Národní úřad pro kybernetickou a informační bezpečnost
Mučednická 1125/31
616 00 Brno – Žabovřesky
IČO: 05800226
ID datové schránky: zzfnkp3

Spisová značka:
350 - 401/2022
Číslo jednací:
3381/2022-NÚKIB-E/350

Brno, 21. března 2022

VAROVÁNÍ

Národní úřad pro kybernetickou a informační bezpečnost, se sídlem Mučednická 1125/31, 616 00 Brno (dále jen „Úřad“), podle § 12 odst. 1 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „zákon o kybernetické bezpečnosti“), vydává toto

varování

před hrozbou v oblasti kybernetické bezpečnosti spočívající v nedodržení smluvních závazků ze strany dodavatelů ICT služeb a produktů s významným vztahem k Ruské federaci.

Úřad hrozbu hodnotí na úrovni Vysoká – Hrozba je pravděpodobná až velmi pravděpodobná.

Úřad v souvislosti s vysokou mírou této hrozby doporučuje orgánům a osobám povinným dle zákona o kybernetické bezpečnosti následující kroky:

1. Prověřit, zda v rámci svých systémů používají ICT služby či produkty závislé na dodavatelích s významným vztahem k Ruské federaci. Významný vztah k Ruské federaci indikují následující ukazatele:

   1.1. Dodavatel má sídlo v Ruské federaci, nebo je závislý na dodávkách z území Ruské federace.

   1.2. ICT produkt nebo služba podstatná pro funkčnost spravovaného či provozovaného informačního či komunikačního systému je dodávána prostřednictvím pobočky dodavatele v Ruské federaci.

   1.3. ICT produkt nebo služba podstatná pro funkčnost spravovaného či provozovaného informačního či komunikačního systému má svůj vývoj či výrobu lokalizované v Ruské federaci.

2. Obdobně pak prověřit, zda jejich významní dodavatelé ve smyslu § 2 písm. n) vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat

(dále jen „vyhláška o kybernetické bezpečnosti“) používají ICT služby či produkty závislé na dodavatelích s významným vztahem k Ruské federaci.

3. V případě, že tyto orgány a osoby nebo jejich významní dodavatelé používají ICT služby či produkty závislé na dodavatelích s významným vztahem k Ruské federaci, dané dodavatele s významným vztahem k Ruské federaci kontaktovat a zjistit:

   3.1. Zda má riziko dopadu sankcí a riziko možné nedostupnosti relevantních služeb řešeno v rámci svého řízení kontinuity činností a jakým způsobem.

   3.2. V případě, že s touto variantou v řízení kontinuity činností dodavatel nepočítá či řešení není v daném případě uspokojivé, zažádat dodavatele o sjednání nápravy.

   3.3. V případě, že náprava podle bodu 3.2. nebude možná, zapracovat (vzhledem ke zvýšené hrozbě nedodržení smluvního závazku) postup pro případ přerušení dodávky této ICT služby či produktu do svého řízení kontinuity činností a zvážit náhradní řešení, pokud je takové náhradní řešení možné.

ODŮVODNĚNÍ

1. Na základě skutečností zjištěných při výkonu své působnosti, stejně tak jako na základě skutečností, které se Úřad dozvěděl od orgánů, které vykonávají působnost v oblasti kybernetické bezpečnosti v zahraničí, i tuzemských partnerů, dospěl Úřad k tomu, že nedodržení smluvních závazků ze strany dodavatelů ICT služeb a produktů s významným vztahem k Ruské federaci představuje hrozbu v oblasti kybernetické bezpečnosti, a proto podle § 12 odst. 1 zákona o kybernetické bezpečnosti vydává toto varování.

2. K vydání tohoto varování vedla kombinace následujících poznatků a zjištění.

3. ICT služby a produkty dodávané společnostmi s významným vztahem k Ruské federaci mohou být v současné situaci významně ovlivněny v důsledku přijímání významných ekonomických sankcí vůči Ruské federaci a ze strany Ruské federace.

4. Výše zmíněné ekonomické sankce (např. významné omezení dovozu strategických komodit do Ruské federace včetně některých ICT technologií či odpojení Ruské federace od systému SWIFT) se mohou na plnění závazků dodavateli s významným vztahem k Ruské federaci přímo či nepřímo projevit v důsledku vícero možných scénářů, následuje popis čtyř vybraných.

