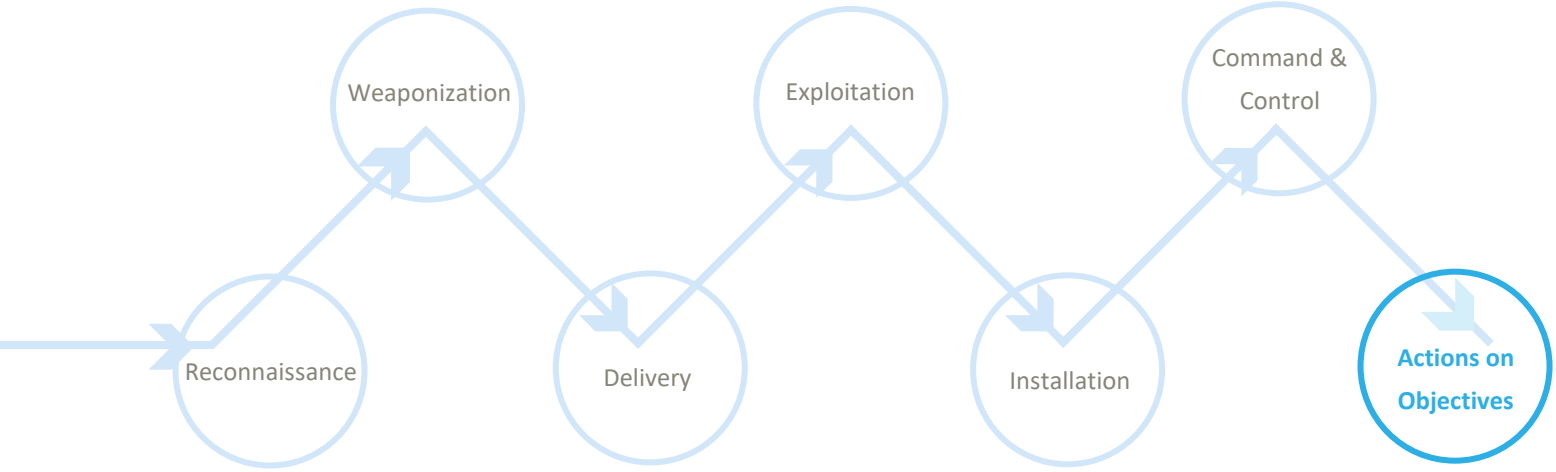
MITRE ID: T1498

Útočníci mohou provádět útoky Network Denial of Service (DoS) za účelem snížení nebo zablokování dostupnosti. Daný typ útoků pak lze provést vyčerpáním šířky pásma sítě, na něž se služby spoléhají. Může se jednat o webové stránky, e-mailové služby, DNS či tzv. web-based aplikace. Útočníci mohou mít různé motivace od politických po hacktivismus nebo snahu odvést pozornost od dalších útoků.

K tomuto typu útoku dojde, když útočníci „zahltí“ šířku pásma síťového připojení svým škodlivým provozem. Ten může generovat jeden systém (Denial of Service, DoS) nebo mnoho systémů (Distributed Denial Service, DDoS). Podobný typ útoku má za následek omezení dostupnosti dat a obvykle nemá dlouhodobější dopady.

Mitigace: Klíčovou mitigační technikou je filtrování síťového provozu. Je třeba odfiltrovat škodlivý provoz od legitimního, což poskytují poskytovatelé internetových služeb (ISP) či třetí strany. V závislosti na objemu může být on-premises filtrování možné blokováním zdrojových adres, jež jsou zdrojem útoku, zacílených portů či protokolů používaných pro přenos.

Znázornění techniky T1498 v kill chainu ukazujícím, kdy útočníci techniku používají:



Zaměřeno na trend: útoky na univerzity a pokročilý výzkum

Vzhledem k začátku akademického roku jsme se tento měsíc rozhodli zaměřit na trend v podobě kybernetických hrozeb, jež směřují na vysoké školství a výzkum, jenž probíhá v univerzitním prostředí.

Obr 1: Ilustrativní obrázek univerzity

Univerzity představují atraktivní cíl kvůli spektru informací, se kterými pracují. Významná část z nich se navíc týká doposud nepublikovaných výzkumů. Vysoké školství pak často disponuje relativně vysokými finančními prostředky, což zvyšuje přitažlivost pro útočníky motivované finančním ziskem, kteří nejčastěji nasazují ransomware. Vzhledem k počtu tisíců či dokonce desetitisíců uživatelů (studentů) jsou navíc univerzity mimořádně závislé na informačních systémech, jež často mohou trpět „každodenními“ problémy (např. zastaralé verze softwaru/hardwaru). Případně nejsou uživatelé dostatečně proškoleni.

V případě univerzitního prostředí je z pohledu útočníků nejefektivnější využít za účelem zajištění prvotního vstupu (spear)phishing, a to vzhledem k vysokému počtu uživatelů. Po vytvoření persistence v cílovém systému se útočník může zaměřit na kybernetickou špionáž směřovanou prioritně do oblasti pokročilého či dosud nepublikovaného výzkumu nebo naopak zašifrování systémů kvůli zisku financí.

Úplně specifickou a stále do jisté míry podceňovanou hrozbou je útok zevnitř, tedy způsobený tzv. insiderem. Podobně si subjekty neuvědomují rizika spjatá s dodavateli.

Doporučení: Je naprosto nezbytné dodržovat základní bezpečnostní standardy, přičemž využít lze také materiály NÚKIB (např. Minimální bezpečnostní standard). Vyjma toho NÚKIB vydal doporučení, která se týkají konkrétních hrozeb (např. spear-phishing).

Akademické instituce by měly celkově usilovat o to, aby disponovaly dostatečnými zdroji v personální, technické i finanční rovině kvůli tvorbě efektivní obrany vůči širokému spektru útočníků. Vzhledem k rozsáhlosti systémů a počtu uživatelů je nutné provádět jejich pravidelná školení. Zvláštní důraz by pak měl být kladen na obranu před útokem zevnitř či kompromitací skrze rizikové dodavatele.

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	25–50 %
Nepravděpodobně	15–20 %
Velmi nepravděpodobně	0–10 %

Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách www.nukib.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	Informace může být sdílena v rámci organizace, které byla informace poskytnuta. Dále může být poskytnuta pouze těm partnerům, kteří splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. Jiným osobám než výše uvedeným, nesmí být informace poskytnuta.
TLP: AMBER+STRICT	Informace může být sdílena pouze v rámci organizace, které byla informace poskytnuta.
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.