5. Samotné sankce uvalené Ruskou federací na Evropskou unii či Českou republiku mohou spočívat ve státním zákazu smluvní závazky vůči společnostem usídleným v Evropské unii potažmo České republice plnit či je do budoucna neprodloužit. Stejně tak mohou plnění závazků společností s významným vztahem k Ruské federaci vůči českým organizacím znemožnit sankce uvalené jinými státy na Ruskou federaci. Dále mohou plnění závazku společnostem s významným vztahem k Ruské federaci znemožnit i ukončené dodávky ICT produktů a služeb ze strany významných nadnárodních ICT společností, které ve významné míře opouštějí ruský trh s technologiemi a službami. Nedostupnost jejich služeb a produktů v rámci Ruské federace může znemožnit poskytování a vývoj služeb a produktů ze strany dodavatelů s významným vztahem k Ruské federaci. Sankce (uvalené na Ruskou federaci)

rovněž spustily odchod mnoha ICT specialistů z Ruské federace, kteří se na vývoji, výrobě a dalších nutných procesech dodavatelů s významnou vazbou na Ruskou federaci podíleli.

6. Pravomoc Úřadu je pro vydání tohoto varování dána ustanovením § 22 písm. b) zákona o kybernetické bezpečnosti, které jej zmocňuje k vydávání opatření. Podle § 11 odst. 2 zákona o kybernetické bezpečnosti patří mezi tato opatření i varování podle § 12 zákona o kybernetické bezpečnosti. Varování vydá Úřad podle § 12 odst. 1 zákona o kybernetické bezpečnosti, dozví-li se zejména z vlastní činnosti nebo z podnětu provozovatele národního CERT anebo od orgánů, které vykonávají působnost v oblasti kybernetické bezpečnosti v zahraničí, o hrozbě v oblasti kybernetické bezpečnosti. V souladu s § 12 odst. 2 zákona o kybernetické bezpečnosti Úřad zveřejní varování na svých internetových stránkách a oznámí je orgánům a osobám uvedeným v § 3 zákona o kybernetické bezpečnosti.

7. Úkolem Úřadu je podle § 22 písm. j) zákona o kybernetické bezpečnosti zajišťovat prevenci v oblasti kybernetické bezpečnosti. Součástí této preventivní činnosti je také poskytování informací o zjištěných hrozbách v oblasti kybernetické bezpečnosti. Pokud však hrozba dosahuje takové intenzity, že informování o ní nelze pokrýt běžnými způsoby preventivní činnosti Úřadu, je v souladu s výše uvedeným Úřad nucen přistoupit k vydání varování podle § 12 zákona o kybernetické bezpečnosti.

8. Úřad upozorňuje, že orgány nebo osoby, které jsou povinny zavést bezpečnostní opatření podle zákona o kybernetické bezpečnosti, v souvislosti s řízením rizik podle § 5 odst. 1 písm. h) bod 3 vyhlášky o kybernetické bezpečnosti při hodnocení rizik a v plánu zvládání rizik zohlední opatření podle § 11 zákona o kybernetické bezpečnosti. Jedním z těchto opatření je i varování podle § 12 zákona o kybernetické bezpečnosti. Na základě výše uvedeného Úřad považuje hrozbu ve výroku tohoto varování za pravděpodobnou až velmi pravděpodobnou. Orgány a osoby, které jsou povinny zavést bezpečnostní opatření podle zákona o kybernetické bezpečnosti, jsou proto povinny tuto hrozbu hodnotit na odpovídající úrovni, tedy na úrovni Vysoká. V případě, že povinná osoba využívá v souladu s odst. 5 přílohy č. 2 vyhlášky o kybernetické bezpečnosti jinou metodu pro hodnocení rizik, je nutno tuto hrozbu hodnotit v rámci této metody na srovnatelné úrovni jako by tomu bylo v případě postupu podle § 5 odst. 1 písm. d) vyhlášky o kybernetické bezpečnosti.

9. Hrozba, před kterou Úřad varuje, přestavuje specifikaci hrozby, jež je typově vydefinována již v rámci vyhlášky o kybernetické bezpečnosti, konkrétně se jedná o typovou hrozbu č. 10 v rámci přílohy č. 3 této vyhlášky „nedodržení smluvního závazku ze strany dodavatele“. S touto hrozbou v její typové obecnosti by tak již nyní měly orgány a osoby povinné podle zákona o kybernetické bezpečnosti pracovat ve svých analýzách rizik a v na ni navazujících procesech. Toto varování pak stanovuje konkrétní míru hrozby vůči dodavatelům, jejichž spolehlivost je ovlivněna současnou geopolitickou situací – vojenským konfliktem Ruské federace s Ukrajinou.

10. Úřad dále upozorňuje, že v souladu s § 4 odst. 4 zákona o kybernetické bezpečnosti jsou orgány a osoby uvedené v § 3 písm. c) až f) zákona o kybernetické bezpečnosti povinny zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich informační nebo komunikační systém a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem

uzavřou. Zohlednění požadavků vyplývajících z bezpečnostních opatření podle věty první v míře nezbytné pro splnění povinností podle zákona o kybernetické bezpečnosti nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.

Ing. Karel Řehka
ředitel
Národní úřad pro kybernetickou a informační bezpečnost
elektronicky podepsáno